UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

PROYECTO FIN DE CARRERA

INFORMÁTICA FORENSE: AUDITORÍA DE SEGURIDAD

Ingeniero de Telecomunicaciones

Jose Manuel Agrelo de la Torre

FEBRERO 2014

Jose Manuel Agrelo de la Torre
Informática forense: auditoría de seguridad

Jose Manuel Agrelo de la Torre
Escuela Politécnica Superior. Dpto. de Ingeniería Informática

IMPRESO EN ESPAÑA – PRINTED IN SPAIN

Informática forense: auditoría de seguridad

AUTOR: Jose Manuel Agrelo de la Torre
TUTOR: Dr. Eloy Anguiano Rey

Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid

FEBRERO 2014

AGRADECIMIENTOS

En primer lugar, quiero agradecerle a mi tutor, Eloy Anguiano, su ayuda y apoyo a lo largo de la realización de todo el proyecto. También me gustaría agradecerle el haberme propuesto este proyecto y el presentarme el mundo de la seguridad siendo mi profesor. También, me gustaría agradecerles a mis otros profesores de la universidad, por haberme enseñado tanto, sobretodo a valerme por mí mismo.

Además quiero agradecer a toda mi familia su apoyo a lo largo, tanto de la carrera, como de la realización del presente proyecto. Los cuales no han dudado en apoyarme y hacerme ver que con esfuerzo todo se puede conseguir. En especial a mi hermana María, que incluso desde el extranjero no ha cesado de apoyarme y preocuparse por mí.

También me gustaría agradecerles a mis compañeros de clase los buenos ratos que me han hecho pasar, haciendo mas leve mi paso por la universidad. Permitiendo de esta manera que no perdiera los ánimos por continuar.

Por último, pero no menos importante me gustaría darle las gracias a mis amigos, que me han apoyado durante incontables años. En especial agradecerles a Zulema Vázquez y Carlos Ramón Rojo, puesto que dejaron de ser solo amigos hace tiempo, y sin su apoyo no habría llegado a ser la persona que soy hoy.

Muchas gracias a todos.

Abstract

This project shows the process of a security audit to a business net to accomplish the fulfilment of the official security normative. Due to a network is needed to make a security audit, the design of the net and its implementation would also be done. Therefore, the project consists of two distinct parts.

In the first part of the project, it begins from a policy established by the company to realize the design and implementation of the network. Along this part, the different procedures to take decisions are explained. Later, starting with the established design the implementation of the network is realized, showing the different programs and configurations used. In this way, the implementation of the net is done preparing it to the security audit.

Once a business network have been design, it proceed to the security audit realization. On the security audit it realizes a normative revision and a business security revision, reviewing both physical security and possible vulnerabilities. For this realization some actual auditing tools will be used such as `Kali™` or *Metasploit™*.

In the end, it presents a report where it resume the different violations of the normative and its solution, as well as, an abstract with the different security breaches that exist on the company. This report would be the one that will be given to the client company after the security audit, so it can solves its security breaches.

Keywords

Design, network, auditory, security, server, `Kali™`, *Metasploit™*, implantation, *firewall*, router, *Nessus™*, security audit, state normative, normative.

Resumen

En este proyecto se muestra el proceso de realización de una auditoría de seguridad a una red empresarial para cumplir con la normativa establecida para los organismos oficiales del estado. Debido a que para la realización de la auditoría se debe contar con una red empresarial, también se realiza el diseño e implementación de la misma. Por lo tanto el presente proyecto consta de dos partes bien diferenciadas.

En la primera parte del proyecto, se parte de una política establecida por una empresa para realizar el diseño de la red y su posterior implantación. A lo largo de la misma, se explican los diferentes procedimientos realizados para la toma de decisiones. Posteriormente, partiendo del diseño establecido se realiza la implementación de la red empresarial explicando los diferentes programas utilizados y las configuraciones utilizadas. De esta manera, se realiza la implementación de la red para la realización de la auditoría.

Una vez se cuenta con la red empresarial, se procede a la realización de la auditoría. En ésta se realiza, tanto una revisión de la normativa que se aplica a los organismos oficiales del estado, como una revisión de la seguridad de la empresa, tanto de la seguridad física como de las posibles vulnerabilidades existentes en los diferentes equipos. Para la realización de esta auditoría se utilizan las herramientas actuales como son `Kali™` o *Metasploit™*.

Por último, se presenta un informe en el que se resumen los diferentes incumplimientos de la normativa y su solución, así como, un resumen de las diferentes brechas de seguridad existentes en la empresa. Este informe sería el informe a presentar a la empresa tras la realización de la auditoría para que corrija sus problemas de seguridad.

Palabras clave

Diseño, red, auditoría, seguridad, servidor, `Kali™`, *Metasploit™*, implantación, *firewall*, *router*, *Nessus™*, auditoría de seguridad, normativa del estado, normativa, BOE.

ÍNDICE

LISTAS

Lista de cuadros

Lista de figuras

Lista de tablas

ACRÓNIMOS

ANSI	American National Standards Institute
BOE	Boletin Oficial del Estado
CUPS	Common Unix Printing System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IMAP	Internet Message Access Protocol
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MDA	Mail Delivery Agent
MTA	Mail Transfer Agent
MUA	Mail User Agent
PDF	Portable Document Format
PHP	HyperText PreProcessor
POP3	Post Office Protocol
RFC	Requests for Comments
RRHH	Recursos Humanos
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TTL	Time To Live
USB	Universal Serial Bus

I

Contenidos previos

1 Introducción

1.1. Motivación

Este proyecto consiste en la realización de una auditoría de seguridad a una red empresarial para la adaptación de la misma para el cumplimiento del Real Decreto 3/2010 [21].

Para la realización de esta auditoría es necesario disponer de una red y, por tanto, se hace necesario el diseño y la implementación de una red empresarial, junto con los servicios de los que dispondrá esta red, a partir de unas políticas establecidas por una empresa hipotética.

Una vez se disponga de esta red se realizará la auditoría de seguridad de la misma comprobando, además de los posibles fallos de seguridad que pueda tener, que cumpla con la normativa de los organismos del estado que se incluye en el Real Decreto 3/2010.

1.2. Objetivos

Los objetivos de este proyecto desde el punto de vista personal son cuatro:

- La adquisición de conocimientos en el proceso que conlleva la implementación de una red empresarial desde el diseño de la misma a partir de unas políticas establecidas por la empresa
- La adquisición de conocimientos en el proceso de realización de una auditoría de seguridad y de las diferentes herramientas que se utilizan para ello
- La adquisición de conocimientos en la normativa vigente de la seguridad de las telecomunicaciones.
- La adquisición de conocimientos acerca los fallos de seguridad más comunes en las redes junto con sus soluciones, y las acciones más frecuentes en los ataques a las redes junto con como prevenirse de los mismos

Por otro lado, desde el punto de vista empresarial los objetivos son tres:

- Obtener una red empresarial con diferentes servicios funcionando correctamente y de forma segura.
- Comprobación del cumplimiento de la normativa que se aplica a los organismos oficiales del estado.
- Realización de un auditoría de seguridad en la que se expresen las diferentes brechas de seguridad existentes en la red empresarial, tanto de seguridad física como de las vulnerabilidades de los diferentes servidores.

1.3. Organización de la memoria

Debido a la naturaleza del proyecto, la realización del mismo se puede diferenciar en dos grandes partes, siendo estas el diseño e implementación de la red y la realización de la auditoría de seguridad respectivamente. Por lo tanto, la memoria del proyecto se ha organizado en tres partes, ya que se añade una parte con los contenidos previos, dividiendo cada una de ellas en los capítulos oportunos:

Parte 1 - Contenidos previos : en esta parte se incluyen los contenidos previos al comienzo del diseño de la red y la auditoría de seguridad. En esta parte se incluyen los siguientes capítulos:

- **Introducción** : capítulo actual en el que se describen los aspectos de motivación, objetivos y organización de la memoria.
- **Estado del arte** : capítulo en el que se expondrá una breve visión de la situación actual respecto a las redes empresariales, así como, de la situación de la seguridad informática en la actualidad. Tratando también, la normativa vigente en este ámbito junto con una breve explicación de los diferentes protocolos utilizados. Por último, se explica que es un auditoría de seguridad y los diferentes tipos que existen.

Parte 2 - Diseño e implementación previo de la red empresarial : a lo largo de esta parte se describirá todo el proceso realizado desde el diseño de la red a partir de las políticas establecidas, hasta la implantación de la propia red funcionando correctamente. En esta parte se incluyen los siguientes capítulos:

- **Políticas de diseño y seguridad de la red** : en este capítulo se encontrarán las diferentes políticas establecidas por la empresa, las cuales se deben cumplir al realizar el diseño de la red.
- **Diseño e implementación de la red** : el contenido de este capítulo incluye el proceso de diseño de la red teniendo en cuenta las políticas establecidas, enumerando cuales son los aspectos a tener en cuenta en el diseño de la misma. También incluye el proceso de implementación de esta misma red explicando el proceso de instalación de los diferentes servicios.
- **Diseño e implementación de la seguridad** : a lo largo de este capítulo se especifican cuales son los diferentes aspectos de seguridad a tener en cuenta en el diseño de una red, así como, cuáles han sido las decisiones tomadas en la red que se diseña acerca de los mismos.
- **Diseño e implementación de los servicios** : en este último capítulo de la parte a la que pertenece se incluye el diseño e implementación de los diferentes servicios. En este proceso se incluye desde la selección del tipo de servidor que se utilizará incluyendo las razones de la elección, hasta cual será la configuración utilizada en la red proporcionando también argumentos acerca de la elección de la misma.

Parte 3 - Auditoría de seguridad : en esta parte se incluye el proceso de realización de la auditoría de seguridad, en la cual se revisará tanto los posibles errores de seguridad existentes en la red, como el cumplimiento de la normativa especificada.

- **Diseño del proceso de auditaje** : a lo largo de este capítulo se incluye cual es el proceso que se seguirá para la realización de la auditoría. Además, se explicarán las diferentes fases del mismo haciendo referencia a las razones de realizar la auditoría tal como se expone.
- **Realización de la auditoría** : en este capítulo se encuentra la propia realización de la auditoría, donde se realiza tanto la revisión de la normativa como el test de penetración. Además, a lo largo de este capítulo se explica también cuales son los diferentes procesos que se han llevado a cabo para la realización de la auditoría en detalle.
- **Reporte de resultados** : en este apartado se encontrarán los informes de los resultados obtenidos con la realización de la auditoría, siendo presentados estos como informe final a entregar al cliente que solicita la auditoría.

2

Estado del Arte

2.1. Redes empresariales

Con el desarrollo de las tecnologías, las empresas han comenzado a aprovecharlas para aumentar los recursos ofrecidos, tanto para los trabajadores como para los clientes, proporcionando servicios de todo tipo, e incluso tan nuevos, como el `Cloud Computing`.

Las redes de estas empresas, han ido creciendo de manera directamente proporcional al desarrollo de las tecnologías y al crecimiento de la empresa. Por lo que este es un pilar importante a tener en cuenta a la hora de crear una empresa. Por tanto, una empresa, actualmente, tiene que plantearse ciertas cuestiones:¿se tienen servidores públicos?, ¿se tienen servidores centrales con información de la empresa?, ¿sólo tendrá acceso cierta gente o podrá acceder todo el mundo? entre muchas otras. Todas estas preguntas, tienen que ser respondidas por la empresa antes de constituir su servicio de redes, sobretodo debe centrar su atención en ¿qué seguridad tendrá mi red de empresas?

Al igual que han ido aumentando los servicios de redes han aumentado sus vulnerabilidades y, por tanto, cada vez es más importante centrar recursos en la ciberseguridad y contratar auditorías de seguridad para poder conocer las brechas de seguridad que tiene la red y poder solucionarlas con la mayor brevedad posible. Pero, sin meterse en algo tan complicado, empezando por el principio ¿Cómo se diseña una red de empresa?

Los tres puntos principales y básicos a los que hay que dar solución son: [30]

Conectarse a internet de manera segura. Una empresa sin acceso a internet, ahora mismo, no tiene cabida en la mente de ningún emprendedor. Es completamente necesario tener acceso a este servicio por parte de cualquier empresa, ya sea una empresa tecnológica o no, ya que permite la conexión directa con los clientes y/o proveedores, así como también permite el acceso remoto a cualquier servidor de la empresa. Lo complicado de este punto es la seguridad ¿cómo se conecta de manera segura a internet? Para ello se tienen los *irewall* o cortafuegos, que puede bloquear el tráfico que recibe en función de unos filtros preestablecidos, eliminando de esta manera las conexiones indeseadas.

Proporcionar servicios inalámbricos. Para poder proporcionar estos servicios es necesario disponer de hardware especifico, como por ejemplo *routers* o *switchs*. Estos dispositivos hace falta que tengan una conectividad alámbrica, la cual es necesario diseñar a la hora de llevar a cabo el siguiente punto. Este servicio permite una gran movilidad de los clientes y los empleados, los cuales pueden conectar sus tablets u ordenadores portátiles desde cualquier punto dentro del espacio de la red de la empresa.

Diseño de cada una de las redes (tanto inalámbricas como alámbricas). Este punto es uno de los grandes desafíos del diseño de red de una empresa, ya que se tiene un gran problema, del cual se ha recalcado en los párrafos anteriores, la seguridad. Hay que especificar que puntos van a ser públicos y cuales van a ser privados, y, de estos privados, cuales van a ser accesibles para qué personas y a través de que sistemas (Acceso remoto o acceso directo a los diferentes puntos). Para poder llevar a cabo este diseño es necesario describir cada punto de la red en una política de diseño y seguridad, en la cual se especificarán cada uno de estos puntos, así como la seguridad de cada conexión dentro de la red.

2.2. Seguridad Informática

La seguridad informática es un aspecto que abarca un gran número de elementos ya que en la actualidad muchas personas disponen de diferentes dispositivos informáticos, como teléfonos móviles inteligentes o *smartphones* u ordenadores, tanto portátiles como de sobremesa.

Debido a esto, en la actualidad, la mayoría de usuarios introduce información sensible en todos estos dispositivos, tanto en empresas como en uso personal, por lo que se debe disponer de una seguridad adecuada para proteger esta información.

Sin embargo, a causa de esto, también están aumentando considerablemente el número de ataques. Según el informe de seguridad 2013 de `Cisco` [23], el número de amenazas aumentó en 2012 casi un 20 %, debido al aumento en la publicidad de los errores de seguridad así como su inclusión en las diferentes herramientas de ataques. Además, en el informe de seguridad Q3 2013 de `TrendLabs` perteneciente a `Tren Micro` [32], se indica que Java, programa instalado en la mayoría de los equipos, ya que se requiere en numerosas páginas web, es uno de los mayores problemas de seguridad existentes.

Actualmente, la naturaleza de los ataques ha cambiado, mientras que anteriormente las amenazas eran conocidas, puntuales y dispersas, en la actualidad, han cambiado notablemente. Ahora las amenazas son persistentes y mucho más sofisticadas, teniendo normalmente un objetivo concreto, por lo que los atacantes actuales pueden llegar a dedicarle mucho tiempo a un mismo objetivo, encontrando diferentes brechas de seguridad en una empresa [19].

A causa de esto, se podría pensar que solo las grandes empresas reciben ataques informáticos, sin embargo, en España y según un estudio de expertos analistas B2B de `Kapersky Lab` el 71 % de las empresas encuestadas sufrieron ataques de de virus, gusanos, *spyware* u otro tipo de programa malicioso [31].

A partir de esta información se puede resumir que en la actualidad están aumentando el número de ataques a todo tipo de empresas, utilizando modernas herramientas y llegando a dedicar mucho tiempo a algunos de los mismos. Y que, en estos ataques, se adquiere información de todo tipo, por lo que cualquier empresa o incluso usuario puede ser víctima de los mismos.

2.3. Normativa nacional de seguridad

La normativa nacional de seguridad incluye, en diferentes documentos, las diferentes medidas que se deben tomar cuando se utilizan medios informáticos.

En este caso, se deberá tener en cuenta la normativa oficial en la que se especifique las diferentes medidas de seguridad que deben de tener tanto una red como sus servicios. Esta normativa se incluye en el Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

A lo largo de este documento se especifican diferentes medidas que se deben de tomar, desde la seguridad perimetral de los servidores, es decir, la seguridad para acceder a ellos físicamente, hasta las medidas que se deben tomar respecto al cifrado de las conexiones.

En este documento se especifican numerosos artículos, siendo algunos de los más importantes respecto al tema que se está tratando:

Artículo 34.1: los sistemas de información, a los que se refiere el presente real decreto, serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.

Anexo III.2: la auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

- Documentación de los procedimientos.
- Registro de incidencias.
- Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.

Además de artículos como los anteriormente expuestos, también se incluyen cuales deben ser las medidas tomadas respecto a la seguridad de los diferentes elementos. Existen un gran número de medidas, por lo que no es adecuado incluirlas en el documento,sin embargo, un ejemplo de estas es el siguiente:

Anexo II.5.8.1: el correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.
- Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.
- Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:
  - Correo no solicitado, en su expresión inglesa “spam”.
  - Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
  - Código móvil de tipo “applet”.
- Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:
  - Limitaciones al uso como soporte de comunicaciones privadas.
  - Actividades de concienciación y formación relativas al uso del correo electrónico.

Ésta normativa incluye numerosos artículos, algunos de los cuales serán citados posteriormente. En caso de querer visualizarlos se puede acceder al BOE (Boletin Oficial del Estado) donde se encuentran [21].

2.4. Protocolos

Para la realización del proyecto se utilizarán diversos protocolos y servicios para poder cumplir con los requisitos del mismo. A continuación se explican los diferentes protocolos y servicios utilizados, así como, cual es su función. Las explicaciones realizadas son muy breves debido a que se trata de protocolos altamente conocidos y se encuentran perfectamente descritos en los RFC (Requests for Comments) de cada protocolo.

2.4.1. TCP/IP

La familia de protocolos que alberga TCP/IP (Transmission Control Protocol/Internet Protocol) es el conjunto de protocolos en los que se basa internet. Estos protocolos permiten la conexión de diferentes ordenadores independientemente del sistema operativo que estén utilizando.

Para más detalles acerca de TCP/IP se puede consultar el RFC correspondiente [17].

2.4.2. DNS

El protocolo DNS (Domain Name System) es el encargado de traducir los diferentes nombres que se utilizan en internet a las direcciones IP de los equipos a los que se refieren estos nombres. DNS es un sistema de

nomenclatura jerárquica que asigna un nombre de dominio con la dirección IP de un equipo.

Para más información acerca de DNS se puede consultar el RFC correspondiente [2].

2.4.3. DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo de cliente/servidor que permite que el cliente obtenga los parámetros de configuración de la red de forma automática. De esta manera, se puede automatizar la configuración de las opciones de red de un equipo con la utilización de un servidor DHCP.

Para más información acerca de DHCP se puede consultar el RFC correspondiente [3].

2.4.4. FTP

FTP (File Transfer Protocol) es un protocolo que sirve para compartir archivos a través de la red. Es un protocolo diseñado para que sea utilizado por diferentes programas aunque una gran cantidad de usuarios lo utilizan.

FTP está orientado a ofrecer la máxima velocidad por lo que no tiene una gran seguridad, pero se puede solucionar este problema mediante la utilización de métodos de cifrado.

Para más detalles en cuanto al funcionamiento de FTP se puede consultar su RFC [4].

2.4.5. HTTP

HTTP (HyperText Transfer Protocol) es un protocolo de transferencia de hipertexto en el cual se basa internet. Es un protocolo sin estado, es decir, que no guarda información de las conexiones anteriores, pero se puede tener esta información con el uso de *cookies*.

Para más información sobre HTTP se puede consultar su RFC [6].

2.4.6. HTML

HTML (HyperText Markup Language) es un lenguaje de marcado que se utiliza para crear documentos de hipertexto como páginas web. Se basa en el uso de etiquetas para hacer referencia al contenido de las páginas web, de forma que contiene solo texto. Siendo el navegador web el encargado de interpretar este texto y formar la visualización final de la página web.

Para mayor detalle acerca de HTML se puede consultar su RFC [5].

2.4.7. PHP

PHP (HyperText PreProcessor) es un lenguaje de programación de uso general de código del lado del servidor que fue originalmente desarrollado para la creación de contenido web dinámico. En la actualidad, es un lenguaje muy utilizado, por lo que ha evolucionado para proporcionar nuevas características acordes a los contenidos actuales. Además, también incluye una interfaz de línea de comandos que se puede utilizar para aplicaciones gráficas independientes.

Para más información acerca de PHP se puede consultar su página web oficial [12].

2.4.8. SQL

SQL (Structured Query Language) es un lenguaje declarativo de acceso a base de datos que permite interaccionar con las mismas. A través de diferentes consultas, se pueden realizar un gran número de operaciones con las bases de datos, desde insertar o borrar información a consultar el contenido de alguna tabla ordenándolo por el valor de algún campo y seleccionando únicamente algunos de los datos.

Es un lenguaje que inicialmente fue inicialmente publicando por el ANSI (American National Standards Institute) y confirmada por ISO (International Organization for Standardization) en 1987. Pero que con el paso del tiempo ha evolucionado a través de diferentes ISO.

2.4.9. SMTP

El SMTP (Simple Mail Transfer Protocol) es un protocolo cuya función consiste en enviar correo electrónico de manera fiable y eficiente. Para ello utiliza conexiones sobre TCP/IP (capa aplicación), pero tiene limitaciones en cuanto a la recepción de mensajes en el servidor de destino, por lo que se utiliza en conjunto con otros protocolos.

Para más detalles acerca de SMTP se puede consultar su RFC [16].

2.4.10. POP3

POP3 (Post Office Protocol) es un protocolo que se utiliza para la recepción de correo electrónico. POP3 establece una conexión con el servidor de correo y se descarga el correo del usuario. Esto tiene como ventaja que se puede acceder a esa información aunque no exista conexión con el servidor. Sin embargo, tiene como desventaja que tiene poca movilidad puesto que solo se puede visualizar el correo en ese dispositivo, por lo que se puede optar por dejar una copia del correo en el servidor para que pueda ser descargada desde otros dispositivos.

Para una información más detallada de POP3 se puede consultar su RFC [13].

2.4.11. IMAP

IMAP (Internet Message Access Protocol) es un protocolo que, al igual que POP3, se utiliza para la recepción de correo electrónico. Sin embargo, IMAP no requiere realizar una descarga del contenido, sino que puede visualizar los correos de forma remota. Además, también permite la modificación del buzón de correo como si se trataran de carpetas locales. A causa de estas características, IMAP requiere de conexión con el buzón para consultar el correo y es mucho mas complejo que POP3.

Para más detalles acerca del funcionamiento o características de IMAP se puede consultar su RFC [7].

2.4.12. Samba

Samba es una implementación del protocolo de compartición de archivos de Windows™ SMB. Mediante este servicio, se permite que equipos con sistemas operativos diferentes de Windows™, actúen como clientes de una red Windows™. De esta manera, se permite que se compartan los archivos independientemente del sistema operativo utilizado.

Para más información acerca de Samba se puede acceder a su página web oficial [15] o al libro [22].

2.4.13. CUPS

CUPS (Common Unix Printing System) es un sistema de impresión modular para sistemas Unix™. Mediante CUPS, un equipo que actúa como servidor reciba las peticiones de impresión de otros equipos y las envía a la impresora adecuada. Además, implementa un servicio de cola de impresión y gestión de grupos entre otros aspectos.

Para más información acerca de CUPS se puede acceder a su página web oficial [1].

2.4.14. SSL

SSL (Secure Socket Layer) es un protocolo criptográfico que proporciona autenticación y privacidad en las conexiones entre dos equipos de la red. Inicialmente solo se autenticaba el servidor, pero SSL ha evolucionado en TLS (Transport Layer Security) haciendo que, tanto el cliente como el servidor tengan que autenticarse. Este protocolo permite diferentes algoritmos criptográficos, eligiéndose cual se utilizará en la fase de conexión de los equipos.

Para más información acerca de SSL o de los diferentes algoritmos criptográficos que utiliza se puede consultar su RFC [18].

2.5. Tipos de auditoría

Una auditoría de seguridad consiste en el análisis y estudio de los diferentes elementos que componen una red, para detectar las diferentes vulnerabilidades que puedan existir en estos elementos.

Para realizar estos estudios se requiere de gente con formación en seguridad y que tenga conocimientos acerca de las diferentes herramientas utilizadas para las auditorías. Estas herramientas consisten en programas que realizan diferentes funciones, desde verificar los puertos abiertos en un equipo, hasta encontrar las vulnerabilidades en el mismo.

Existen diferentes formas de realizar una auditoría de seguridad y, por lo tanto, diferentes tipos de estas. Una manera de clasificarlas es según la información que tenga tanto el auditor como los responsables de seguridad de la empresa auditada. A partir de esta clasificación se definen diferentes tipos de auditoría, que son conocidos como: ciego, doble ciego, caja gris, doble caja gris, tándem e inversa. A partir de estos tipos de auditoría se puede dar más importancia a un aspecto de la seguridad o de las aptitudes del auditor [20].

Los tipos de auditoría más utilizados en la actualidad son:

Doble ciego: también conocido como Test de Penetración, este tipo de auditoría permite comprobar la situación a la que se enfrentaría cualquier usuario que pretenda atacar a la empresa. Además, también se pueden estudiar los diferentes métodos de respuesta de el equipo de seguridad de la empresa comprobando si han sido capaces de detectar y bloquear los diferentes ataques realizados en la auditoría.

Caja gris: también conocido como Test de Vulnerabilidades, este tipo de auditoría sirve como un estudio de las vulnerabilidades existentes en el sistema auditado. Por lo tanto, muchas veces las empresas utilizan estos test para un estudio propio acerca de los problemas de seguridad existentes en sus sistemas.

Una vez se ha elegido el tipo de auditoría a realizar se deben de seguir unos procedimientos más específicos para cada uno. Estos procedimientos serán explicados más adelante al detallar la auditoría de seguridad.

II

Diseño e implementación previo de la red empresarial

3

Políticas de diseño y seguridad de la red

La red que se utilizará será una red empresarial en la que se deberán instalar diferentes servicios y medidas de seguridad. Además, también se especificarán otras directivas que tendrán que ser tenidas en cuenta para la creación de la red y sus servicios. Estas políticas son establecidas por la empresa y, por lo tanto, es necesario cumplirlas todas. Este conjunto de políticas que se tendrán en cuenta se pueden agrupar en diferentes grupos, siendo estos los que se muestran a continuación.

3.1. Servicios

La red debe tener capacidad para proveer de los servicios necesarios para la empresa de forma correcta. Estos servicios a proveer son los siguientes:

Servidor de archivos: se proveerá a la red de un servicio de compartición de archivos de acuerdo a las siguientes características:

- **Servidor interno:** se deberá contar con un servido de archivos para la red de la empresa en el que se almacenarán los diferentes archivos de diferentes usuarios o departamentos, de forma que los usuarios necesarios tengan acceso a los mismos. Por lo tanto, en este servidor de archivos se pueden encontrar archivos de gran importancia, por lo que debe ser un servidor de acceso limitado.
- **Servidor para clientes e invitados:** se proveerá de un servidor de archivos al que deben poder acceder los diferentes clientes, así como, los diferentes invitados. En este servidor se almacenarán, también, archivos tales como listas de precios que deben ser accesibles para cualquier usuario de internet. Por lo tanto, en este servidor no se deben limitar los accesos de ninguna manera.

Página web: la red debe poseer su propia página web. Ésta será la utilizada para la propia página de la empresa. En esta página se deberán poder gestionar diferentes usuarios y noticias, por lo que deberá tener asociada una base de datos propia del servidor web.

Servidor de correo: se proveerá de un servicio de correo electrónico. La red debe tener un servidor de correo propio que atienda al correo del propio dominio. En este servidor se almacenarán los diferentes correos de la empresa, pudiendo acceder al mismo desde cualquier parte de internet para que el usuario pueda leer su correo.

Base de datos interna: se debe tener en la red una base de datos. Ésta será utilizada para el funcionamiento de un programa propio de la empresa, por lo que contendrá información sensible. Debido al tipo de información que albergará, el servidor debe tener un acceso restringido y deberá ser confiable.

Servidor Samba: además del servidor de archivos, se debe contar con un servidor Samba. Este servidor se debe incluir para que los diferentes trabajadores puedan almacenar los archivos importantes en un servidor del que se realizarán copias de seguridad periódicamente. Además, este servidor debe permitir su uso en diferentes sistemas operativos para que se pueda utilizar el servicio para intercambiar archivos entre estos.

Servidor de impresión Linux: debido a la forma de trabajo de la empresa, es necesario que se cuente con un

servidor de impresión Linux. Este servidor debe poder utilizarse por todos los trabajadores de la red, de forma que se pueda acceder a las diferentes impresoras del mismo desde todos los puestos de trabajo con el sistema operativo GNU/Linux™.

3.2. Red

Debido a la estructura de la empresa, la red debe cumplir ciertas especificaciones. Éstas existen para que se pueda asegurar que se proveen de servicio a los suficientes puestos de trabajo, así como, a los diferentes clientes que necesiten una conexión. Por lo tanto, a la hora de diseñar tanto la red como sus servicios se deben tener en cuentas las siguientes especificaciones:

- La empresa cuenta con, aproximadamente, 100 puestos de trabajo, pero se debe poder proveer de servicios a un número mayor de equipos de forma que no se deba detener el crecimiento de la red por necesitar una modificación de la misma.
- En los puestos de trabajo se utiliza tanto Windows™ como diferentes distribuciones de GNU/Linux™, siendo el segundo mucho más abundante.
- Se debe proveer acceso a internet a los diferentes servicios públicos a los clientes e invitados que se encuentren en la sede de la empresa. De esta manera, se debe asegurar que cualquier cliente pueda tener acceso a internet en sus diferentes visitas a la sede de la empresa. También es necesario que se provea de acceso a los posibles invitados que existan cuando se realicen los diferentes eventos en la empresa.
- La red debe estar preparada para un aumento en la carga de los servicios significativa, de forma que, en caso de un gran aumento del número de trabajadores, no sea necesario una modificación completa de la red y sus servicios.
- Cuando un equipo se conecte a la red, debe tener acceso a los servicios básicos sin necesidad de realizar configuraciones extras. De esta manera, se permite que tanto los trabajadores como los clientes o invitados puedan conectar sus dispositivos personales para tener acceso a internet sin necesidad de configuraciones complejas, permitiendo un acceso a internet sin necesidad de conocimientos informáticos.
- A fin de poder configurar los diferentes servidores, todos estos deberán ser accesibles desde los puestos de trabajo de la empresa.

3.3. Seguridad

Respecto a la seguridad de la red se deben cumplir también un conjunto de especificaciones. Éstas están orientadas a que se mantenga una gran seguridad en la red mientras se mantienen los diferentes servicios de la misma de forma correcta y sin molestias para el usuario. Además, se deben de proteger los servicios con información sensible, así como, proteger las transferencias de esa información entre los diferentes equipos. Por lo tanto, se deben de tener en cuenta las siguientes especificaciones:

- Algunos de los servicios solo deben de ser accesibles desde los puestos de trabajo de la empresa. Esta medida se debe a que es necesario limitar el acceso a los servicios por usuarios indeseados o desde equipos no controlados fuera del entorno de trabajo. Por lo tanto, los servicios seleccionados solo podrán ser accesibles desde los puestos de trabajo de la empresa. Estos son:
  - Servidor de archivos interno: debido a que puede contener archivos con información sensible solo se permitirá su acceso desde los puestos de trabajo de la red.
  - Base de datos interna: debido a que todos los puestos de trabajo guardarán información de su actividad en esta base de datos se debe mantener segura. Por lo tanto, solo se permitirá el acceso a la base de datos desde los puestos de trabajo de la empresa, limitando los accesos indeseables.

  - Servidor Samba: al igual que con el servidor de archivos, el servidor Samba puede contener información sensible. De esta manera, también se limitará el acceso al mismo, permitiéndolo únicamente desde los puestos de trabajo de la empresa.
  - Servidor de impresión Linux: debido a que el acceso a las impresoras está limitado a los trabajadores de la empresa es innecesario que se pueda acceder al servidor de impresión desde fuera de la red empresarial. Por lo tanto, el servidor de impresión también contará con acceso restringido al mismo.

- Debido a la información sensible que se puede transmitir entre los diferentes equipos y los servidores, todas las conexiones de los servicios anteriormente citados deberán estar protegidas. Esta medida se debe a la necesidad de proteger la información para evitar que sea capturada por usuarios indeseados.
- El acceso a la red empresarial en los diferentes puestos de trabajo sera limitado permitiendo únicamente los servicios de internet. De esta manera se pretende mantener los puestos de trabajo aislados del resto de internet tratando de mantenerlos seguros. Por lo tanto, los puestos de trabajo solo tendrán acceso a internet y el resto de conexiones desde o hacia los puestos de trabajo desde internet será bloqueado.
- Por el contrario, los diferentes clientes e invitados, así como, los servicios públicos de la red no tendrán limitado el acceso ni las conexiones con internet. Por lo tanto, tendrán una mayor libertad de actuación, pero a su vez, tienen una menor seguridad, dejando las medidas de seguridad en manos del propietario del dispositivo que se conecte a la red.

Los diferentes servicios públicos nombrados anteriormente serán aquellos servicios a los que se deba poder acceder desde cualquier punto de internet y que, por lo tanto, son más vulnerables. Estos servicios son:

Servidor de archivos para clientes e invitados: como este servidor contendrá archivos que deben ser accedidos por cualquier usuario de internet, como archivos de precios, debe poder ser accedido desde cualquier punto de internet.

Página web: debido a que será la página web propia de la empresa es necesario que se pueda acceder de forma anónima desde cualquier punto de la red.

Servidor de correo: a consecuencia de que este servidor contendrá los correos de todos los empleados, es necesario que estos puedan tener acceso al correo electrónico desde cualquier lugar, por lo que se debe poder acceder al servidor desde cualquier punto de internet.

4

Diseño e implementación de la red

Una vez establecida la política que debe seguir la red, así como los servicios que debe proporcionar, se debe realizar el diseño de la red final. Para el diseño de esta red se deben tener en cuenta diferentes factores entre los que están el número de equipos a los que la red debe dar servicio y las diferentes medidas de seguridad que debe tener la misma [26], así como, las políticas establecidas anteriormente.

4.1. Estructura de la red

El primer aspecto que se tendrá en cuenta es la política de diseño, que establece que algunos servicios son de acceso único para los equipos de los trabajadores, mientras que a otros servicios se debe poder acceder desde cualquier parte de la red como la página web.

De esta manera, se decide crear dos zonas diferenciadas en la red para poder aislar estos servicios. Esta decisión se toma debido a que en caso de estar todos los servicios y equipos en una misma red es más complicado mantener un acceso seguro, ya que, a pesar de los diferentes métodos de autenticación, los servicios de acceso único se volverían más vulnerables al poder acceder a ellos desde partes públicas de la red.

Por lo tanto, se decide crear dos redes conectadas entre sí y a su vez conectadas a internet. A estas redes se las denominará: zona privada y zona pública. Así, la zona privada será la que contenga los servicios a los cuales solo se debe acceder desde los equipos de la empresa; y, la zona pública, aquella en la que se encontrarán los servicios a los que se podrá acceder desde toda la red.

4.2. Tamaño de la red

El siguiente aspecto que se tiene en cuenta para el diseño de la red es el tamaño que tendrán ambas subredes nombradas anteriormente.

Este es un aspecto muy importante a tener en cuenta, ya que es uno de los costes que la empresa tendrá que asumir y, en caso de utilizar una red demasiado pequeña con el fin de disminuir el coste, no se podrá aumentar el tamaño de la red de forma simple, sino que se tendrá que realizar una nueva configuración de todos los servicios para que funcionen correctamente, incumpliéndose las políticas establecidas.

El tamaño de la red se establece a través de la máscara de red. Ésta es un parámetro de las redes que indica cuantos bits de la dirección IP de un equipo indican la red y cuantos bits indican la dirección del propio equipo.

Para la elección del tamaño de ambas redes se deben tener en cuenta varios aspectos. Como ya se ha especificado, el primer aspecto a tener en cuenta es el coste, este parámetro hará que se elija el menor tamaño de red que cumpla todas las características, ya que, el precio de la red aumenta con el tamaño de la misma.

El siguiente aspecto a tener en cuenta es el número de equipos que contiene la red. En este caso, se ha seleccionado un tamaño de red de 256 equipos por red, es decir, una red de clase C. Se ha seleccionado este tipo de red debido a que es la red que más se utiliza y, además, es una red con capacidad para 255 equipos lo que es suficiente para cumplir con la política especificada.

Existen diferentes formas de indicar la máscara de red, una de ellas es, como ya se ha especificado, diciendo que se usará una máscara de clase C. Otras formas de especificar que se trata de esta máscara de red son: /24 o *255.255.255.0*. En el primer caso se indica el número de bits que corresponden a la especificación de la red, y en el segundo caso se indica, con bits a 1, los bits que especifican la red.

4.3. Interconexión de las redes

También, se debe elegir la manera de interconectar ambas redes y la forma de conectar ambas con internet. En este caso se ha decidido conectar la red privada directamente a internet a través de un *router*. Se ha tomado esta decisión debido a que hay un interés en que la red privada tenga velocidades de transmisión mayores que la red pública.

Por tanto, al conectar la red privada directamente con internet se evita que la información tenga que atravesar la red pública. Además, también se tienen en cuenta cuestiones de seguridad acerca de la posible interceptación del tráfico que atraviesa una red, pero este aspecto será explicado más ampliamente en el diseño de la seguridad de la red. De esta manera, se tendría conectada la red privada de la empresa directamente a internet a través de un *router* en el que se colocarán diferentes medidas de seguridad.

Posteriormente, se conectarán ambas redes entre si mediante un *router*. Este será el encargado de transmitir la información entre ambas redes, así como, de encaminar el tráfico de la red pública a través del *router* de la red privada hacia internet y viceversa. Esta conexión se debe realizar debido a que si no existiera la red pública estaría completamente aislada. Al añadir la conexión con la red privada se permite que ambas redes se comuniquen, aspecto necesario establecido por la política de diseño de la red que especifica que la página web, cuyo servidor se localizará en la red pública, debe poder ser configurada desde la zona privada de la red.

Además, es necesario añadir el encaminamiento hacia internet y viceversa porque si no se estableciera esta conexión, los servicios de la red pública no podrían ser accedidos y, por lo tanto, servicios como la página web quedarían aislados de internet eliminando su funcionalidad. El esquema de red resultante sería el que se puede observar en la figura 4.1.

Figura 4.1: Esquema de red inicial. Se muestran las dos zonas que conformarán la red empresarial junto con las conexiones entra las mismas y con internet.

4.4. Selección de direcciones IP

Para seleccionar todas las características de las diferentes redes se tienen que especificar cuales son las direcciones IP que utilizarán.

Estas direcciones IP normalmente las facilita el proveedor de servicios de internet cuando se solicitan las redes que se quieren usar. Esto es así porque la dirección IP consiste en una dirección única en todo internet que identifica a cada equipo y, por tanto, deben usarse unas direcciones que el proveedor de servicios de internet reserve para el uso de la empresa.

En este caso se ha decidido utilizar las direcciones *192.168.1.0/24* para la red privada y *192.168.2.0/24* para la red pública. Estas direcciones IP son direcciones locales, esto se debe a que se realiza una simulación de la red. Sin embargo, se utilizarán estas direcciones a modo de direcciones de internet para la realización del presente documento.

Se debe tener en cuenta que a la hora de indicar las direcciones de cada red se indica también la máscara de red de la misma ya que con esta combinación se puede determinar cuales son todas las direcciones IP que pertenecen a cada red. La elección de estas direcciones ha sido debido a que el bloque de direcciones de *192.168.0.0/16* está reservado para el uso privado relativo a redes, por lo que no se interferirá con ninguna otra dirección a la que se pueda querer acceder desde los equipos de la red.

4.5. Diseño final de red

Finalmente, se contaría con dos redes separadas: zona privada y zona pública. De estas dos redes, la red de la zona privada estaría conectada a internet a través de un *router*. La red de la zona pública estaría conectada a la zona privada a través de otro *router*. Este será el encargado de encaminar la información de forma correcta entre la zona pública e internet. Las redes de la zona privada y pública serán dos redes de clase C con las IP *192.168.1.0/24* y *192.168.2.0/24*, respectivamente. Este diseño se puede observar en la figura 4.2.

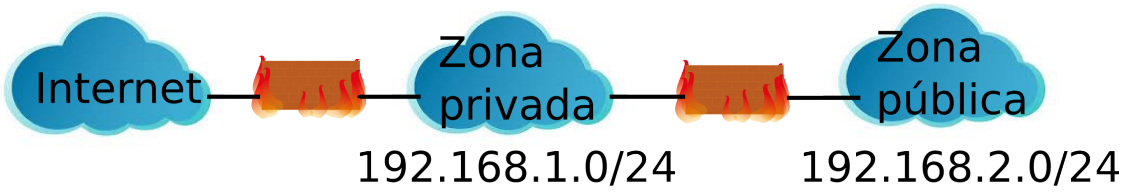

Figura 4.2: Estructura final de la red con la asignación IP. Se pueden observar las dos zonas de red interconectadas entre sí y a internet.

4.6. Implantación de la red

Una vez que se tiene el diseño completo de la red se debe comenzar su implementación.

4.6.1. Selección de configuración

Evidentemente es necesario configurar correctamente los equipos de la red. Para ello, en esta red, la configuración se puede realizar de dos formas: configuración estática de direcciones IP y configuración mediante un

servidor DHCP.

Dirección IP estática

La configuración estática de direcciones IP consiste en la configuración manual de todos los equipos una vez conectados a la red. De esta manera, cada equipo tendría siempre la misma IP y la misma configuración de red (puerta de enlace, máscara de red, servidores de nombre). Esta configuración permite que cada equipo quede completamente asociado a una misma dirección IP que lo identifica en todo momento en la red, sin embargo, si se requiere realizar tanto un cambio en la configuración de la red, como un cambio de los servidores de nombres, habría que realizar un cambio manual en todos los equipos. Esto conllevaría un gran tiempo en el que la red no funcionaría correctamente por no poder resolver los diferentes nombres que se utilicen.

Utilización de DHCP

La otra configuración más utilizada es la configuración de la red a través de un servidor DHCP. Éste es un servidor que a través del protocolo DHCP se encarga tanto de proporcionar direcciones IP a los nuevos equipos que están en la red, como de renovar las IP de los equipos ya conectados. Con la utilización de este servidor se automatiza la configuración de la red de los diferentes equipos que conectan a la misma, ya que el propio servidor DHCP es el encargado de proporcionar tanto la dirección IP como el resto de configuraciones de la red. De esta manera, al automatizar el proceso de configuración de la red, si se quisiera realizar un cambio en la configuración de toda la red, solo habría que cambiar la configuración del servidor DHCP para que éste, automáticamente, cambiara las configuraciones de los diferentes equipos conectados a su red. Además, también es posible transmitir tablas de rutas, de forma que se pueden cambiar las tablas de rutas de todos los clientes modificando únicamente el servidor.

Sin embargo, debido a que el servidor DHCP proporciona direcciones IP de manera automática se podría plantear un problema, puesto que los equipos no tendrían por qué tener siempre la misma dirección y no estarían completamente identificados con una dirección IP a lo largo del tiempo, lo que haría que no se pudiera conectar con los mismos sin comprobar su dirección IP previamente. No obstante, los servidores DHCP cuentan con dos tipos de configuraciones básicas que se pueden establecer de forma simultánea para solucionar este problema.

La primera configuración consiste en establecer la dirección IP que le debe proporcionar a un equipo indicando la dirección física del mismo, es decir, cada equipo quedaría completamente identificado con una dirección IP. Sin embargo, con la utilización de este sistema la configuración correcta de la red se puede volver muy tediosa, ya que todos los equipos de la red deberían tener su entrada en el archivo de configuración de servidor DHCP.

La otra configuración posible del servidor DHCP consiste en establecer un rango de direcciones IP, las cuales el servidor DHCP automáticamente proporciona a los equipos que conectan a la red independientemente de su dirección física. Con este método, la configuración del servidor DHCP es muy simple, ya que solo habría que configurar un rango de direcciones IP lo suficientemente grande como para que todos los equipos de la red puedan tener una dirección IP y finalizaría la configuración. Sin embargo, con esta configuración los diferentes equipos obtendrían direcciones IP establecidas por el servidor DHCP, por lo que, estas podrían cambiar. A pesar de que el servidor guarda una pequeña memoria cache para asignar siempre la misma dirección IP al mismo equipo y direcciones IP nuevas a los nuevos equipos en la red, no es posible asegurar que cada equipo obtenga siempre la misma dirección IP, lo que produciría un problema debido a que los servidores no tendrían direcciones IP fijas y, por lo tanto, no se podrían acceder a ellos correctamente.

Configuración utilizada

No obstante, el servidor DHCP permite una configuración mixta, es decir, se pueden utilizar ambas configuraciones de forma simultánea. De esta manera, se configurarán los diferentes servidores para que mantengan una dirección IP fija a través de su dirección física, y posteriormente se utilizará un rango de direcciones IP para

el resto de los equipos, los cuales pueden cambiar su dirección IP sin presentar ningún problema.

Por tanto, en la red empresarial se utilizará el rango de direcciones 1-99 para los diferentes *router* y servidores, el rango 100-200 para proporcionar direcciones IP a los diferentes equipos, y se reservará el rango 201-254 para posibles usos futuros. En caso de que el rango 100-200 de direcciones IP fuera insuficiente este se podría aumentar de forma simple. Únicamente se debería cambiar la configuración en el servidor DHCP teniendo en cuenta previamente que no se podrá asignar ninguna dirección de ese rango de forma fija, por lo que los servidores que estuvieran en el nuevo rango deberían cambiar su dirección IP.

5 Diseño e implementación de la seguridad

Una vez que se ha establecido la estructura de la red y los servicios que va a contener la misma, se debe especificar la seguridad que se va a establecer en la misma. La seguridad de la red abarca diferentes aspectos, desde la configuración del *firewall* hasta la política de establecimiento de contraseñas.

5.1. Diseño de red seguro

El primer aspecto que se va a tener en cuenta en la seguridad es el ya comentado en el diseño de la red. Este aspecto explica el por qué se conecta la zona privada a internet directamente en vez de conectar la zona pública.

La razón de conectar las redes de esta manera se debe a que es necesario evitar que todo el tráfico de la red privada atraviese la red pública. Esto se debe a que si alguien consigue acceso a la zona pública, que como su propio nombre indica sería muy fácil, podría utilizar programas para capturar todo el tráfico que hay en la red, lo que en caso de no ir cifrado le proporcionaría información directa de la acción que quiere realizar el usuario de la zona interna. En caso de utilizar algún método para cifrar la información esta tarea se volvería mucho más difícil o incluso imposible, dependiendo del cifrado que se utilice y de la contraseña utilizada. Por tanto, si conectáramos las redes de forma inversa todo el tráfico de la red privada pasaría a través del *router* de la propia red hacia el *router* de la red pública, por lo que atravesaría la red posibilitando que un usuario conectado a la red pública capturara su tráfico.

Para establecer esta medida de seguridad se eligió, en la fase de diseño de la red, la configuración adecuada para evitar los problemas aquí explicados y, por lo tanto, se evitaría el problema de usuarios capturando el tráfico de la red. Sin embargo, es imposible evitar que el tráfico de la red pública sea capturado por un usuario conectado a la red, y en caso del tráfico de la red pública podría capturarse tanto por un usuario conectado a la red pública como a la red privada. Sin embargo, debido a que el tráfico de la red pública no contiene tanta información sensible es un aspecto menos peligroso. Por otro lado, es imposible evitar que un usuario capture el tráfico de su propia red por lo que evitar que se capture el tráfico de la red privada por un usuario de la misma es imposible, sin embargo, al limitar el acceso a esta red solo podrían capturar el tráfico los propios empleados de la empresa, disminuyendo de esta manera el riesgo.

Por lo tanto, la configuración utilizada es la ya comentada anteriormente de utilizar dos zonas de red: zona privada y zona pública. Posteriormente, se conecta la zona privada directamente a internet, también se conecta la zona pública a la zona privada para que tenga acceso a internet a través de la misma.

5.2. Política de contraseñas

Otro aspecto a tener en cuenta es la política de creación de contraseñas que se utilice. La política de creación de contraseñas es la encargada de establecer como deben ser las contraseñas, es decir, cual debe ser su longitud, si debe tener números o caracteres especiales, si tiene una caducidad, si se pueden repetir contraseñas anteriores, etc. Esta política es muy importante, ya que, un gran problema de seguridad es el uso de contraseñas muy simples o de poca longitud, puesto que estas contraseñas permiten hacer ataques por fuerza bruta con bastante eficacia. Un ataque por fuerza bruta consiste en probar contraseñas de un diccionario, donde se encuentra un gran número de contraseñas, intentando averiguar la contraseña probando cada vez una hasta que acierta.

En la red se han mantenido las políticas por defecto que, en el caso de cuentas de usuario de Ubuntu™, consiste en contraseñas de 6 caracteres. Se ha decidido mantener la política por defecto debido a que se crearán diferentes usuarios en los que se probarán diferentes contraseñas, desde contraseñas muy cortas y simples a contraseñas largas en las que se mezclan letras, números y caracteres especiales sin un sentido aparente.

Debido a que se ha elegido mantener las políticas de contraseñas por defecto no es necesario realizar ningún cambio en la configuración de la misma. Sin embargo, si se quisiera cambiar las políticas de las contraseñas habría que cambiar los archivos de configuración.

Puesto que la mayoría de servicios utilizan las cuentas del propio sistema operativo Ubuntu™, en la mayoría de los casos se tendría que modificar el archivo de políticas de contraseñas del propio sistema. En este archivo se pueden configurar diferentes aspectos, desde la longitud de la contraseña y los tipos de caracteres que se deben usar, hasta el número de intentos que se tiene para introducir la contraseña correcta. La ruta a este archivo se encuentra en el cuadro 5.1.

```
/etc/pam.d/common-password
```

Cuadro 5.1: Ruta al archivo de políticas de contraseñas de Ubuntu™.

5.3. Utilización de cifrados

En la seguridad de la red también es muy importante el cifrado que se utiliza. El proceso de cifrado consiste en modificar la información mediante un algoritmo que requiere de una clave, de esta manera la información puede enviarse por la red sin que se pueda observar la información enviada en texto plano, es decir, sin codificar. Este proceso es muy importante, ya que, en caso de que en la red hubiera un usuario capaz de capturar el tráfico de la red éste sería capaz de observar toda la información que se transfiere, y si, por ejemplo, está transfiriendo un archivo al servidor FTP, el usuario que esté escuchando la información podría conseguir este mismo archivo que podría contener información sensible.

Por consiguiente, se utilizarán conexiones cifradas, mediante SSL, en todos los servicios de la zona privada, sin embargo, para los servicios de la zona libre se podrá utilizar tanto conexiones cifradas como conexiones sin cifrar. Esta elección se debe a que en la zona privada se debe mantener una seguridad muy elevada pues se está tratando con información sensible de la empresa,además, en esta zona solo se podrán conectar empleados, por lo que se les podrá exigir que utilicen conexiones cifradas. Por otro lado, en la zona pública se encontrarán servicios que podrán utilizar usuarios que no pertenecen a la empresa y, por lo tanto, no se les puede exigir que mantengan conexiones cifradas. Sin embargo, en los servicios de la zona pública también se pueden utilizar conexiones cifradas para aquellos usuarios que quieran aumentar la seguridad de las conexiones.

5.4. Utilización firewall

5.4.1. Características

Adicionalmente, en la política de la seguridad hay que tener en cuenta la utilización de un *firewall*. Éste es un software que analiza algunos datos de los paquetes que atraviesan el equipo donde está instalado y, a partir de un conjunto de políticas y normas, decide que acción tomar con paquete, si dejarlo pasar o eliminarlo entre otras acciones. De esta manera, si se configura correctamente el *firewall* se podrá controlar el acceso a la red de forma eficiente, ya que se podría rechazar todo el tráfico en función de su origen o destino, así como de su puerto de origen y puerto de destino.

La utilización de este software es muy útil debido a que si no se utilizara ningún *firewall* toda la red quedaría expuesta a conexiones externas puesto que el *router* no filtra ninguna información y, por lo tanto, cualquier usuario podría conectar con un equipo de nuestra red interna a la que no se debe tener acceso desde el exterior.

En este caso se ha decidido utilizar un *firewall* en el *router* de conexión con internet, de esta manera todas las conexiones, tanto entrantes como salientes, con internet lo atravesarán y podrán ser controladas por el mismo. Además, al introducir el *firewall* en este punto también se pueden tomar las decisiones de acción respecto al tráfico que lo cruce en función de la zona de destino de nuestra red, ya que al tratarse de diferentes subredes diferentes es muy fácil saber cual es su destino.

Además de este *firewall* también se utilizará otro en el equipo que actuará de *router* entre ambas partes de la red empresarial, para, de esta manera, poder proteger ambas zonas correctamente.

Se ha decidido utilizar el *firewall* de iptables debido a que es el más utilizado en `GNU/Linux`™ y es un software instalado de manera predefinida en todas las distribuciones de `Ubuntu`™, por lo que no será necesario instalar software adicional.

5.4.2. Funcionamiento firewall

Una vez se ha instalado el *firewall*, en el *router* se debe llevar a cabo su configuración. Cuando un paquete de información le llega al *firewall*, éste atraviesa un conjunto de tablas de normas en función del destino que tenga, en este caso solo se utilizarán tres de esas tablas: INPUT, OUTPUT y FORWARD. Solo se configurarán estas tablas por ser las más utilizadas y porque si están correctamente configuradas se puede implementar una gran seguridad únicamente con estas tablas. El flujo de paquetes a través de las diferentes tablas se pueden observar en la imagen 5.1.

En función del destino del paquete que atraviesa el *firewall*, éste atravesará una tabla diferente de INPUT, OUTPUT o FORWARD. Si el paquete tiene como destino el equipo del *firewall* o sale del mismo atraviesa las tablas de INPUT y OUTPUT respectivamente. Por otro lado, si el paquete atraviesa el *firewall* debido a un redireccionamiento, es decir, que atraviesa el *firewall* porque es un paquete de una comunicación entre internet y la red de la empresa, el paquete atraviesa la tabla de FORWARD. De esta manera, la configuración de las tablas INPUT y OUTPUT serán las que establecerán el acceso al propio *firewall*, mientras que la tabla de FORWARD será la que establezca las normas de acceso a la red de la empresa.

Dentro de cada una de estas tablas se establece una política y un conjunto de normas. Con cada paquete que entra en una tabla se va comprobando las diferentes normas en las que se encuentran diferentes filtros en función de las características de los paquetes (destino, origen, puerto de destino,etc.). En caso de que el paquete cumpla todas las características de una norma se realiza la acción que marque esa norma, ya sea aceptar el paquete o eliminarlo entre otras. En caso de que el paquete no cumpla ninguna de las reglas se tiene en cuenta la política de la tabla, esta política establece que se debe hacer con los paquetes que no cumplan ninguna regla estableciendo si se deben aceptar o eliminar entre otras posibles acciones. De esta manera, a través de las diferentes normas y políticas se pueden tomar decisiones de las acciones a tomar con cada tráfico en función de

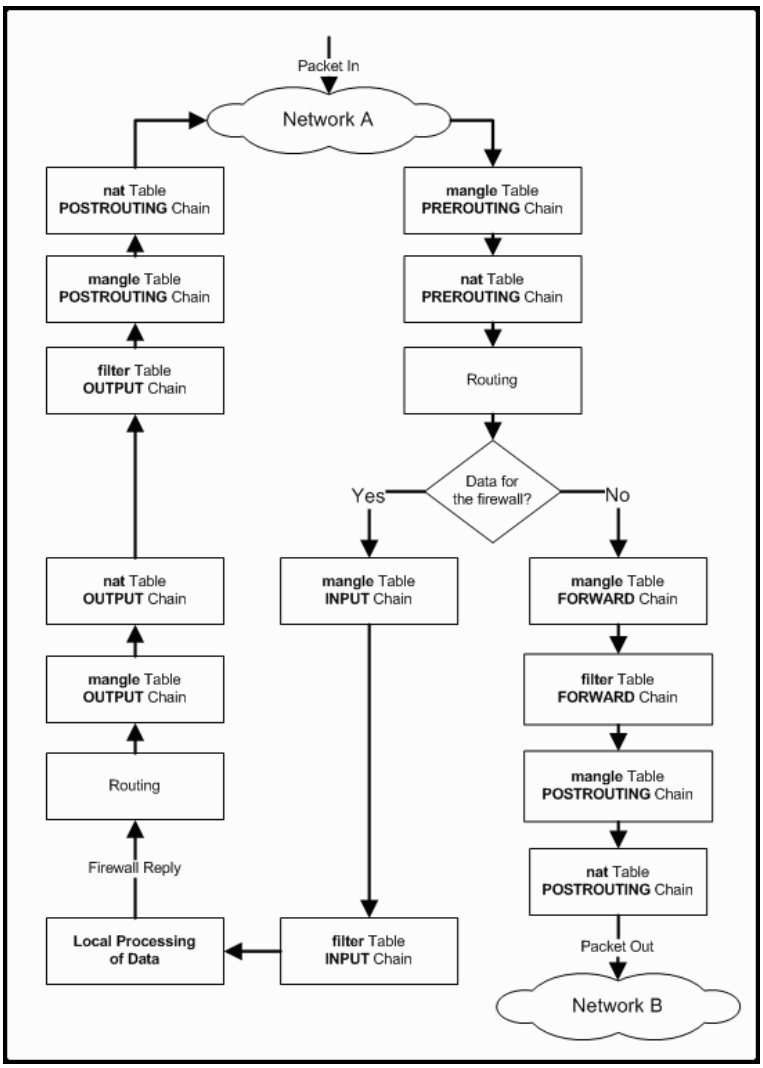

Figura 5.1: Funcionamiento de las tablas de iptables. Se muestra el flujo que siguen los diferentes paquetes al atravesar el *firewall* en función del origen y el destino de los mismos.

sus características, pudiendo, por ejemplo, eliminar paquetes dirigidos a una red concreta o redireccionando los paquetes con destino a una red concreta.

5.4.3. Configuración firewall

La configuración en el *firewall* que se utilizará en el *router* de conexión a internet será la siguiente:

- Políticas de las tablas:
  - Tabla INPUT: DROP.
  - Tabla OUTPUT: DROP.
  - Resto de tablas: ACCEPT.
- Se permite el tráfico en INPUT desde localhost.
- Se permite el tráfico en INPUT desde la red privada de la empresa.
- Se permite el tráfico FORWARD, es decir, redirección en las siguientes condiciones:
  - Con destino a la red interna y el puerto 80, 8080 y 443: para permitir conexiones a internet.
  - Con destino a la red interna y el puerto 53: para permitir el tráfico DNS.
  - Tráfico con destino a la red pública de la empresa para todos los puertos: cumpliendo la política de la empresa de no proteger la zona pública de la empresa.
- Se bloquea el resto del tráfico FORWARD con destino a la red interna, tanto desde internet como desde la red para invitados.
- Se enmascara el tráfico FORWARD saliente de la red hacia internet.

Además de esta configuración, también se deben de añadir las configuraciones de los cuadros 5.2 y 5.3 para permitir el redireccionamiento de paquetes y que el equipo tenga la ruta correcta para encaminar la red pública.

```
echo 1 >/proc/sys/net/ipv4/ip_forward
```

Cuadro 5.2: Comando para permitir redireccionamiento. Mediante este comando se permite que el equipo redireccione los paquetes que recibe, por lo que puede ser utilizado como *router*.

```
route add -net 192.168.2.0/24 gw 192.168.1.25 dev eth1
```

Cuadro 5.3: Comando para crear la ruta a la red pública. Con este comando se le indica al equipo que todos los paquetes que tengan como destino la red *192.168.2.0/24* deben dirigirse al equipo *192.168.1.25*, el cual es el *router* de enlace entre ambas redes.

Por otro lado, también se debe configurar el *firewall* que se establecerá entre ambas redes de la empresa, este *firewall* tendrá la siguiente configuración:

- Políticas de las tablas:
  - Tabla INPUT: DROP.
  - Tabla OUTPUT: DROP.

    - Resto de tablas: ACCEPT.
- Se permite el tráfico en INPUT desde localhost.
- Se permite el tráfico en INPUT desde la red privada de la empresa.
- Se bloquea el tráfico FORWARD con destino a la red interna.
- Se enmascara el tráfico FORWARD saliente de la red hacia la red privada y entrante desde la misma.

Además de esta configuración, también es necesario permitir el redireccionamiento de paquetes con el comando anteriormente utilizado del cuadro 5.2.

Para más detalles acerca del uso de *firewall* y su configuración se pueden consultar los libros correspondientes [29, 33].

6

Diseño e implementación de los servicios

Una vez que se ha diseñado la estructura completa de la red y su completa configuración se debe proceder a señalar los diferentes servidores que se utilizarán y sus configuraciones. Además, también se debe especificar en que equipos se instalarán los diferentes servicios, de forma que quedaría finalizada la estructura de la red completa con todos los servicios adjudicados a diferentes máquinas. Por lo tanto, se tendrán que elegir los diferentes servidores que se utilizarán, debido a que para cada servicio se cuenta de un amplio abanico de servidores que pueden proporcionarlo.

A continuación se expondrán los diferentes servidores utilizados, así como las configuraciones utilizadas. Sin embargo, si se requiere mas información acerca de como configurar los diferentes servicios o acerca de su instalación, se puede consultar el apéndice A.

6.1. Elección de sistema operativo

La primera selección que se debe hacer es el sistema operativo que se utilizará en los servidores ya que hay diversos sistemas operativos disponibles a tal fin.

En la actualidad existen numerosos sistemas operativos diferentes, pero se pueden destacar por su difusión tres sistemas operativos. Éstos son:

Windows™: es uno de los sistemas operativos más utilizados en la actualidad, pero la mayoría de sus servidores son de pago y es un sistema operativo que consume muchos recursos. Además, para los servidores gratuitos en muchos casos es difícil mantenerlos actualizados, puesto que se depende de una revisión manual de las diferentes páginas de estos servidores en busca de actualizaciones en caso de que no exista una comprobación por parte del propio servidor.

GNU/Linux™: es el sistema operativo utilizado en servidores por la mayoría de administradores y personal de seguridad debido a su fácil configuración. Además, proporciona un gran número de servicios a través de proyectos de *Open Source* que se ofrecen de forma gratuita a través de sus librerías de descargas. Adicionalmente, la actualización de sus servidores resulta muy sencilla, ya que al tratarse de paquetes de librerías, solo es necesario comprobar las librerías para actualizar todos los programas y servicios del equipo, al tiempo que se actualiza el propio sistema operativo.

Mac OS X™: siendo el sistema operativo de Apple™ es poco utilizado fuera de sus propios ordenadores. Este sistema operativo cuenta con servicios propios que pueden llegar a tener problemas de compatibilidad con otros sistemas operativos. Este sistema no se tendrá en cuenta, ya que en la empresa no se utiliza este sistema operativo, por lo que podría causar problemas de compatibilidad innecesarios.

Para esta empresa se ha decidido utilizar el sistema operativo de Ubuntu™ basado en GNU/Linux™ para instalar los diferentes servidores. Esta decisión se debe a que es un sistema operativo en el que se dispone de un gran número de servicios gratuitos de *Open Source* que nos permiten proporcionar los servicios requeridos por la

empresa sin necesidad de invertir en el pago de licencias. Además, es un sistema operativo en el que la mayoría de estos proyectos están en continuo desarrollo de forma que si se mantiene una buena política de actualización, la mayoría de los problemas de seguridad son corregidos en un corto espacio de tiempo permitiendo mantener los servicios de manera segura. La elección de Ubuntu™, dentro de las opciones de los sistemas operativos GNU/Linux™, se debe a que se trata de una de las distribuciones más utilizadas, por lo que, será más posible que los diferentes administradores conozcan el sistema operativo y su funcionamiento.

6.2. Servidor de archivos

6.2.1. Selección de servidor

En el capítulo 3.1 se especificó que se requerían dos servidores de archivos, pero no se especificó que tipo de servidores. Dentro de las diferentes posibilidades se ha decidido utilizar servidores de FTP. Se ha seleccionado este tipo de servidores debido a su uso muy común y que permite una conexión desde diferentes sistemas operativos. Además, es un servicio muy extendido, por lo que para el servidor para clientes e invitados es una buena lección para que los diferentes usuarios de internet puedan acceder al mismo.

Una vez se ha seleccionado que se utilizará un servidor FTP se debe seleccionar cual es el servidor concreto que se utilizará, ya que las librerías de Ubuntu™ ofrecen numerosas opciones. En este caso se ha optado por utilizar ProFTPD™.

La elección de este servidor se debe a que se trata de un servidor gratuito muy utilizado. Además, ProFTPD™ cuenta con un gran número de módulos que le permiten expandirse y fusionar sus servicios con otros servicios diferentes. Esta característica hace que, en caso de que en la red se instale servicios de cuentas de usuarios, como LDAP (Lightweight Directory Access Protocol) o Directorio Activo, el servidor ProFTPD™ solo tendrá que configurar sus módulos para seguir funcionando correctamente sin necesidad de realizar grandes cambios. De esta manera, se tiene en cuenta la política de en caso de gran crecimiento de la red no sea necesario modificarla, ya que servicios como LDAP o *Directorio Activo* son servicios típicos de redes grandes para facilitar el control de cuentas de usuario y permisos.

Para la instalación de ProFTPD™ se utilizarán las librerías oficiales de Ubuntu™, de esta manera, se asegura que se trata de software oficial y se podrá actualizar de manera sencilla.

6.2.2. Configuración del servidor

Una vez se ha seleccionado el servidor ProFTPD™ se debe especificar su configuración. Debido a la existencia de dos servidores con características muy diferenciadas se deberán configurar también de manera diferente.

Servidor interno

En el caso del servidor interno se necesita un servidor con acceso limitado a usuarios de la empresa en el que se mantenga seguridad en las transacciones. Por lo tanto, se ha decidido utilizar las siguientes configuraciones:

- Utilización de cifrado SSL: como es necesario mantener las conexiones protegidas se ha decidido utilizar un cifrado SSL para conectar con el servidor de forma imprescindible.
- No permitir usuarios anónimos: debido a que en este servidor se guardará información sensible, no se permitirán este tipo de usuarios.
- Los usuarios solo podrán consultar sus archivos o aquellos a los que se les permita acceso a través de permisos de grupo.

Servidor externo

En el caso del servidor de archivos externos se cuenta con unas características diferentes. Se trata de un servidor de acceso público en el que se guardarán archivos a los que deben de tener acceso todos los usuarios. Por lo tanto, tendrá las siguientes configuraciones:

- Se permitirán usuarios anónimos: debido a que todos los usuarios de internet deben de tener acceso al servidor, es necesario que se establezca un usuario anónimo para todos estos.
- Se creará una zona para compartir archivos pública: como existirán archivos a los que todos los usuarios deben tener acceso, se debe crear una zona en la que se guarden todos estos archivos de acceso público.
- Se permitirán conexiones sin cifrar: a causa de ser un servidor público no se puede exigir conexiones cifradas, ya que se estableció en la política que este servidor no debe limitar el acceso. Por lo tanto, se permitirán tanto conexiones cifradas mediante SSL como conexiones sin cifrar, dejando en el usuario la decisión acerca de la seguridad de su conexión.

6.3. Página web

6.3.1. Selección de servidor

Para proveer de una página web acorde con las políticas especificadas por la empresa, se debe contar con una página que conecte con una base de datos para gestionar, tanto su contenido como sus usuarios. Por lo tanto, se debe elegir una plataforma que incluya estas características.

De entre las diferentes opciones existentes se ha decidido utilizar Joomla™. Esta decisión está motivada por el fácil uso de Joomla™, así como, por el cumplimiento de todos los requisitos, es decir, que cuenta con bastante seguridad y una base de datos para controlar el contenido de la página web.

Joomla™ es un sistema de gestión de contenidos que permite desarrollar páginas web dinámicas e interactivas. Para ello necesita de diversos componentes para crear y gestionar correctamente estos contenidos. Los componentes que Joomla™ necesita son:

Servidor Apache™: como se quiere albergar una página web es necesario de un servidor web que provea este servicio. Por lo tanto, para el uso de Joomla™ será necesario contar con un servidor Apache™.

PHP: debido a que Joomla™ crea páginas web en código php, será necesario que el servidor soporte este tipo de lenguaje, para ello se debe instalar PHP.

Base de datos MySQL: puesto que se requiere una gestión de contenidos y usuarios, Joomla™ debe tener acceso a una base de datos. Para la base de datos se instalará MySQL, esta elección se debe a que es la base de datos que Joomla™ especifica que se debe usar para su funcionamiento.

Para la instalación de los diferentes componentes se utilizarán los paquetes de las librerías oficiales de Ubuntu™, ya que de esta manera se asegura que no se trata de software maligno, y además, se podrá utilizar una política de actualización muy simple.

Una vez se tienen instalados los diferentes componentes necesarios para Joomla™, se descarga este a través de su página web oficial indicada en el cuadro 6.1.

http://www.joomla.org/

Cuadro 6.1: Página oficial de Joomla™.

6.3.2. Configuración del servidor

En la configuración del servicio de la página web se pueden diferenciar las configuraciones de los diferentes servicios instalados necesarios para que Joomla™ funcione correctamente, así como, la propia configuración de Joomla™.

6.3.3. Configuración Apache

Para el servidor Apache™ se utilizará una configuración por defecto, ya que, únicamente se utilizará para albergar la página web. Por lo que, se considera que la configuración por defecto conlleva suficiente seguridad.

6.3.4. Configuración PHP

Como el servicio de PHP se debe instalar únicamente para que el equipo sea capaz de ejecutar este tipo de código, no será necesario configurarlo de ninguna manera específica. Por lo que, únicamente se instalara sin modificar ningún aspecto de su configuración.

6.3.5. Configuración MySQL

Como la página web obtendrá, tanto su contenido como los diferentes usuarios que pueden conectar a la misma, desde la base de datos, es necesario que se configure correctamente para que no se produzcan intrusiones en la misma.

Para ello, se instalará la base de datos de forma normal, pero posteriormente a su instalación se utilizará un proceso de instalación segura. Con este proceso se cambian las configuraciones necesarias para contar con un servidor seguro, estas son:

Eliminar usuarios anónimos: como la base de datos se utilizará únicamente para la página web, no se necesitan usuarios anónimos, por lo que, se desactiva su uso.

Eliminar el acceso de administrador remoto: el tener la base de datos instalada en el mismo equipo que la página web, en caso de querer gestionarla desde la página web no se necesita acceso remoto, por lo que se elimina esta opción para mantenerla más segura.

Eliminar bases de datos de prueba y acceso a las mismas: puesto que se ha realizado una instalación correcta, se eliminan las bases de datos de prueba y el acceso a las mismas, protegiendo el acceso a las bases de datos que se creen posteriormente.

Recargar la tabla de privilegios: al realizar este proceso se recargan todos los permisos que se hayan modificado, por lo que, todos los cambios realizados tendrán un efecto inmediato asegurándonos que las medidas tomadas están surgiendo efecto inmediato.

Al realizar esta configuración se aumenta el nivel de seguridad de la base de datos considerablemente, atendiendo a las políticas establecidas.

6.3.6. Configuración Joomla

En la propia instalación de Joomla™ se pueden efectuar la configuración del mismo.

Las configuraciones utilizadas son la utilización del correo "postmaster@dominio.com" como correo del administrador de la página web. De esta manera, se utiliza un correo en el que no se especifica quien atenderá al mismo, pudiendo configurar esa dirección de correo electrónico posteriormente en el servidor de correo.

También, se decide no permitir el acceso mediante FTP. Esta decisión se ha tomado debido a que se contará con un servidor de FTP dedicado a este servicio únicamente, por lo que utilizar el servicio de FTP de Joomla™ no será necesario.

El resto de configuraciones se mantienen por defecto debido a que es una configuración que cumple las diferentes políticas establecidas.

6.4. Servidor de correo

El servicio de correo electrónico es un conjunto de elementos que al agruparse ofrecen unos servicios que permiten tanto enviar como recibir correos electrónicos.

Estos servicios se implantan a través de tres diferentes software. Estos software son:

MUA (Mail User Agent): el agente de correo de usuario son los propios clientes de correo. Estos clientes son los encargados de proporcionar una interfaz al usuario tanto para leer como para enviar y recibir correos.

MTA (Mail Transfer Agent): el agente de transferencia de correo es el programa encargado de transferir los correos entre las diferentes máquinas utilizando el protocolo SMTP.

MDA (Mail Delivery Agent): el agente de entrega de correo es el programa encargado de conectar con el almacén donde se alberguen todos los correos electrónicos. Una vez establecida esta conexión, el MDA es el encargado de presentarle estos correos al buzón de correo del usuario, donde éste podrá leerlo correctamente.

6.4.1. Selección de servidor

Debido a lo anteriormente comentado, para disponer de un servicio de correo electrónico completo se necesitará al menos de un software que implemente cada uno de los agentes.

En este caso, debido a que los diferentes MUA no presentan grandes diferencias entre los existentes, se dejará su elección al usuario del equipo. Siendo los MUA más comunes KMail™, Evolution™, Mozilla Thunderbird™ o Microsoft Outlook™ entre otros.

Seleción de MTA

Para el servicio de MTA se ha decidido utilizar Postfix. Esto se debe a que Postfix es un sistema muy utilizado que surgió como evolución de Sendmail™, siendo un MTA de uso y configuración muy sencillo teniendo una gran seguridad al mismo tiempo. Además, Postfix cuenta con un gran número de compatibilidades con diferentes protocolos haciendo, que en caso de querer ampliar el servicio al uso de otros protocolos, no sea necesario cambiar el servidor, atendiendo de esta manera a la política establecida.

Por lo tanto, se utilizará un servidor Postfix como servidor MTA.

Selección de MDA

En la selección del MDA se ha optado por utilizar Dovecot™. Esta elección se debe a diversas características de Dovecot™ que hacen que sea una opción adecuada. Estas características son:

- Gran rendimiento: es uno de los MDA con mayor rendimiento que hay.
- Soporta diferentes formatos de buzón de correo: de esta manera, permite integrarse con el formato más adecuado que se crea oportuno.
- Soporta tanto IMAP como POP3: puede proporcionar ambos servicios, permitiendo que cada usuario elija el servicio que se acomode a sus gustos.
- Es un servidor orientado a la seguridad: los desarrolladores de Dovecot™ se centraron en la seguridad creando un servicio altamente seguro.
- Cuenta con un gran número de plugins: al tener estos plugins Dovecot™ puede integrarse con otros servicios tales como LDAP, atendiendo de esta manera a la política de crecimiento de la red. Ya que, en caso de que la red crezca y se instale un servicio como LDAP, solo sería necesario configurar el plugin correspondiente para que Dovecot™ siguiera funcionando.

Por lo tanto, se utilizará un servidor Dovecot™ como servidor MDA proporcionando los servicios de IMAP y POP3.

6.4.2. Configuración del servidor

Configuración de Postfix

En la instalación de Postfix es necesario que se realicen algunas configuraciones para que funcione correctamente.

Se selecciona una configuración general de “Internet Site”, debido a que es la opción que más se adecua con las políticas y funcionamiento de la empresa. Además, se selecciona “dominio.com” como “System mail name”, en esta opción se especifica cual es el dominio con el que trabajará el servidor. La utilización de “dominio.com” se debe a que al estar realizando una simulación no se cuenta con un dominio propio que se pueda incluir, por lo que se utiliza esta opción para el proyecto.

Posteriormente, se ha elegido que el usuario que reciba los correos enviados al “postmaster” sea el usuario “root” del equipo donde se encuentra instalado el servidor. Esto se debe a que los correos enviados al “postmaster” son los que tienen como destino el administrador del servidor, por lo tanto, se ha elegido el administrador de ese equipo para que reciba estos correos.

Además, se configuran las opciones que establecen que se recibirá el correo con destino “dominio.com”, es decir, que se recibirán todos los correos dirigidos a “ejemplo@dominio.com”, donde “ejemplo” es cualquier usuario.

Por último, también se configura las redes desde las cuales se reenviarán correo para únicamente reenviar correo que proceda de las redes de la empresa. De esta manera, se evita que se pueda utilizar el servidor para reenviar correo no deseado a otros MTA.

Configuración de Dovecot™

Para Dovecot™ se deben de seleccionar diferentes configuraciones que establezcan tanto la forma de autenticación de los usuarios con el servidor, como el tipo de formato de buzón que se utiliza.

Se ha configurado que para la autenticación de usuarios no se permitan autenticaciones en texto plano, es

decir, sin ningún cifrado. Además, para poder comprobar posibles ataques también se activa el guardado de las contraseñas erróneas en el `log`, pero con cifrado para evitar que si algún usuario tiene un error al autenticarse si otro usuario malicioso se haga con el `log` tenga la contraseña fallida en texto plano, aumentando de esta manera la seguridad.

Posteriormente, se ha configurado la utilización de “mbox” como formato de buzón. Este formato de buzón utiliza un único archivo por cuenta de correo electrónico en el que guarda todos los correos de ese usuario. Se ha decidido utilizar este formato de buzón de correo debido a que a diferencia de “maildir” no tiene problemas por tener que bloquear los archivos.

Por último, se configurará `Dovecot`™ para que permita conexiones desde cualquier punto internet, atendiendo, de esta manera, a la política que especifica que el correo debe ser accesible desde cualquier punto de internet.

6.5. Base de datos interna

6.5.1. Selección de servidor

Para ofrecer el servicio de base de datos se debe seleccionar el tipo de base de datos que se utilizará, así como, el servidor que proveerá esa base de datos. En este caso se ha elegido utilizar una base de datos SQL. Esta decisión se debe a que el lenguaje SQL tiene un uso muy extendido siendo el lenguaje más utilizado para la gestión de bases de datos.

Posteriormente, entre las diferentes opciones de bases de datos que utilicen SQL se ha decidido utilizar `PostgreSQL`™. Esta elección se debe a las diferentes características de `PostgreSQL`:

Servidor libre: `PostgreSQL`™ se trata de un servidor gratuito que se mantiene en desarrollo lo que produce que sea muy fácil mantenerlo actualizado.

Alta concurrencia: se permiten realizar varias conexiones simultáneas a la misma tabla de una base de datos sin necesidad de utilizar sistemas de bloqueaos que ocasionen problemas.

Ejecución de funciones: `PostgreSQL`™ permite la ejecución de funciones en diferentes lenguajes de programación otorgando una gran funcionalidad.

6.5.2. Configuración del servidor

La base de datos conlleva dos configuraciones distintas. Por un lado se debe configurar el acceso al propio servidor y, por otro lado, se debe configurar la base de datos y los diferentes permisos de su contenido y las conexiones a la misma.

Lo primero será crear una base de datos para la utilización por la empresa. Para ello se crea una base de datos utilizando como plantilla la instalada por defecto con el servidor `PostgreSQL`™, ya que se trata de una base de datos vacía que contiene las propiedades básicas.

Posteriormente, para la gestión de la base de datos se utilizará la herramienta de `pgAdmin III`, esto se debe a que través de una conexión con la base de datos se proporciona una interfaz muy sencilla que permite crear, eliminar o modificar los diferentes elementos de la base de datos. A través de esta herramienta se crearán los diferentes elementos de la base de datos, tales como usuarios, grupos o tablas, y sus configuraciones.

Por otro lado, se debe configurar el acceso al servidor, en este caso se decide que el servidor estará a la escucha de conexiones en toda la red, pero que únicamente se podrán conectar usuarios de la red interna de la empresa con usuarios con contraseña codificada con “md5”. Con esta medida, se permite el acceso a la base

de datos, pero al mismo tiempo se limita el acceso a usuarios con permisos para acceder a la misma. Además, al permitir conexiones únicamente con cifrado, se aumenta la seguridad evitando que puedan ser capturados los credenciales del usuario.

6.6. Servidor Samba

6.6.1. Selección de servidor

Puesto que en la propia política se especifica que se requiere un servidor Samba, no es necesario elegir que servidor se utilizará. Se utilizará el servidor Samba instalándolo a partir de las librerías oficiales de Ubuntu™.

6.6.2. Configuración del servidor

La configuración utilizada en Samba especificará cual será el funcionamiento del mismo, puesto que parte de la configuración consiste en especificar cuales son las diferentes carpetas que serán compartidas.

Por lo tanto, las opciones utilizadas serán las siguientes:

- Grupo de trabajo “WORKGROUP”. Se ha elegido este grupo de trabajo puesto que los diferentes equipos Windows™ utilizan este grupo de trabajo por defecto, lo que elimina el tener que configurar esta opción para que estos equipos tengan acceso al servidor Samba.
- Se elige “Samba” como “netbios name”. Con esta opción se especifica el nombre que tendrá el servidor en la red, quedando claramente identificado que se trata del servidor Samba a través del nombre.
- Se podrá conectar únicamente con la red interna de la empresa. De esta manera se aumenta la seguridad del servidor, ya que no se permiten conexiones desde el exterior de la red interna.
- Los fallos en la identificación del usuario rechaza la conexión. Con esta opción se asegura que no se realicen conexiones anónimas con el servidor o que un fallo en la identificación del usuario le conceda unos permisos no esperados.
- Se creará una zona compartida pública para todos los usuarios de samba. En esta zona compartida se compartirán los archivos a los que deban tener acceso todos los usuarios con acceso al servidor Samba.
- Todos los usuarios tendrán compartida su carpeta personal. De esta manera se asegura que todos los usuarios del servidor Samba puedan utilizar el mismo para mantener archivos de forma segura o para utilizar los mismos archivos en diferentes puestos de trabajo o sistemas operativos.

6.7. Servidor de impresión Linux

6.7.1. Selección de servidor

Para la selección del servidor de impresión Linux no existen tantas opciones como para otros servicios. En este caso se ha elegido utilizar CUPS. Esta elección está motivada porque se trata de un servicio que viene incorporado el cliente en los diferentes sistemas operativos de GNU/Linux™, lo que facilita su utilización. Además, debido a esta misma característica es un servidor muy usado para compartir las impresoras a través de GNU/Linux™ únicamente.

Para su instalación se utilizarán las librerías oficiales de Ubuntu™, asegurando de esta manera que se trata de software oficial y permitiendo una actualización sencilla.

6.7.2. Configuración del servidor

Para la configuración del servidor de impresión se utilizará la interfaz web del mismo debido a su mayor sencillez. Sin embargo, para que se permita el acceso a la interfaz web se debe realizar una configuración preliminar.

En esta primera configuración se activará la configuración a través de la interfaz web. Aunque esta configuración a través de la web se limitará. Para limitar el acceso solo se permitirán conexiones desde la red de la empresa y, además, solicitarán que se introduzca el usuario administrador del equipo donde esté instalado el servidor de impresión. De esta manera se limita el acceso a la interfaz web aumentando la seguridad del mismo.

Posteriormente, se instalarán las diferentes impresoras a través de la misma interfaz seleccionando los *drivers* correspondientes, quedando de esta manera el servidor funcionando por completo correctamente.

6.8. Asignación de equipos a los servidores

Una vez se han definido los diferentes servidores a usar, se debe especificar en que equipos se instalarán los servidores.

En este caso se ha decidido instalar los diferentes servicios en equipos separados en su mayoría. Esto se debe a que en caso de aumentar la carga de la red considerablemente se podrían producir problemas de congestión de tráfico en caso de que un mismo equipo contuviera varios servicios. Además, al aumentar el tamaño de la red también aumenta la información que deben albergar los diferentes servidores, ya que se guardará más información en la base de datos o en los servidores de archivos por ejemplo.

Como se especificó anteriormente, se utilizará `Ubuntu`™ para los diferentes equipos de la red, pero se utilizará `Ubuntu Server`™ o `Ubuntu`™ para los servidores. Para aquellos servicios que no requieren una interfaz de usuario para instalar, configurar y gestionarlos, se utilizará `Ubuntu Server`™, ya que de esta manera se reduce la carga al equipo, puesto que `Ubuntu Server`™ es un sistema más ligero. Por otro lado, para los servicios que necesiten una interfaz de usuario se utilizará `Ubuntu`™.

Además de esto, también se debe especificar cuales son las diferentes direcciones IP de los servidores, ya que como se explicó anteriormente, se utilizarán direcciones IP fijas para estos.

Por lo tanto, se ha decidido seguir la distribución especificada en la tabla 6.1.

Servicio	Dirección IP	Dirección Física
DHCP	192.168.1.1	00:1F:C6:7D:FA:C6
Samba	192.168.1.5	00:50:56:22:D0:A0
FTP Interno y CUPS	192.168.1.6	00:50:56:33:41:9D
Base de datos	192.168.1.7	00:50:56:37:79:4F
DHCP Libre	192.168.1.25 // 192.168.2.1	00:50:56:29:5D:12 // 00:0C:28:8C:15:01
FTP Libre	192.168.2.5	00:50:56:2A:A2:C6
Correo	192.168.2.6	00:50:56:35:9F:4F
Web	192.168.2.7	00:50:56:33:82:84

Tabla 6.1: Tabla de distribución de servicios a equipos con sus direcciones IP y direcciones MAC. En la tabla se muestran los diferentes servicios existentes en la red junto con la dirección IP y dirección MAC del equipo que provee ese servicio.

Una vez asignados estos servidores, la configuración final de la red es la que se puede observar en la imagen 6.1.

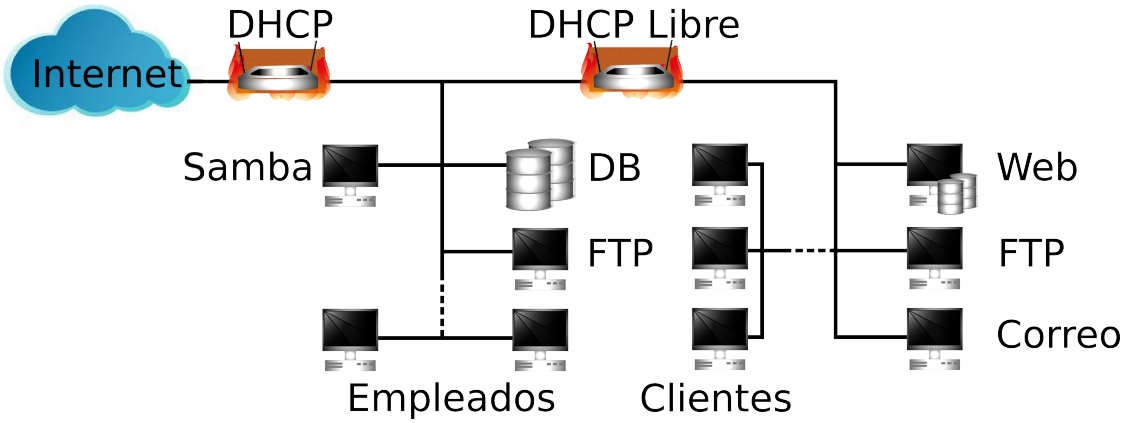

Figura 6.1: Estructura final de la red con la asignación de equipos a los servicios establecidas. Se puede observar las dos zonas de la red, junto con los diferentes servidores existentes en cada zona.

III

Auditoría de seguridad

7

Diseño del proceso de auditaje

La razón de la realización de la auditoría a la empresa es debido a que tiene un acuerdo con un organismo oficial. Entre otras especificaciones, este acuerdo establece que la empresa debe cumplir la normativa nacional de seguridad que afecta a los organismos públicos.

De esta manera, se realizará una auditoría de seguridad con diferentes procedimientos. A lo largo de ésta, se realizará tanto una revisión del cumplimiento de la normativa como una auditoría en la que se analicen las posibles vulnerabilidades existentes, tanto en la seguridad física como en las vulnerabilidades de software de los diferentes equipos. Sin embargo, debido a que en la normativa se establecen diferentes aspectos de seguridad, también se revisará su cumplimiento en función de las diferentes vulnerabilidades que puedan existir.

Para la realización de la auditoría se parte de la red anteriormente creada en la que se han añadido diferentes usuarios. Debido a que la creación de un gran número de usuarios con prácticamente los mismos permisos no añade un gran interés al proyecto, se ha decidido crear un número menor de usuarios teniendo en cuenta el impacto de las contraseñas.

Por lo tanto, para estudiar este impacto de las contraseñas, en cada servicio se han creado tres usuarios con diferentes niveles de complejidad en las contraseñas. De esta manera, se pretende que se pueda estudiar el impacto de las diferentes contraseñas para la seguridad.

Dentro de cada grupo de tres usuarios se han definido los siguientes niveles de complejidad:

Nivel bajo: en este nivel se han utilizado contraseñas que consisten en palabras habituales o combinaciones de números simples. Algunos ejemplos de estas contraseñas son *password* o *123456*.

Nivel medio: para el nivel medio se han utilizado contraseñas que consistían en una palabra en la que algunas letras se cambiaban por números. Algunos ejemplos son *c0rr3ct0* o *pr0y3ct0*.

Nivel alto: en el nivel más alto se han utilizado contraseñas de grandes longitudes en las que se combinan letras, números y caracteres especiales sin sentido aparente. En este nivel algunos ejemplos son *mju7YGVfr4ESZ789IJN* o *<aw3EDCvfr4 %&/ygHN*.

Por otro lado, para el usuario administrador del sistema se ha utilizado, en la mayoría de los casos, una práctica muy habitual en las empresas. Ésta consiste en la utilización del mismo nombre de usuario y contraseña para el administrador de los diferentes servicios. Esto se debe a que muchas veces el usuario encargado de gestionar los diferentes servicios es el mismo, puesto que suele ser un experto en informática, y no utiliza diferentes usuarios por la complejidad que supone recordarlos todos. Con esto, se pretende mostrar el gran error de seguridad que puede conllevar utilizar el mismo usuario y contraseña para la administración de diferentes servicios.

Adicionalmente, para que se acentúe la importancia de las actualizaciones y puedan existir un mayor número de vulnerabilidades en la red empresarial, se ha realizado la última actualización de todos los servicios el día 24 de noviembre de 2013. Por otro lado, la última actualización de las herramientas de ataque se realizó el día 24 de diciembre de 2013. De esta manera, se ha dejado un periodo de 2 meses de diferencia de actualización entre los servicios y las herramientas de ataque, permitiendo de esta manera la aparición de un mayor número

de vulnerabilidades.

7.1. Revisión de normativa

Debido a que la empresa creada es hipotética no dispone de una sede. Por lo tanto, toda la normativa que afecta la seguridad de acceso a los diferentes elementos de la red, así como, de localización de los mismos no puede ser comprobada. En este caso, se supondrá que se ha comprobado la normativa sin encontrar incumplimientos.

Por otro lado, como se especificó anteriormente, no se creará un gran número de usuarios, por lo que las normativas que hacen referencia a los diferentes permisos de usuarios y grupos no serán revisadas. Sin embargo, a diferencia de la normativa referente a la seguridad perimetral, estos artículos si serán explicados en el informe de seguridad.

La normativa a tener en cuenta es la que se especifica para las instituciones oficiales del estado. Ésta se recoge en el Real Decreto 3/2010 que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, donde se especifican todas las medidas que se tendrán en cuenta.

7.2. Revisión de la seguridad física

En la revisión de la seguridad física se deben de revisar las condiciones físicas de la empresa. Puesto que se trata de una empresa hipotética y no cuenta con una sede, se especificarán los aspectos que se deben comprobar. Una vez especificados, se expondrán diferentes fallos para que quede reflejado en el informe final de resultados.

En este capítulo se revisarán aspectos como el control de acceso a los diferentes puestos de trabajo y puntos de conexiones con las redes entre otros. Las revisiones ha realizar son:

Controles de acceso: deben de existir diferentes controles de acceso para que los usuarios no puedan utilizar equipos para los que no tienen permisos. Los diferentes controles que deben existir son:

- **Control de acceso a los servidores:** debe ser restringido, de manera que únicamente los diferentes administradores puedan tener acceso a los servidores en los que tienen permisos.
- **Control de acceso a la zona de la red privada:** únicamente los trabajadores deben de tener acceso a las zonas donde se encuentran los equipos de la red privada.
- **Control de acceso a la zona de la red para invitados:** debe tener un control de acceso. Aunque se trate de una red para invitados, puesto que tiene algunos de los servicios implementados en esa red,por lo que es necesario tener un control de acceso a esa zona.

Control de las conexiones a la red: puesto que se cuenta con servicio de DHCP en cuanto un ordenador se conecte con la red obtendrá una dirección IP y completo acceso a la red. Por lo tanto, se debe tener un control en los diferentes puntos de acceso a la red para evitar conexiones no deseadas.

Control de identificaciones: se debe contar con un control de identificaciones de usuario. De esta manera se contará con la información de que usuarios se encuentran en cada zona de la sede de forma que es posible localizar accesos a cuentas de usuarios que no se encuentran en la empresa. Además, en caso de producirse un incidente de seguridad, es posible reducir el número de usuarios que han podido producirlo.

7.3. Revisión de la seguridad de usuario

En este capítulo se revisará la seguridad relativa a los usuarios. Este tipo de seguridad es la que tiene mayor complejidad de ser revisada puesto que cuenta con un factor humano y, por tanto, no se puede asegurar la veracidad de la información que proporcionan los trabajadores.

En este apartado se deben de revisar los diferentes aspectos de seguridad relacionados con los usuarios de la red, es decir, los diferentes trabajadores de la empresa. Los aspectos a tener en cuenta en este apartado son:

Abandonar el puesto de trabajo: se debe comprobar las diferentes formas de actuar de los trabajadores al abandonar su puesto de trabajo. En este proceso se comprobará si los usuarios bloquean los equipos al ausentarse de sus puestos de trabajo en cortos periodos de tiempo o si detienen todas las conexiones de su equipo y lo apagan cuando termina su jornada.

Políticas de contraseñas: se comprobarán las políticas de establecimiento de contraseña. En estas políticas se incluyen tanto la complejidad como la longitud de las mismas, además también se incluye la posibilidad de establecerles una caducidad. Esta caducidad establece cada cuanto se debe cambiar la contraseña de un servicio.

Guardado de contraseñas: se debe comprobar que los usuarios no almacenen sus contraseñas en ningún lugar sea o no accesible a otras personas.

Contraseñas: se debe realizar un control de las diferentes contraseñas utilizadas por los usuarios. En esta comprobación se debe comprobar tanto la complejidad de las mismas como su repetición en los diferentes servicios de la red. También se comprobará la caducidad de las contraseñas, es decir, si se establece un cambio forzoso de contraseña pasado un tiempo.

7.4. Test de penetración

Se revisarán las diferentes vulnerabilidades existentes en los equipos de la red. Para ello se realizará una auditoría de seguridad de la red.

Debido a que ya existen unos conocimientos previos de la red, se ha decidido utilizar un modelo de auditoría de seguridad organizado en diferentes fases. Cada una de estas fases es independiente de las posteriores, y permiten una organización eficiente del trabajo. Sin embargo, es posible que sea necesario volver a una fase anterior debido a que no se cuenta con la información necesaria para continuar con la auditoría y es necesario obtenerla.

Así mismo, la auditoría de seguridad se ha basado en un modelo de *Doble Ciego* o *Test de Penetración* [25],sin embargo, se modificará ligeramente este modelo para mostrar las funciones de algunos de los elementos de la red. A continuación se especificarán las diferentes fases y en que consiste cada una.

7.4.1. Recopilación de información

La primera fase de un *Test de penetración* es la recopilación de información acerca de la empresa a auditar. En este proceso se trata de reunir toda la información posible acerca de la empresa a través de diferentes medios, desde redes sociales o la página de la empresa, hasta el uso de herramientas específicas.

Esta recopilación de información se debe a que esta información será la que se utilizará en las fases posteriores para analizar las vulnerabilidades. Por lo tanto, se debe adquirir toda la información disponible. Por ejemplo, acerca de la red de la empresa, para saber cuales serán los objetivos de los ataques, o información acerca de la actividad de la misma, para tratar de averiguar cuales serán los mecanismos de seguridad que tendrá y donde se localizará la información sensible.

7.4.2. Análisis de vulnerabilidades

Una vez finalizada la fase de recopilación de la información, comienza la fase de *Análisis de vulnerabilidades*. Esta fase, como su propio nombre indica, consiste en el análisis de los diferentes elementos de la red, de forma que se descubran las diferentes vulnerabilidades existentes en los mismos.

A lo largo de esta fase, por lo tanto se utilizan herramientas como `Nessus`™ o `Nmap`™. Estos son escáneres de vulnerabilidades que, dadas las direcciones IP de los diferentes equipos a analizar, presentan un informe de las vulnerabilidades existentes en los equipos. Sin embargo, estos programas no son completamente fiables, puesto que pueden presentar falsos positivos o falsos negativos, es decir, que pueden existir vulnerabilidades no detectadas o alguna de las detectadas no ser una vulnerabilidad real. Por lo tanto, es una buena práctica utilizar diferentes escáneres de vulnerabilidades para contrastar los resultados.

7.4.3. Explotación

Una vez analizados todos los equipos obteniendo las diferentes vulnerabilidades existentes en los mismos, comienza la fase de explotación. Esta fase consiste en la utilización de diferente software como `Metasploit`™ para realizar diferentes ataques a los equipos aprovechando las vulnerabilidades encontradas.

A través de este software se pueden realizar diferentes acciones, dependiendo del tipo de vulnerabilidad existente y de las intenciones del atacante. En el caso más extremo, a través de estas herramientas se puede tomar un control total del equipo con la vulnerabilidad, consiguiendo acceso de administrador al mismo. De esta manera, se podría conseguir acceder a toda la información que contenga ese equipo que puede ser información sensible.

8

Realización de la auditoría

En este capítulo, se especificará como se han realizado los procesos de la auditoría, enumerando los diferentes pasos realizados. Para ello se presentarán diferentes secciones que explicarán los procesos de forma aislada.

8.1. Revisión de normativa

En este apartado se revisará la normativa exponiendo los diferentes artículos de la normativa a tener en cuenta. Se expondrá, únicamente, el número del artículo a tener en cuenta y una breve explicación del mismo, para más detalle acerca de los diferentes artículos tratados se puede consultar el BOE [21].

Se comprueba la configuración de los diferentes equipos comprobando el cumplimiento del artículo. Tras la realización de la revisión se comprueba que:

Artículo 19: Seguridad por defecto: solo se deben proporcionar los servicios mínimos establecidos y que deben ser seguros.

- Los diferentes equipos solo proporcionan los servicios que especifican.
- Los diferentes servicios tienen limitada su administración por un usuario administrador y, en alguno de los casos, tienen una limitación de administración desde únicamente la red interna de la empresa.
- Los sistemas solo pueden utilizarse de forma segura a excepción de la utilización de contraseñas poco seguras, pero este aspecto se comentó anteriormente que no se tendría en cuenta. Se asegura la utilización de forma segura de los servicios permitiendo un uso con cifrado únicamente por ejemplo.

Artículo 21. Protección de información almacenada y en tránsito: se deben mantener los datos seguros, ya sea en la transmisión o en el almacenamiento de los mismos.

- Para los equipos propios de la empresa se utiliza una conexión cifrada para algunos de los servicios. Sin embargo, tanto para el servicio de Samba, como para equipos personales de los usuarios, no se tiene en cuenta este aspecto, por lo que habría que corregirlo.

Artículo 22. Prevención ante otros sistemas de información interconectados: se deben tener en cuenta los riesgos de conectar una red pública.

- Debido a la política inicial de la empresa, no se tienen en cuenta los riesgos de tener una zona pública de la red que permita conectar a cualquier usuario. Por lo tanto, se establece un problema grave de seguridad por no tener en cuenta este aspecto.

Artículo 23. Registro de actividad: debe existir un control de las actividades de los usuarios que permita analizar las actividades indebidas.

- No se realiza ningún control de las actividades de los usuarios a excepción de los registros de actividades de alguno servicios. Sin embargo, si que se graba un registro cuando se produce un error en

una autenticación en algún servicio o una actividad para la que no se tiene permisos.

Artículo 24. Incidentes de seguridad: debe existir un sistema de detección de código dañino y un registro de estos incidentes.

- No existe ningún método de detección o reacción frente a código dañino. Además, tampoco existe ningún registro de los diferentes incidentes de seguridad que se produzcan.

Artículo 25. Continuidad de la actividad: deben existir copias de seguridad y sistemas que puedan garantizar la continuidad de las operaciones.

- No existe ningún método de copia de seguridad de ninguno de los servicios ni bases de datos.

Artículo 42. Actualización permanente: se debe mantener una política de actualizaciones que mantenga los diferentes equipos actualizados correctamente.

- No existe una política de actualización existente. Sin embargo, como se explicó anteriormente, se realizó una última actualización de todos los sistemas en una fecha concreta para poder mostrar la importancia de mantener un sistema actualizado.

Además de los propios artículos, según lo establecido en el artículo 34, se deben realizar auditorías de seguridad de forma periódica que comprueben lo establecido en los anexos. Por lo tanto, también hay que revisar la normativa establecida en los diferentes anexos.

En el primer anexo se especifica como clasificar los servicios según los daños que puede causar un fallo en su funcionamiento, o como se deben identificar los diferentes errores. En este caso, se utilizará la categoría MEDIA, puesto que para que fuera de categoría ALTA sería necesario que un paro de las actividades de la empresa significara un paro en las actividades de una entidad gubernamental, y en este caso no es así. Por otro lado, no se utiliza la categoría de BAJA para que se pueda ver la aplicación de un gran número de medidas, ya que en esta categoría se elimina gran parte de la normativa.

En el segundo anexo se encuentra la normativa que se debe comprobar en la auditoría a realizar y,por tanto, debe ser revisada. En este anexo la normativa se encuentra separada en tres grandes bloques:

Marco organizativo: está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

Política de seguridad: la política de seguridad debe ser aprobada por un organismo superior, y en este caso no ha sido revisada por ninguna entidad.

Normativa de seguridad: no existen documentos que especifiquen el uso correcto de los equipos ni las responsabilidades con respecto al cumplimiento o violación de estas normas.

Procedimientos de seguridad: no existe documentación donde se especifique como llevar a cabo las diferentes tareas habituales, ni que hacer en caso de un comportamiento anómalo.

Proceso de autorización: no existe ningún proceso formal de autorizaciones para ninguna utilización de los diferentes servicios o equipos.

Marco operacional: constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin. A su vez, este marco está dividido en diferentes categorías:

Planificación: no existe documentación que especifique los diferentes riesgos, ni tampoco existe documentación acerca de la seguridad de la red. Sin embargo, parte de esta documentación será creada con la realización de esta auditoría.

Control de acceso: respecto al control de acceso se cumple la normativa a excepción de que las tareas críticas, tales como administración de servicios, deben realizarse por al menos dos usuarios diferentes. También se incumple que no se utilizan elementos de seguridad física como tokens para la identificación de usuarios.

Explotación: se cumple parte de esta normativa, puesto que se mantiene una política de funcionalidad mínima y seguridad por defecto. Sin embargo, no existe un control de incidencias ni tampoco existe

protección frente a código dañino.

Servicios externos: puesto que no se utilizan para ninguna tarea de la red empresarial, no se aplica esta normativa.

Continuidad del servicio: no existe un análisis de impacto de los diferentes problemas que pueden provocarse por un breve fallo en alguno de los servicios.

Monitorización del sistema: puesto que no se trata de una categoría ALTA esta normativa no se aplica.

Medidas de protección: se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. Este apartado se encuentra dividido en diferentes secciones:

Protección de las instalaciones e infraestructuras: puesto que se ha realizado una virtualización de la red y, además, se trata de una empresa hipotética que no cuenta con una oficina real, esta normativa no se puede comprobar.

Gestión del personal: puesto que no se han creado puestos de trabajo no se puede comprobar esta normativa. Sin embargo, habría que informar y formar a los diferentes trabajadores para conozcan cuales son sus obligaciones y tareas en la empresa.

Protección de los equipos: esta normativa se cumple correctamente ya que los diferentes equipos se bloquean automáticamente después de un periodo de inactividad requiriendo una nueva identificación del usuario.

Protección de las comunicaciones: se cumple esta normativa ya que se protegen las comunicaciones con el uso de un *firewall* y con la autenticación de los equipos antes de comenzar una transmisión mediante SSL.

Protección de los soportes de información: esta normativa no es comprobable por las características ya comentadas de ser un caso hipotético.

Protección de las aplicaciones informáticas: puesto que no se realiza un desarrollo de aplicaciones, no es aplicable esta normativa.

Protección de la información: no existe ningún método para catalogar la información. Además, tampoco existe un sistema de firma digital ni se ha realizado una limpieza de los *metadatos* de los archivos.

Protección de los servicios: en este apartado se establecen las medidas que se deben establecer para diferentes servicios. Estas son:

Protección del correo electrónico: se cumple parte de la normativa, ya que se utiliza cifrado SSL. Sin embargo, no hay ningún método de protección frente a virus, troyanos y otro *malware* que pueda adjuntarse en los correos.

Protección de servicios y aplicaciones web: se tiene en cuenta el proteger el acceso a los contenidos obviando la autenticación. Sin embargo, no hay métodos de prevención frente a ataques de escalado de privilegios, “cross site scripting” o programas de manipulación.

Protección frente a la denegación de servicio: se cumple parte de la normativa puesto que se ha tenido en cuenta la carga de la red en la creación de los servicios. Sin embargo, no existen métodos de prevención frente a este tipo de ataques.

8.2. Revisión de la seguridad física

En este capítulo se revisará la seguridad física de la red. Para ello se deben verificar diferentes aspectos de la sede empresarial explicados anteriormente.

Para la comprobación de las diferentes medidas de seguridad física se debe contar con acceso completo a la empresa, de forma que se pueden realizar las comprobaciones personalmente.

Al realizar la revisión de estos aspectos se ha encontrado un cumplimiento en varios de los tenidos en

cuenta: se cuenta con un control de acceso a las diferentes zonas de la red y se tiene un control de los diferentes puntos de acceso a la red.Sin embargo, no se realiza un control de acceso a los servidores y cualquier empleado puede tener acceso a los mismos.

Además, el control de identificación de usuarios se realiza mediante un código de empleado y una contraseña, por lo que, al no tratarse de un token físico, cualquier persona podría acceder a la empresa con los credenciales de usuario de otro empleado.

8.3. Revisión de la seguridad de usuario

En este capítulo se realizará una revisión de los diferentes aspectos de seguridad relacionados con los usuarios de la red.

Para las comprobaciones de los aspectos anteriormente comentados se utilizarán diferentes métodos a tener en cuenta:

Abandonar el puesto de trabajo: para esta comprobación se realizará un pequeño cuestionario a algunos trabajadores acerca se sus costumbres de trabajo, entre las que se encontrarán el abandono de su puesto. Además, se realizará una visita imprevista a la empresa en la que se comprobará si se cumplen las medidas necesarias.

- Tras estas comprobaciones no se han encontrado problemas de seguridad. Los cuestionarios indican que los trabajadores bloquean correctamente sus equipos y no se encontraron disconformidades en la visita a la empresa.

Políticas de contraseñas: para la comprobación de las mismas se debe contar con acceso a los diferentes servidores que tiene la empresa. Una vez se cuente con el acceso a los servidores se comprueba las políticas de creación de contraseñas de los diferentes servicios.

- Tras la comprobación de las políticas se observa que las políticas permiten la utilización de contraseñas muy débiles, además se comprueba que no existe caducidad de las contraseñas ni se controla su repetición para los diferentes servicios.

Guardado de contraseñas: al mismo tiempo que se realiza el cuestionario acerca de la costumbre de bloqueo del ordenador también se utiliza el cuestionario para comprobar si los usuarios guardan sus contraseñas en algún lugar, ya sea un archivo en el ordenador o en algún medio físico en su puesto de trabajo. También se realizará una comprobación de el puesto de trabajo de alguno de los empleados al azar.

- Tras esta comprobación física se encuentra que, a pesar de que los usuarios dicen no guardar las contraseñas en ningún lugar, se han encontrado algunos puestos de trabajo con contraseñas de los diferentes servicios utilizados.

Contraseñas: se deben de realizar dos procesos diferentes. El primero consiste en la comprobación de la repetición de contraseñas, mientras que el segundo corresponde con la complejidad de las mismas. Para el primero de los procesos se debe contar con una lista de las diferentes contraseñas, para conseguirlas se debe acudir a los administradores de los servicios, aunque no siempre es posible contar con esta lista. Para la comprobación de la complejidad de las contraseñas se utilizara el programa `Hydra` cuyas características y funcionamiento están explicados en el apéndice B.4.2.

- Una vez obtenida la lista de contraseñas se observa que las utilizadas para las cuentas de administración de algunos servidores están repetidas. Esto es muy peligroso puesto que si algún usuario consiguiera sustraer la contraseña de un servidor podría acceder a los demás de forma trivial.

  Debido a que la comprobación de la complejidad de las contraseñas es un proceso laborioso, este proceso se ha especificado a continuación.

8.3.1. Complejidad de las contraseñas

Como se especificó anteriormente para la comprobación de la complejidad de las contraseñas se utilizará el programa `Hydra`. A través de este programa se prueban todas las diferentes combinaciones de usuario y contraseña de un diccionario tratando de acceder a un servicio.

Lo primero que se debe seleccionar es el diccionario a utilizar. Un diccionario es un conjunto de posibles usuarios o contraseñas que se utilizan habitualmente es los equipos. Existen un gran número de diccionarios de diferentes tamaños y con diferentes tipos de usuarios, habitualmente separados por el idioma o la temática utilizada.

En este caso, se utilizará un diccionario muy pequeño en el que se encuentran 500 de los usuarios y contraseñas mas utilizados. La decisión de utilizar este diccionario se debe a que se está tratando de mostrar como la mayoría de las contraseñas utilizadas por los usuarios se encuentran en diccionarios muy simples.

Además de la utilización de este diccionario, se ha incluido la utilización de una opción que permite intercambiar algunas letras con números de apariencia similar. Se ha decidido utilizar esta opción puesto que es muy utilizada por los usuarios en la creación de sus contraseñas y, de esta manera, se tratará de demostrar que no añade mucha seguridad a las contraseñas. Algunos de los cambios que se realizan entre letras y números son: I->1, E->3, A->4, S->5, O->0, S->$.

Tras realizar los ataques a los diferentes servicios se han obtenido los siguientes resultados:

- Las contraseñas de los usuarios establecidas como débiles han sido todas extraídas con satisfacción.
- Algunas de las contraseñas de los usuarios establecidas como medias han sido extraídas, pero no la totalidad de las mismas.
- Ninguna de las contraseñas de los usuarios establecidos como fuertes han sido extraídas.

A la vista de estos resultados se puede observar que la utilización de contraseñas que consisten en palabras o palabras con el intercambio de letras por números pueden llegar a ser muy débiles. Además, también se puede observar como las contraseñas de gran longitud que consisten en combinaciones de letras, números y símbolos sin ninguna relación son muy seguras, ya que no se ha conseguido extraer ninguna de ellas. Sin embargo, conviene recordar que se está utilizando un diccionario muy pequeño, por lo que es posible que con la utilización de otros diccionarios se obtuvieran más contraseñas.

Un ejemplo de la utilización de este programa para la comprobación de la contraseña ha sido utilizando el comando del cuadro 8.1. Con la utilización de este comando se comprobó las contraseñas del servicio de FTP. El resultado obtenido se puede observar en la imagen 8.1.

```
hydra -L diccionario.txt -P diccionario.txt 192.168.1.6
ftps -f
```

Cuadro 8.1: Ejemplo de utilización de `Hydra`. En este comando se realiza un ataque con el archivo *diccionario.txt* como diccionario, realizando el ataque al servicio FTP del equipo *192.168.1.6*.

Además de este tipo de ataque por diccionario también existen ataques por fuerza bruta, estos consisten en ir probando todos los usuarios y contraseñas posibles combinando los diferentes caracteres imprimibles que tiene un ordenador. Este tipo de ataques no se suele utilizar ya que es muy lento y usualmente los administradores de los equipos suelen darse cuenta de que se están tratando de averiguar las contraseñas con este tipo de ataque. De esta manera, también se puede demostrar que las contraseñas de mayor longitud añaden seguridad a los servicios.

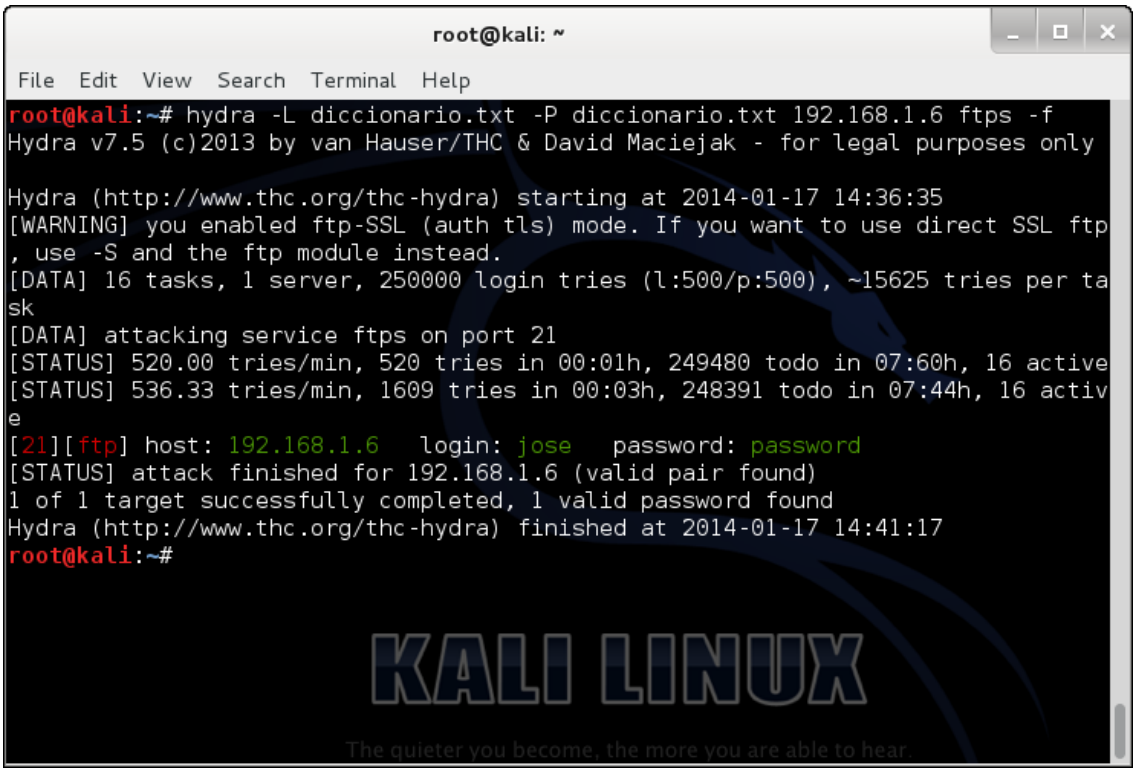

Figura 8.1: Resultado de ataque por diccionario a FTP. Se puede observar que `Hydra` obtiene los credenciales de *jose/password* como usuario/contraseña.

8.4. Test de penetración

En esta parte del documento se explicarán los diferentes procedimientos realizados en el proceso del *Test de Penetración*. Para la realización del mismo se utilizará una distribución de `Kali`™, para los detalles acerca de sus características se puede consultar el apéndice B.1.

8.4.1. Recopilación de información

En este proyecto, no se realizará la fase completa, puesto que no se cuenta con alojamientos en internet, por lo que no se puede obtener ninguna información a través de éste. Por lo tanto, se partirá de la dirección de la página web y se tendrá en cuenta que se ha deducido que la información más sensible se encuentra en la base de datos, así como que se trata de una empresa de tamaño medio. Esta información se podría haber obtenido de forma simple a través de la propia página de la empresa observando el tipo de empresa que es.

Por lo tanto, se trata de averiguar toda la información posible acerca de la red a partir de la página web. Para ello a través del comando del cuadro 8.2, con la utilización de *traceroute* averiguamos cuales son los diferentes *routers* por los que pasan los paquetes que se envían a la página web, así como la dirección del servidor donde se aloja la página web. El resultado obtenido se muestra en la figura 8.2.

```
traceroute www.pfc.com
```

Cuadro 8.2: Comando para utilizar traceroute a la página web de la empresa.

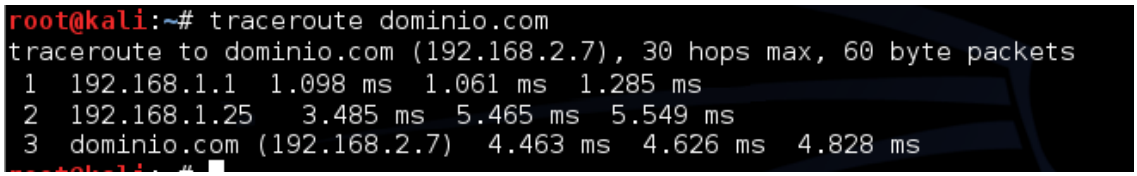

Figura 8.2: Resultado de traceroute a la página web. En la imagen se pueden observar los diferentes *routers* que atraviesan los paquetes desde el equipo que ejecuta el comando hasta la página web de la empresa.

A partir de estos resultados, se puede observar que los paquetes atraviesan dos *routers* que pertenecen a la red privada de la empresa, ya que se puede observar que acaban los diferentes *routers* públicos, inexistentes en este caso por no realizarse el ataque desde internet. Por lo tanto, se averigua que tanto el *router* de dirección IP *192.168.1.1* como el de dirección IP *192.168.1.25* son *routers* de la empresa.

Una vez conocidas las direcciones IP de los diferentes *routers* de la empresa, se trata de averiguar el tamaño de la red de la empresa. Finalmente, se opta por establecer que las redes de la empresa son dos redes de clase C. La elección de este tamaño de red se debe a dos razones: con la información obtenida en internet se sabe que se trata de una empresa pequeña, y, también, es el tamaño de red más utilizado para redes de tamaño medio.

Por lo tanto, después de los procedimientos explicados ya se conocerían cuales son las redes a analizar, siendo las mismas: *192.168.1.0/24* y *192.168.2.0/24*.

8.4.2. Análisis de vulnerabilidades

Debido a que se cuenta con un *firewall*, se realizarán tres escáneres de vulnerabilidades diferentes, uno desde el exterior de la red, como un atacante real, y otros dos desde ambas zonas del interior de la red. La realización de estos diferentes análisis se debe a la necesidad de comprobar la seguridad de los diferentes elementos desde los diferentes puntos de la red, ya que pueden existir ataques desde cualquier punto de la red.

Para la realización de estos análisis se utilizará la herramienta `Nessus`™, cuyo funcionamiento se explicará en el apéndice B.2. A partir de esta herramienta, y utilizando como objetivo las redes extraídas en la fase de *Recopilación de la Información*. Se tratará de encontrar todas las vulnerabilidades existentes.

Observando los informes, los cuales se pueden consultar en el apéndice D, se puede ver que están organizados agrupando las vulnerabilidades por equipo, y además, éstas constan de un código de colores para poder identificar fácilmente la severidad de las mismas.

Asimismo, se pueden observar grandes diferencias entre los diferentes análisis realizados. Estas diferencias se deben a la existencia de los *firewall* que separan ambas redes de internet y entre ellas. Como se especificó anteriormente, la zona privada de la red solo debe ser accesible desde el interior de la misma, mientras que la zona pública de la red puede ser accedida desde cualquier punto de la red, ya que se encuentran los diferentes servicios que necesitan acceso público.

Esta configuración se puede observar en los diferentes informes de los análisis. Al comparar los diferentes informes se puede observar como únicamente en el análisis desde el interior de la red se pueden observar vulnerabilidades en la misma. En el resto no se muestran los equipos de la red interna debido a que se bloquea el tráfico a esa red por cuestiones de seguridad y política de la empresa.

Por otro lado, se puede observar como la parte pública de la red es accesible desde cualquier punto, por lo que aparecen sus vulnerabilidades en los diferentes informes.

Una vez realizados estos análisis se deben de comprobar las vulnerabilidades existentes en los mismos, teniendo en cuenta que las vulnerabilidades que aparecen en el informe realizado desde el exterior de la red son

las más importantes, puesto que se pueden aprovechar las mismas desde cualquier punto de la red.

8.4.3. Explotación

En esta parte del proceso se comprueban las diferentes vulnerabilidades que aparecen en los análisis, tratando de conseguir toda la información posible de la red e incluso el control de alguno de los equipos a través de ellas.

Al observar los diferentes análisis podemos observar que no existen un gran número de vulnerabilidades en los diferentes equipos, a excepción del equipo con dirección IP *192.168.2.105*. Este equipo corresponde a uno de los clientes de la empresa que se encontraba conectado a la red en el momento del análisis, por lo tanto, no se analizarán las vulnerabilidades de este equipo en profundidad. Sino que únicamente se realizará un análisis superficial explicando como pueden afectar a la propia red de la empresa.

Al observar los análisis de seguridad, obviando el equipo del cliente, podemos observar que la mayoría de vulnerabilidades existentes son de información, en color azul, es decir, que únicamente son vulnerabilidades que permiten obtener algo de información acerca del equipo o de los servicios que provee el mismo. A través de estas vulnerabilidades se puede conocer los diferentes servicios que existen en los equipos, éstas no son muy importantes, puesto que gran parte de esta información es conocida por los usuarios de la red. Sin embargo, también pueden ser peligrosas puesto que proporcionan información a un posible atacante que podría facilitar los ataques.

Las siguientes vulnerabilidades con mayor severidad son las catalogadas con riesgo bajo, en color verde. Las existentes de esta categoría advierten de dos problemas existentes:

- Problemas de utilización de cifrados de tipo RC4, que permiten que si un usuario captura una gran cantidad de tráfico en texto plano cifrado pueda ser capaz de descifrar obteniendo el texto enviado. Esta vulnerabilidad se debe tener en cuenta, sin embargo, no es muy importante debido a que la cantidad de tráfico que se debe capturar debe tener un formato específico, además, es necesario capturar una gran cantidad de tráfico para aprovechar esta vulnerabilidad.
- Problemas que permiten una autenticación sin cifrar. Esta vulnerabilidad aparece tanto en el servidor web como en el servidor FTP de la zona de invitados ya que ambos permiten una autenticación en texto plano. Esta vulnerabilidad es inevitable, ya que en la política de la empresa se especifica que se debe poder realizar estas conexiones sin cifrar.

Posteriormente, en el informe están las vulnerabilidades catalogadas como de riesgo medio. En esta categoría están especificadas las siguientes:

- Los certificados utilizados en los cifrados no son seguros puesto que son autofirmados. Esta vulnerabilidad se debe a que al tratarse de un caso hipotético no se cuenta con una entidad certificadora segura que pueda proveer unos certificados confiables.
- mDNS Detection: permite extraer información acerca del equipo en el que se encuentra. Esta vulnerabilidad es importante debido a que permite conocer datos específicos del equipo tales como el sistema operativo con su versión exacta y una lista de los servicios. Esto es muy peligroso ya que existen páginas que cuentan con listas de las vulnerabilidades y la forma de explotarlas de cada sistema operativo. Por lo tanto, podría aprovecharse esta información para conocer alguna error de seguridad que pueda no aparecer en el análisis.
- Existe una vulnerabilidad que permite obtener información acerca de el servicio de PHP instalado en el equipo. Esta información permite realizar ataques específicos que vulneren la versión de PHP instalada, al igual que la anterior.
- Vulnerabilidad que permite un ataque XSS a través del cual se podría inyectar código para que sea ejecutado en el entorno de seguridad de la página afectada. De esta manera, se podría ejecutar código malicioso

con el que se podría llegar a conseguir todos los datos de la base de datos de la página o incluso eliminarlos o modificarlos.

- Se permiten conexiones al servidor FTP de forma anónima. Esta vulnerabilidad existe puesto que se permiten conexiones anónimas al servidor FTP de la zona de invitados, ya que está establecido de esta manera en las políticas de la empresa.
- Existe una vulnerabilidad que permite un ataque conocido como *Man in the middle*. A través de este ataque, se puede interceptar el tráfico que se dirige al servidor Samba.

Por último, existe una vulnerabilidad crítica en el cliente Windows™. Esta permite que se realice un bloqueo de este equipo. Además, es posible que permita que se ejecute código en equipo afectado, aunque en la actualidad no se conoce la forma de aprovecharla para esto.

Una vez analizadas las diferentes vulnerabilidades de los equipos de la red empresarial podemos observar que no existe ninguna que permita conseguir el control de ninguno de los equipos de forma rápida. Sin embargo, el equipo del cliente invitado si que cuenta con algunas de estar vulnerabilidades, por lo que se tratará de vulnerar los equipos de la red empresarial aprovechando el equipo del cliente.

Para tomar el control del equipo del cliente se ha decidido utilizar la vulnerabilidad del servidor Samba, con la que, gracias a `Metasploit`™, podemos conseguir una consola con permisos de administrador en el equipo del cliente.

Para aprovechar la vulnerabilidad se utilizará el exploit especificado en el cuadro 8.3, así como del *payload* indicado en el cuadro 8.4.

```
use exploit/multi/samba/usermap_script
```

Cuadro 8.3: Exploit utilizado para vulnerar el equipo.

```
set PAYLOAD cmd/unix/reverse
```

Cuadro 8.4: Payload utilizada para vulnerar el equipo.

A través de estos dos elementos, utilizando el equipo del cliente como equipo a atacar, conseguimos una consola en el equipo del cliente, tal como se puede observar en la imagen 8.3.

Una vez que se tiene esta consola se trata de averiguar información que pueda afectar a la empresa. En este caso a través de esta consola se consigue acceder a un archivo donde el usuario del equipo ha guardado sus credenciales para conectar con la base de datos de la página web, debido a que tiene acceso a la misma para colocar publicidad en la página web.

Una vez localizados estos credenciales se realiza una conexión con la base de datos de la página web, y se observa que se pueden obtener un gran número de datos de la misma. Además, también se permite eliminar contenido de la misma, por lo que existiría una gran vulnerabilidad en la red empresarial a través del equipo del cliente. Estos resultados se pueden observar en la imagen 8.4.

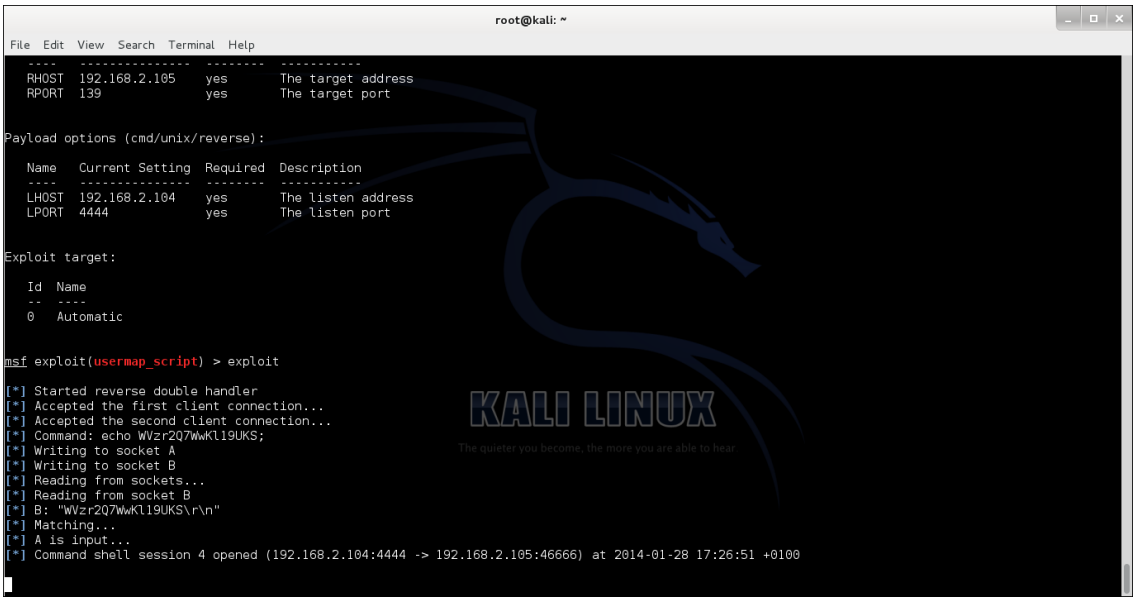

Figura 8.3: Consola remota del equipo del cliente tras la explotación. Se puede observar como se consigue una explotación con éxito y se consigue una consola en el equipo atacado.

Figura 8.4: Información visible de la base de datos de la página web.

9 Reporte de resultados

En este capítulo se mostrarán los resultados obtenidos en la realización del auditoría. Para ello, se presentarán varios documentos diferentes, en éstos se especificarán las medidas que se deben de tomar para cumplir correctamente con la normativa oficial, así como las diferentes vulnerabilidades existentes y como corregirlas. En los diferentes informes se realizará un resumen con sus soluciones de los incumplimientos de normativa o vulnerabilidades, para poder verlos en detalle se debe referir a la revisión de la normativa o a los informes de los análisis respectivamente.

Estos documentos serán los informes a presentar al cliente junto con el presupuesto. También, en caso de solicitarlo se le presentarían los informes de Nessus™ del apéndice D como informes técnicos junto con el apartado de revisión de la normativa.

9.1. Informe del cumplimiento de la normativa

En este informe se presentarán los diferentes incumplimientos de la normativa junto con las diferentes medidas que se deben realizar para corregir los mismos. estas son:

- Incumplimientos de normativa por no existir documentación. Se debe realizar documentación en la que se especifiquen los siguientes aspectos:
  - Uso correcto de los equipos y responsabilidades por el cumplimiento o violación de estas normas.
  - Como realizar las tareas habituales y que hacer en caso de situación anómala.
  - Procesos de autorización para la utilización de los diferentes servicios.
  - Riesgos existentes en los sistemas y seguridad de la red. Pudiéndose utilizar los informes de la presente auditoría para esta documentación.
  - Análisis de impacto de un breve fallo en alguno de los servicios.
- Incumplimientos de la normativa por no utilizar cifrado en todos los servicios. Se debe añadir cifrado en algunos servicios como Samba, ya que algunos no utilizan cifrados.
- Se debe realizar un control de las actividades de los usuarios para controlar las actividades indebidas.
- Es necesario añadir un método de detección y reacción frente a código dañino, así como un control de los incidentes de seguridad que se produzcan.
- Se debe añadir mecanismos de copia de seguridad de los diferentes servidores, puesto que no existe ninguno.
- Hay que establecer una política de actualización de los servicios.
- Las administraciones críticas deben de ser realizadas por al menos dos usuarios, por lo que habría que crear nuevos administradores en los servicios.
- Se debe crear un método para catalogar la información.

- Habría que contratar una entidad certificadora para obtener certificados confiables.
- Hay que crear un sistema de firma digital y de eliminación de los metadatos de los diferentes archivos.
- Se deben instalar sistemas de protección de protección frente a virus, troyanos u otros *malware* en el servidor de correo electrónico. Además, también se debe incluir un sistema de prevención frente a los ataques de denegación de servicios.

9.2. Informe de la seguridad física

En este informe se presentarán los diferentes problemas de seguridad física, así como la manera de corregirlos. Estos problemas existentes son:

- No existe un control de acceso a los servidores.
  - Se debe incluir un control de acceso a los servidores permitiendo únicamente el acceso a los mismos a los administradores con permisos.
- El control de identificación de empleados utiliza un código y una contraseña, por lo que cualquier usuario podría utilizar los credenciales de otro.
  - Es necesario aumentar el control en estos sistemas, ya sea mediante la implantación de controles biométricos, como huella dactilar, o bien mediante la utilización de elementos físicos como tarjetas de empleado. Sin embargo, con esta última medida sigue existiendo la probabilidad de que se produzca un robo de la identificación y, por lo tanto, una brecha de seguridad.

9.3. Informe de la seguridad de usuario

En este informe se presentarán los diferentes problemas de la seguridad de usuarios, así como sus soluciones. Estos problemas son:

- Las políticas de establecimiento de contraseñas permiten la utilización de contraseñas muy débiles. Además, no existe ninguna caducidad de las mismas pudiendo utilizar siempre la misma contraseña.
  - Es necesario cambiar las políticas de contraseñas de los diferentes sistemas para que no permitan la utilización de contraseñas débiles, asimismo, también es recomendable añadir caducidad a las mismas. Puesto que los diferentes servicios utilizan las cuentas del sistema operativo como cuentas de los servicios, para cambiar estas políticas se debe modificar la política del sistema, la cual se controla a través del archivo indicado en el cuadro 9.1.

/etc/pam.d/common-password

Cuadro 9.1: Archivo con las políticas de contraseñas en Ubuntu™.

- Algunos de los empleados guardan sus contraseñas en archivos de los equipos o en medios físicos en sus entornos de trabajo.
  - Debido a que este problema de seguridad se produce por la conducta de los empleados, se recomienda desarrollar alguna charla de concienciación acerca de la importancia de esta actuación para evitarla.
- Existen contraseñas débiles y se permite la repetición de las contraseñas en diferentes servicios. Incluso ha sido posible encontrar los credenciales de diferentes cuentas de usuario con la utilización de ataques

por diccionario con la utilización de un diccionario muy reducido.

- Se debe realizar un cambio general de contraseñas tras el cambio en las políticas de las mismas, para que de esta manera se utilicen contraseñas seguras. Además, es aconsejable instruir a los trabajadores de la importancia de utilizar diferentes contraseñas para los diferentes servicios, siendo estas además complejas.

9.4. Informe de vulnerabilidades

En este informe se presentarán las diferentes vulnerabilidades existentes en la red empresarial, junto a una apreciación de la gravedad se encontrará como corregir esa vulnerabilidad.

Inicialmente se comenzará explicando la importancia de los diferentes análisis y posteriormente se expondrán las diferentes vulnerabilidades y sus soluciones.

En el proceso se han realizado tres análisis diferentes desde diferentes puntos de la red. Estos corresponden con: exterior de la red, zona pública de la red y zona privada de la red.

En los tres análisis, además de los equipos propios de la red empresarial, se ha encontrado el equipo de uno de los clientes conectados a la red para invitados. Este equipo es el que tiene la dirección IP *192.168.2.105*. Debido a que no forma parte de la red empresarial no se tiene en cuenta, excepto para tratar de aprovechar sus vulnerabilidades para acceder a la red empresarial.

A través del análisis del exterior de la red podemos ver cuales son las vulnerabilidades que expondrían más a la red, puesto que pueden ser explotadas desde cualquier punto de internet. En éste se comprueba que no hay vulnerabilidades en la zona privada de la red, ya que no se ha sido capaz de establecer siquiera si existe algún equipo en esta red. Sin embargo, la zona pública de la red si contiene vulnerabilidades puesto que esa zona no se protege por el *firewall* tal como se especifica en la política de la empresa.

En el informe desde la zona pública de la red se pueden observar las mismas vulnerabilidades que en el informe desde el exterior. Esto se debe a que, al igual que el *firewall* exterior, el existente entre ambas redes protege correctamente la zona privada de la red. Sin embargo, al igual que en el análisis desde el exterior de la red, existen diferentes vulnerabilidades en los equipos de la zona pública de la red. Las existentes en este análisis toman bastante importancia, puesto que cualquier persona con acceso a una conexión en la red de invitados podría aprovecharlas.

Con el análisis desde la zona privada de la red se pueden ver todas las vulnerabilidades existentes. Esto se debe a que debido a las políticas de seguridad el *firewall* no bloquea ninguna conexión a la zona pública de la red para realizar configuraciones, por lo que todas las vulnerabilidades existentes en esta zona pueden ser explotadas desde la zona privada de la red. Asimismo, debido a que las conexiones entre la zona privada de la red no atraviesan ningún *firewall* no son filtradas, por lo que cualquier vulnerabilidad existente podrá ser explotada. Debido a esto, en este análisis se muestran todas las vulnerabilidades de la red empresarial. Éstas cobran mucha importancia puesto que afectan a todos los servicios de la red, incluyendo los más importantes como la base de datos de la empresa. Sin embargo, estas vulnerabilidades solo pueden ser explotadas desde la zona privada de la red, por lo que si se protege el acceso a la zona de trabajo, únicamente los diferentes trabajadores podrán explotar estas vulnerabilidades, aunque no deben perder importancia por este hecho.

Una vez analizada la importancia de los diferentes análisis y su función, se procede a exponer las diferentes vulnerabilidades y sus soluciones. Éstas se tratarán por grupos, ya que un gran número de ellas aparecen de forma repetida en diferentes equipos o tienen unas características muy similares. Se organizarán de mayor a menor gravedad teniendo en cuenta además la zona de la red en la que se encuentre:

Vulnerabilidades criticas: conllevan un gran peligro en las redes. Esto se debe a que las vulnerabilidades críticas permiten desde ejecutar código en el equipo de forma remota hasta conseguir una consola del

mismo.

- A excepción del equipo del cliente solo existe una vulnerabilidad crítica. Esta vulnerabilidad se encuentra en el equipo con Windows™ de la red privada, es decir, el equipo de un trabajador. A pesar de ser una vulnerabilidad crítica no conlleva mucho peligro puesto que en la actualidad no se conoce forma de ejecutar código remoto, sino únicamente de detener el servicio de DNS del equipo afectado.
  - Para solucionar esta vulnerabilidad solo es necesario realizar las actualizaciones de Windows™.

Vulnerabilidades medias: no presentan un peligro muy alto, puesto que normalmente no permiten obtener un gran provecho de las mismas de forma rápida. Sin embargo, es posible que con estas vulnerabilidades se consiga acceso completo al equipo afectado. Las vulnerabilidades existentes son:

- *SMB Signing Disabled*: esta vulnerabilidad se debe a una configuración no completamente segura de Samba. Es posible hacer un ataque conocido como *Man in the middle*, permitiendo interceptar el tráfico entre un cliente y el servidor Samba.
  - Se debe obligar que se realice un proceso conocido como *saludo* entre el cliente y el servidor, haciendo que no sea posible este tipo de ataque.
- Certificados SSL: Este grupo de vulnerabilidades avisan de los diferentes problemas existentes debido a los certificados utilizados. Pues que los certificados son autofirmados una parte de estas vulnerabilidades no se puede eliminar.
  - Contratar una entidad certificadora que proporcione certificados SSL seguros y con un cifrado complejo.
- *mDNS Detection*: esta vulnerabilidad permite que se obtenga información acerca del servidor como el sistema operativo y la versión exacta del mismo. Esta vulnerabilidad no permite un control del equipo, pero al conocer la versión del sistema operativo se pueden encontrar otras vulnerabilidades de ese sistema no detectadas por el escáner.
  - Filtrar el tráfico UDP al puerto 5353.
- *PHP Information Disclosure*: esta vulnerabilidad permite que con una dirección específica se pueda conseguir información acerca del servicio de PHP instalado en el equipo. Esta vulnerabilidad lo único que permite es la obtención de información, sin embargo, debido a que PHP puede contener errores en alguna versión concreta, es posible aprovechar esta información para atacar un equipo.
  - Se debe cambiar el valor de *expose_php* a *Off* en el fichero de configuración *php.ini*.
- *Joomla libraries XSS*: debido a que `Joomla™` no es capaz de establecer una correcta configuración para el parámetro de lenguaje, existe una vulnerabilidad. A través de esta vulnerabilidad, un atacante podría ser capaz de ejecutar código HTML o *scripts* en el equipo afectado.
  - No existe una corrección en la actualidad por lo que se recomienda eliminar el módulo.

Vulnerabilidades bajas: pueden aprovecharse para realizar un ataque a un equipo, pero usualmente no conllevan un gran riesgo por que no se pueden aprovechar directamente, sino que hacen falta otras situaciones para poder aprovecharlas.

- Certificados SSL y cifrado: este conjunto de vulnerabilidades se repite en varios equipos. Estas vulnerabilidad solo indican que se utilizan cifrados RC4 que pueden ser peligrosos, también se informa de la utilización de certificados con claves de poca longitud.
  - Cambiar la configuración del cifrado para evitar la utilización de cifrados RC4 y cambiar los certificados para que utilicen claves de mayor longitud.
- Autenticación en texto plano: esta vulnerabilidad, existente en el servidor web, indica que se transmiten credenciales de usuario de la página en texto plano. Esto hace que un usuario que se encuentre en la misma red pueda capturar el tráfico y averiguar los credenciales de los usuarios que conecten.

- Asegurarse de que toda la información sensible como los credenciales de usuario se transmiten a través de HTTPS.

Vulnerabilidades de información: no son muy importantes, ya que solo ofrecen información acerca del equipo que tiene la vulnerabilidad. Esta información son datos como los servicios que tiene un equipo, que ya se conoce puesto que se debe saber donde están los diferentes servidores para poder utilizarlos.

- Existe un gran número de vulnerabilidades de este tipo, pero puesto que no conllevan peligro y que son muy similares no se tratan en detalle.
  - Algunas de estas vulnerabilidades no es posible evitarlas debido a que son por tener los servicios activos. El resto se pueden evitar cambiando la configuración de los servidores.

Vulnerabilidades inevitables por la política: existen debido a la política establecida por la empresa. Para poder corregir estas vulnerabilidades habría que cambiar la política de la empresa.

- *Anonymous FTP Enabled*: debido a que se requiere un servidor de archivos con acceso desde cualquier punto de la red, es necesario que se permitan conexiones anónimas.
- *FTP Supports Clear Text Authentication*: debido a que se requiere un servidor FTP accesible por todo el mundo, se permiten conexiones sin cifrar, puesto que muchos usuarios de la red no tienen los conocimientos informáticos suficientes para utilizar conexiones cifradas. Por lo tanto, para permitir un acceso desde cualquier punto de la red se permiten conexiones sin cifrar.
- *DHCP Server Detection*: esta vulnerabilidad únicamente indica que se ha encontrado un servidor DHCP en este equipo. Esta vulnerabilidad no implica peligro, pero puede ser aprovechada por un atacante para conocer la topología de la red en la que se encuentra.
- *IP Forwarding Enabled*: esta vulnerabilidad indica que existe un equipo que realiza reenvío de paquetes, esto se debe a que se utiliza este equipo como *router* de enlace entre ambas zonas de la red empresarial, por lo que es necesario que reenvíe los paquetes de una red a otra.

Bibliografía

[1] CUPS. Available from: http://www.cups.org. 2.4.13

[2] Domain Names - Implementation and Specification - RFC 1035. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc1035.txt. 2.4.2

[3] Dynamic Host Configuration Protocol (DHCP) - RFC 2131. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc2131.txt. 2.4.3

[4] File Transfer Protocol (FTP) - RFC 959. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc959.txt. 2.4.4

[5] Hypertext Markup Language - 2.0 - RFC 1866. Technical report, IETF. Available from: http://tools.ietf.org/html/rfc1866. 2.4.6

[6] Hypertext Transfer Protocol - HTTP/1.1 - RFC 2616. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc2616.txt. 2.4.5

[7] Internet Message Acces Protocol - Version 4rev1 (IMAP4) - RFC 3501. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc3501.txt. 2.4.11

[8] Joomla. Available from: http://www.joomla.org. A.2.4

[9] Kali Linux. Available from: http://www.kali.org/. B.1

[10] Manual de Hydra. Available from: https://www.thc.org/thc-hydra. B.4.2

[11] Metasploit. Available from: http://www.metasploit.com/. B.3.2

[12] PHP. Available from: http://www.php.net. 2.4.7

[13] Post Office Protocol - Version 3 (POP3) - RFC 1939. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc1939.txt. 2.4.10

[14] ProFTPD. Available from: http://www.proftpd.org. A.1.1

[15] Samba. Available from: http://www.samba.org. 2.4.12

[16] Simple Mail Transfer Protocol (SMTP) - RFC 2821. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc2821.txt. 2.4.9

[17] TCP/IP - RFC 1180. Technical report, IETF. Available from: http://www.ietf.org/rfc/rfc1180.txt. 2.4.1

[18] The Secure Sockets Layer (SSL) Protocol Version 3.0 - RFC 5246. Technical report, IETF. Available from: http://tools.ietf.org/html/rfc5246. 2.4.14

[19] Detección de APTs, Mayo 2013. Available from: http://www.inteco.es/Estudios/deteccion_apts. 2.2

[20] Marta Barceló and Pete Herzog. *The Open Source Security Testing Methodology Manual 3*. ISECOM, 2010. 2.5

[21] B.O.E. Administración electrónica. Esquema Nacional de Seguridad. Technical report, Agencia Estatal, 2010. 1.1, 2.3, 8.1

[22] Gerald Carter, Jay Ts, and Robert Eckstein. *Usign Samba*. O'Reilly Media Inc., 2007. 2.4.12, A.5.1

[23] CisoLabs. 2013 Cisco Annual Security Report. Technical report, Cisco System Inc., 2013. 2.2

[24] Kyle D. Dent. *Postfix: The Definitive Guide*. O'Reilly Media Inc., 2003. A.3.1

[25] David Keneddy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. *Metasploit: The Penetration Tester's Guide*. No Starch Press Inc., 2011. 7.4

[26] Olaf Kirch and Terry Dawson. *Guía de Administración de Redes con Linux*. O'Reilly Media Inc., 2000. 4

[27] Ben Laurie and Peter Laurie. *Apache: The Definitive Guide*. O'Reilly Media Inc., 2002. A.2.1

[28] Regina Obe and Leo Hsu. *PostgreSQL: Up and Running*. O'Reilly Media Inc., 2012. A.4.3

[29] Gregor N. Purdy. *Linux iptables Pocket Reference*. O'Reilly Media Inc., 2004. 5.4.3

[30] Microsoft TechNet. Diseñar la red. Available from: http://technet.microsoft.com/es-es/library/dd568932.aspx. 2.1

[31] Redacción Redes Telecom. Los ataques contra empresas españolas se multiplican, Novimebre 2013. Available from: http://www.redestelecom.es/seguridad/noticias/1070885002503/ataques-empresas-espanolas-multiplican.1.html. 2.2

[32] TrendLabs. TrendLabsSM 3Q 2013 Security Roundup. Technical report, Trend Micro, 2013. 2.2

[33] Zwicky, Elizabeth D., Cooper, Simon, Chapman, and D. Brent. *Building Internet Firewalls*. O'Reilly Media Inc., 2000. 5.4.3

IV

Apéndices

A

Instalación completa de los servicios

En este apéndice se especificarán los procesos de instalación y configuración de los diferentes servicios proporcionados por la red. También, se especificarán las configuraciones necesarias para que los diferentes clientes puedan disfrutar de todos los servicios proporcionados por la red correctamente.

A.1. Servidor de archivos: FTP

Para el servidor de archivos se especificó que se utilizaría el servidor ProFTPD™ para proporcionar este servicio. Ambos servidores de archivos se configurarán prácticamente de la misma manera, la única excepción será que mientras que el servidor FTP privado únicamente permitirá conexiones cifradas mediante SSL, el servidor FTP para clientes e invitados aceptará tanto conexiones SSL como conexiones sin cifrar.

A.1.1. Instalación FTP genérica

Para instalar este servidor se utilizarán los repositorios de paquetes propios de Ubuntu™ para asegurar que se trata se software oficial. Para instalar el servidor se procede a instalar el paquete de proftpd con el comando del cuadro A.1.

```
apt-get install proftp-basic
```

Cuadro A.1: Comando para instalar el paquete ProFTPD™.

Después de instalar este paquete ya se tendría el servidor ProFTPD™ instalado, pero se tendrá que configurar correctamente. Para ello se tendrá que cambiar su archivo de configuración, la localización de este archivo se especifica en el cuadro A.2.

```
/etc/proftp/proftpd.conf
```

Cuadro A.2: Ruta al archivo de configuración de ProFTPD™ en Ubuntu™.

En este archivo se encuentra gran parte de la configuración del servidor, encontrándose el resto de la configuración en diferentes archivos del mismo directorio.

En este caso se deja una configuración muy similar a la predeterminada, a excepción de algunos pequeños cambios. Estos cambios son:

- Se elimina la marca de comentario de la línea “DefaultRoot ~”. De esta manera se evita que un usuario pueda acceder a archivos fuera de su carpeta personal cuando conecte con el servidor.
- Se elimina la marca de comentario de la línea “Include /etc/proftpd/tls.conf”. De esta manera se hace que el servidor incluya en su configuración el archivo “tls.conf”, al realizar este cambio si se configura correctamente el archivo “tls.conf” se podría conectar al servidor mediante SSL.

Posteriormente, debido a que se han activado las conexiones con cifrado SSL se debe realizar su configuración. Para configurarlo correctamente se tiene que modificar el archivo cuya ruta se especifica en el cuadro A.3.

```
/etc/proftpd/tls.conf
```

Cuadro A.3: Ruta al archivo de configuración para SSL de ProFTPD™ en Ubuntu™.

En este archivo se deberá configurar los diferentes certificados que se utilizarán entre otros aspectos, para ello se tiene que eliminar la marca de comentario de las siguientes líneas:

- TLSEngine
- TLSLog
- TLSProtocol
- TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
- TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key
- TLSVerifyClient off

De esta manera se especificaría que se utilice SSL y los diferentes certificados y claves que utilizará para el cifrado.

Posteriormente, debido a que para utilizar SSL se necesita la clave y el certificado, habrá que crearlos. Puesto que se trata de una simulación se utilizará un certificado propio auto-firmado. Para crear este certificado se utiliza el comando especificado en el cuadro A.4.

```
openssl req -x509 -newkey rsa:1024 -keyout
/etc/ssl/private/ proftpd.key -out /etc/ssl/certs/proftpd.crt
-nodes -days 365
```

Cuadro A.4: Comando para crear los certificados para ProFTPD™. Con este comando se crean certificados autofirmados RSA que se utilizarán para ProFTPD™.

Al ejecutar este comando se tendrán que introducir algunos datos de la entidad que firma el certificado, estos datos serán los que se le facilitarán a un usuario que intente conectar y que debe decidir si el certificado es confiable o no. Como los certificados serán auto-firmados se utilizarán datos ficticios de una entidad hipotética. Los datos solicitados se pueden observar en la figura A.1.

Mediante este proceso se tendría una configuración genérica para ambos servidores, pero debido a que su utilización no será la misma, deben tener algunas pequeñas modificaciones en su configuración para que

```
root@ubuntu:/# openssl req -x509 -newkey rsa:1024 -keyout /etc/ssl/private/proft
pd.key -out /etc/ssl/certs/proftpd.crt -nodes -days 365
Generating a 1024 bit RSA private key
....++++++
.........................++++++
writing new private key to '/etc/ssl/private/proftpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SP
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PFC
Organizational Unit Name (eg, section) []:Proyecto
Common Name (e.g. server FQDN or YOUR name) []:dominio.com
Email Address []:postmaster@dominio.com
root@ubuntu:/# _
```

Figura A.1: Captura de pantalla de la creación de certificados para ProFTPD™. En esta imagen se pueden observar las diferentes preguntas que se deben contestar para la creación de los certificados.

cumplan las políticas establecidas.

Para los detalles no especificados a continuación, así como, para obtener más información de ProFTPD™ se debe acceder a su página web oficial [14].

A.1.2. Configuración servidor FTP interno

El servidor FTP se utilizará para compartir archivos entre diferentes empleados y grupos de empleados, estos datos podrán ser información sensible por lo que se tendrá que configurar el sistema de forma segura.

Para el servidor FTP interno se tendrá que configurar que únicamente acepte conexiones cifradas mediante SSL para mantener una seguridad mayor. Para ello se tiene que eliminar la marca de comentario de la línea:

- TLSRequired on

De esta manera el servidor solo aceptará conexiones cifradas mediante SSL impidiendo que se pueda obtener la información de la conexión de forma muy sencilla.

A.1.3. Configuración servidor FTP libre

El servidor FTP libre se utilizará para compartir información entre los diferentes clientes e invitados que se conecten a la red de la zona libre. También se utilizará para compartir archivos con cualquier usuario sin necesidad de identificarse y para poder presentar archivos como listas de precios a través de internet. Por lo tanto, el servidor FTP libre debe aceptar conexiones anónimas. Asimismo, al no conocer el usuario que se conectará al servidor es posible que no disponga de la posibilidad de utilizar conexiones cifradas, por lo que se debe aceptar cualquier tipo de conexión quedando en el usuario que conecta la responsabilidad de utilizar conexiones cifradas o no.

Debido a que en la configuración genérica ya se configura las conexiones cifradas y, por defecto, el servidor

acepta tanto conexiones cifradas como sin cifrar, no se tendrá que realizar ningún cambio para esto. Sin embargo, se tendrá que modificar la configuración del servidor para que permita conexiones anónimas y tenga una zona de compartición de archivos pública.

Para ello se debe realizar un cambio en la configuración. Este cambio consiste en añadir la configuración del usuario anónimo. Estos cambios se deben de realizar en el archivo de configuración indicado en el cuadro A.2 mostrado anteriormente, siendo los cambios a realizar el añadir el código mostrado en el cuadro de código A.1.

```
86   <Anonymous ~ftp>
87     User    ftp
88     Group    nogroup
89     # We want clients to be able to login with "anonymous" as well as "ftp"
90     UserAlias    anonymous ftp
91     # Cosmetic changes, all files belongs to ftp user
92     DirFakeUser on ftp
93     DirFakeGroup on ftp
94
95     RequireValidShell  off
96
97     # Limit the maximum number of anonymous logins
98     MaxClients    10
99
100    # We want 'welcome.msg' displayed at login, and '.message' displayed
101    # in each newly chdired directory.
102    DisplayLogin    welcome.msg
103    DisplayChdir  .message
104
105    # Limit WRITE everywhere in the anonymous chroot
106    <Directory *>
107      <Limit WRITE>
108        Allow 192.168.1.*
109        DenyAll
110      </Limit>
111    </Directory>
112
113  </Anonymous>
```

Código A.1: Código de configuración de ProFTPD™ para el servidor libre.

A.1.4. Creación de cuentas de usuario

Una vez se cuenta con el servidor FTP completamente funcionando, se deben de configurar las diferentes cuentas de usuario que podrán utilizar el servicio.

En este caso, el servidor ProFTPD™ utiliza las cuentas del sistema como cuentas de usuario, es decir, que para crear un usuario del servicio FTP solo se requiere que se cree una cuenta del mismo con contraseña.

Para crear un usuario por lo tanto se tendrán que utilizar los comandos indicados en los cuadros A.5 y A.6. De esta manera, se obtendrá un usuario del servicio FTP cuya carpeta personal será accesible a través del servicio.

```
useradd usuario -m
```

Cuadro A.5: Comando para crear un usuario en Ubuntu™.

```
passwd usuario
```

Cuadro A.6: Comando para establecer una contraseña a un usuario en Ubuntu™.

A.2. Página web

Para establecer la página web de la empresa se especificó que se utilizaría Joomla™. Éste es un sistema de gestión de contenidos que, apoyándose en otras plataformas como Apache™, es capaz de crear y gestionar una página web y todos los aspectos relacionados con la misma. Para ello, Joomla™ debe disponer de acceso a varios servicios en el equipo en el que se instalará el servidor web. Por lo tanto, antes de comenzar la instalación de Joomla™ tendremos que instalar los servicios necesarios para que funcione correctamente. Estos servicios son:

A.2.1. Instalación de Apache

Para alojar la página web creada a través de Joomla™ es necesario disponer de un servidor web, en el caso de Joomla™ está especificado que se debe tratar de un servidor Apache™.

Para instalar Apache™ se utilizarán las librerías de paquetes de Ubuntu™. Para ello se introducirá el comando mostrado en el cuadro A.7.

```
apt-get install apache2
```

Cuadro A.7: Comando para instalar Apache™.

La configuración de Apache™ será la predeterminada, ya que únicamente se utiliza Ubuntu™ para el funcionamiento de Joomla™ y la configuración por defecto es adecuada. Para más detalles acerca de la configuración de Apache™ o de su funcionamiento se puede consultar el libro [27].

A.2.2. Instalación de MySQL

Para que Joomla™ pueda gestionar, tanto los usuarios como los contenidos de la página web, es necesario que disponga de una base de datos. La base de datos utilizada por Joomla™ es MySQL ya que viene establecido que debe ser este tipo de base de datos.

Para instalar la base de datos MySQL se utilizan los comandos mostrados en los cuadros A.8, A.9 y A.10.

Al ejecutar el comando del cuadro A.9 aparecerá una pantalla como la de la figura A.2 en la que se solicita una contraseña para el usuario administrador de la base de datos.

```
apt-get install mysql-server libapache2-mod-auth-mysql
php5-mysql
```

Cuadro A.8: Comando para instalar una base de datos MySQL. A través de este comando se instalan los diferentes paquetes que serán necesarios para el correcto funcionamiento de MySQL.

```
mysql_install_db
```

Cuadro A.9: Comando para instalar y configurar una base de datos MySQL. Mediante la utilización de este comando se comienza un proceso a través del cual se configura la base de datos.

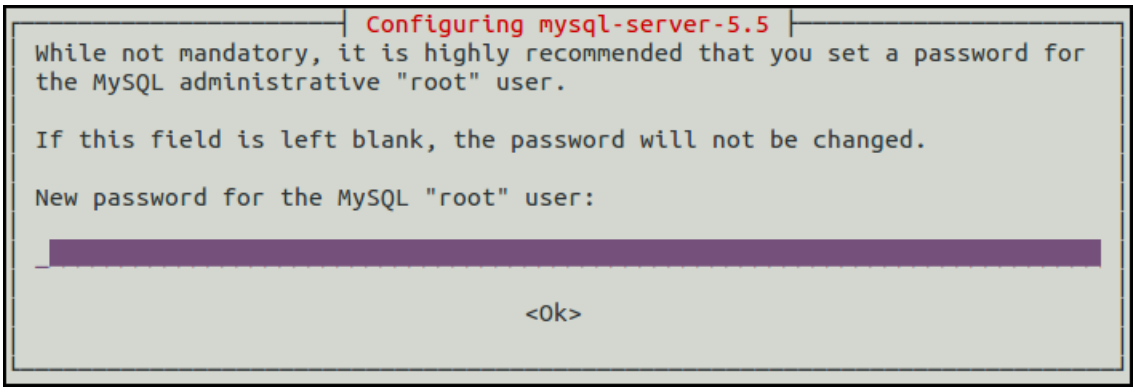

Figura A.2: Captura de pantalla con la petición de contraseña de MySQL. En esta captura se puede observar el cuadro de diálogo donde se solicita la contraseña del usuario “root”.

```
/usr/bin/mysql_secure_installation
```

Cuadro A.10: Comando para configurar una base de datos MySQL. Con este comando se realiza una configuración de la base de datos de forma que quede segura.

Posteriormente, al ejecutar el comando del cuadro A.10 se realizará unas preguntas a través de la consola. Estas preguntas son para una configuración segura de la base de datos, por lo que se contestará que si a todas para que realice los ajustes necesarios para que la base de datos sea segura. Las preguntas que son realizadas se pueden observar en las figuras A.3 y A.4.

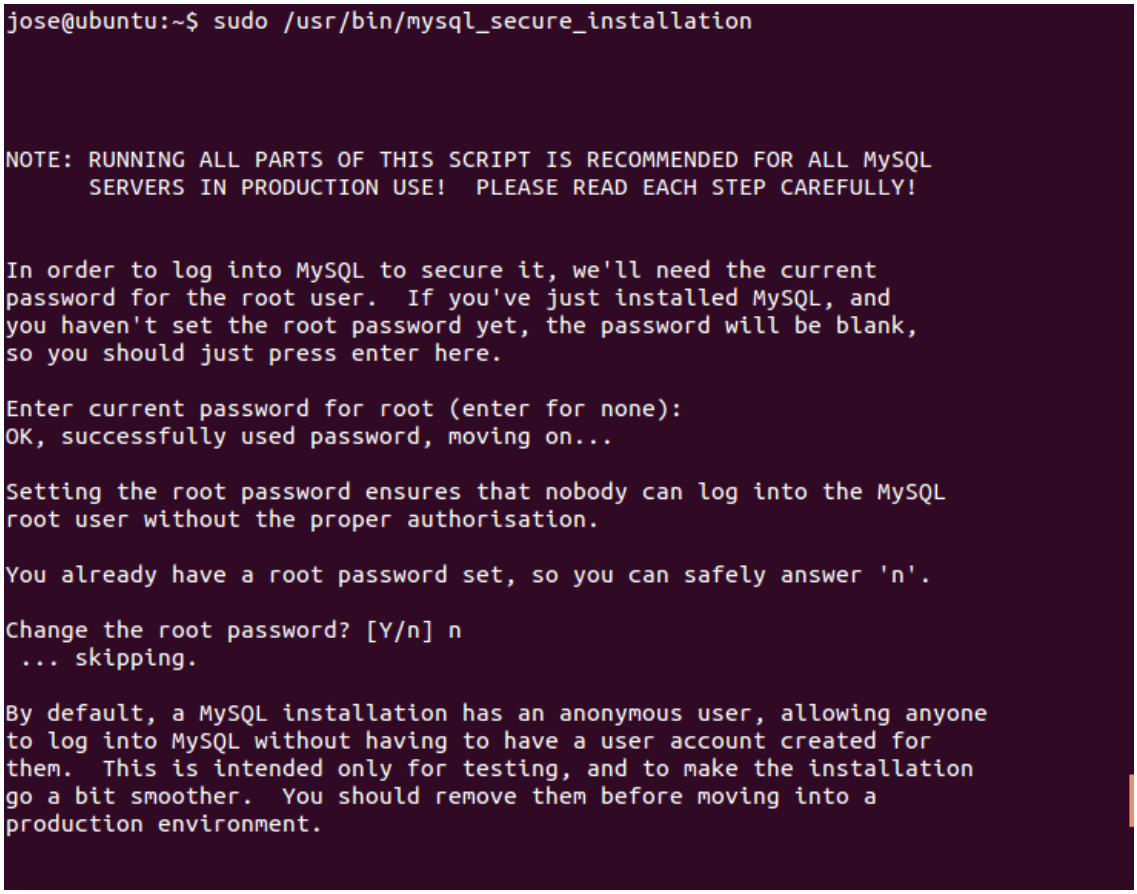

Figura A.3: Captura de pantalla con las preguntas de configuración segura de MySQL.

Con estos comandos lo que se hace es instalar la base de datos y crear una configuración inicial de la misma. Por lo tanto, se requerirán algunos datos para la base de datos y su correcta configuración. Una vez instalada con su usuario la creación de las diferentes tablas será tarea de Joomla™ en su instalación.

A.2.3. Instalación de PHP

Para la creación de la página web Joomla™ utiliza código PHP, por lo que es necesario instalar un servicio de PHP.

Para la instalación de este servicio se utiliza el comando del cuadro A.11.

```
apt-get install php5 libapache2-mod-php5 php5-mcrypt
```

Cuadro A.11: Comando para instalar PHP. Mediante este comando se instalan los paquetes necesarios para el correcto funcionamiento de PHP.

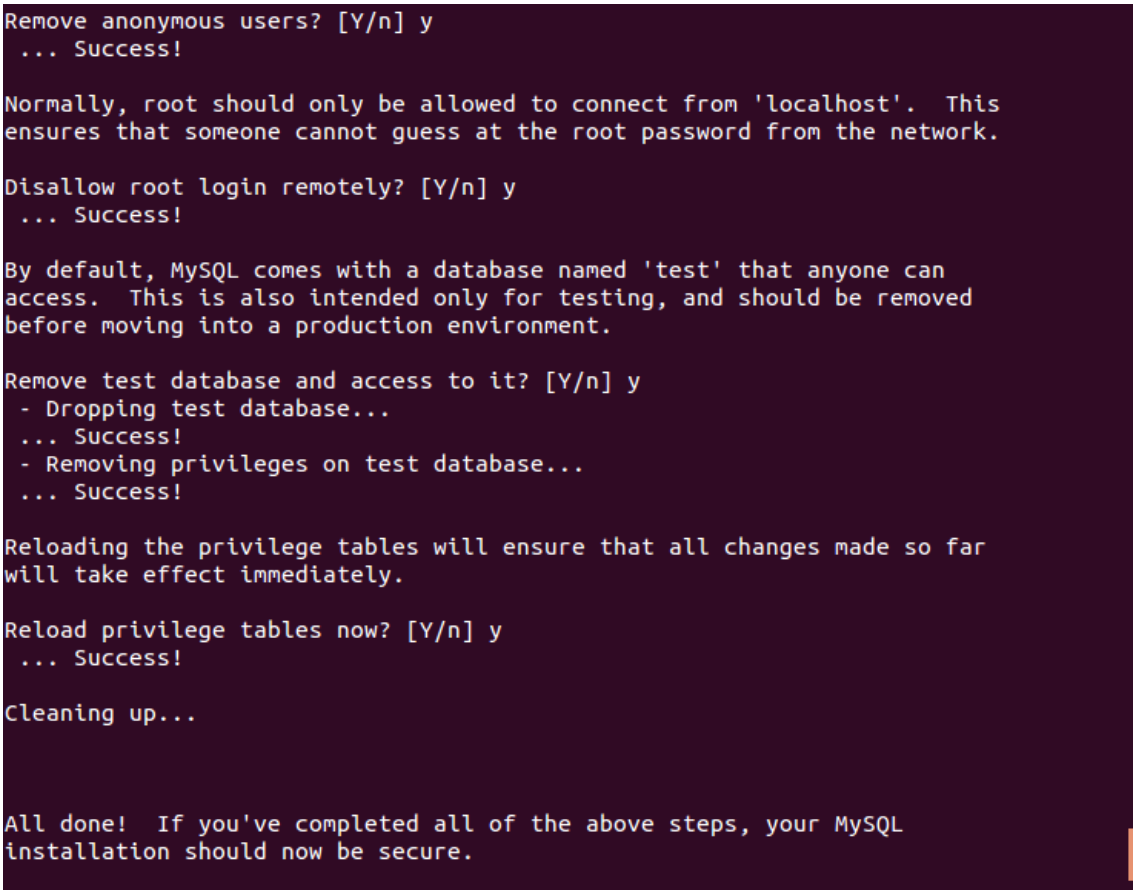

Figura A.4: Captura de pantalla con las preguntas de configuración segura de `MySQL`.

Este servicio tiene una instalación muy básica y no será necesario realizar ninguna configuración extra para que funcione correctamente, por lo que no se realizará ninguna acción extra.

A.2.4. Instalación de Joomla

Una vez instalados estos servicios se procede a la instalación de Joomla™. Para ello se debe acceder a la página oficial de Joomla™ y descargar el paquete de instalación.

www.joomla.org

Cuadro A.12: Página web oficial de Joomla™.

Una vez descargado el paquete de instalación habrá que descomprimirlo en "/var/www", este directorio es el cual Apache™ tiene establecido por defecto para el contenido que ofrece a través del servidor web.

Una vez que se descomprime el contenido de el paquete descargado en la carpeta indicada se debe cambiar el propietario de los archivos. Este cambio de propietario es necesario porque el propietario de estos archivos sería el usuario que está realizando las tareas de instalación. Sin embargo, la instalación se realiza a través de un navegador web, por lo que el usuario que debe poseer estos archivos es el que ejecuta el navegador web.

En este caso, el usuario que debe poseer estos archivos es "www-data", por lo que se cambiará el propietario. Para cambiar el propietario se utilizará el comando del cuadro A.13 desde la carpeta "/var/www".

```
chown www-data:www-data * -R
```

Cuadro A.13: Comando cambiar el propietario de archivos en Ubuntu™. Con este comando se cambia el propietario de los archivos de la carpeta en la que se ejecuta y todas sus subcarpetas a "www-data".

Una vez que se ha cambiado el propietario de estos archivos se debe proceder a la instalación y configuración de Joomla™. Para ello se utilizará un navegador web en el equipo para acceder a la dirección "localhost". Al acceder a esta dirección, aparecerá una página web como la de la figura A.5 que guiará a través de la instalación y configuración de Joomla™.

Una vez introducidos los datos en la primera página se pasa a la siguiente donde habrá que introducir los datos con los que se instaló la base de datos MySQL, los datos requeridos se pueden observar en la figura A.6.

Posteriormente, el la siguiente página se solicitan los datos de un servicio FTP para utilizarlo con la página web, como en este caso no se utilizará se dejará desactivado. Por último, se muestra una pagina en la que se puede elegir algún tipo de página de ejemplo, en este caso se ha elegido la opción "Datos de tipo blog". Además, se muestra un resumen de las diferentes opciones introducidas a lo largo de la instalación, una vez se ha revisado que los valores son correctos, se procede a la instalación de Joomla™.

Al finalizar la instalación a través del navegador web, Joomla™ pedirá que se cree el archivo "configuration.php" con el contenido que indica. Para ello se accede al directorio "/var/www" y se crea el archivo solicitado con el contenido que indica Joomla™.

Por último, para que la página funcione correctamente se debe eliminar los archivos de instalación de Joomla™. Para ello se debe eliminar la carpeta que contiene estos archivos, para borrar esa carpeta se debe ejecutar el comando del cuadro A.14 desde el directorio "/var/www".

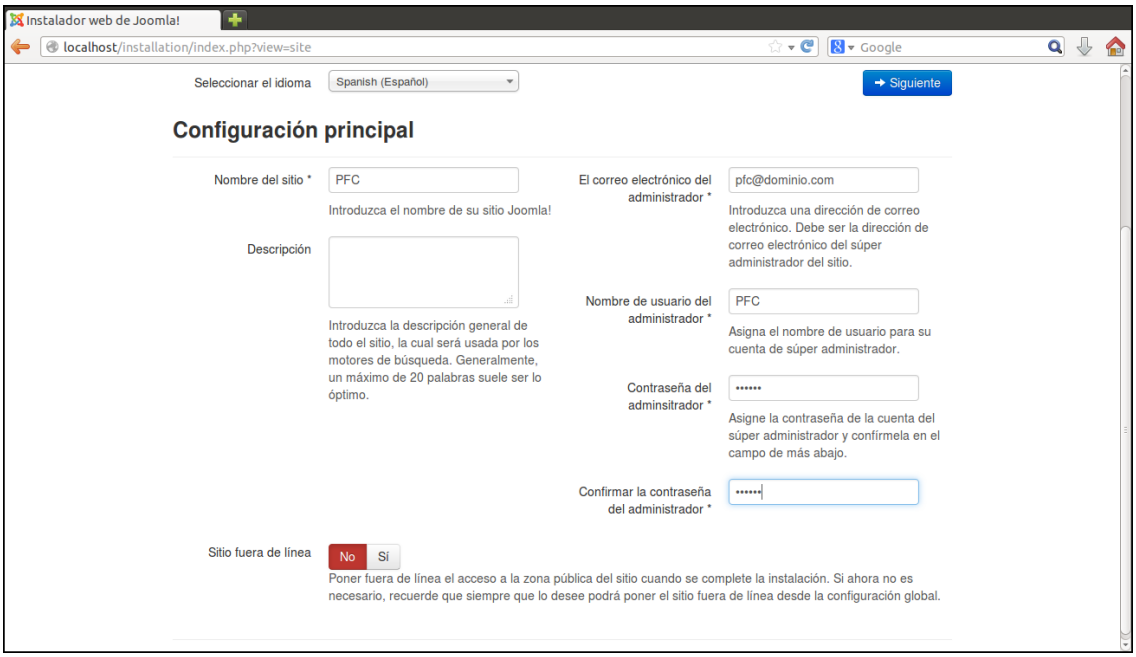

Figura A.5: Captura de pantalla de la instalación de Joomla™. En esta imagen se puede observar la primera pantalla de instalación de Joomla en la que se solicitan algunos de los datos.

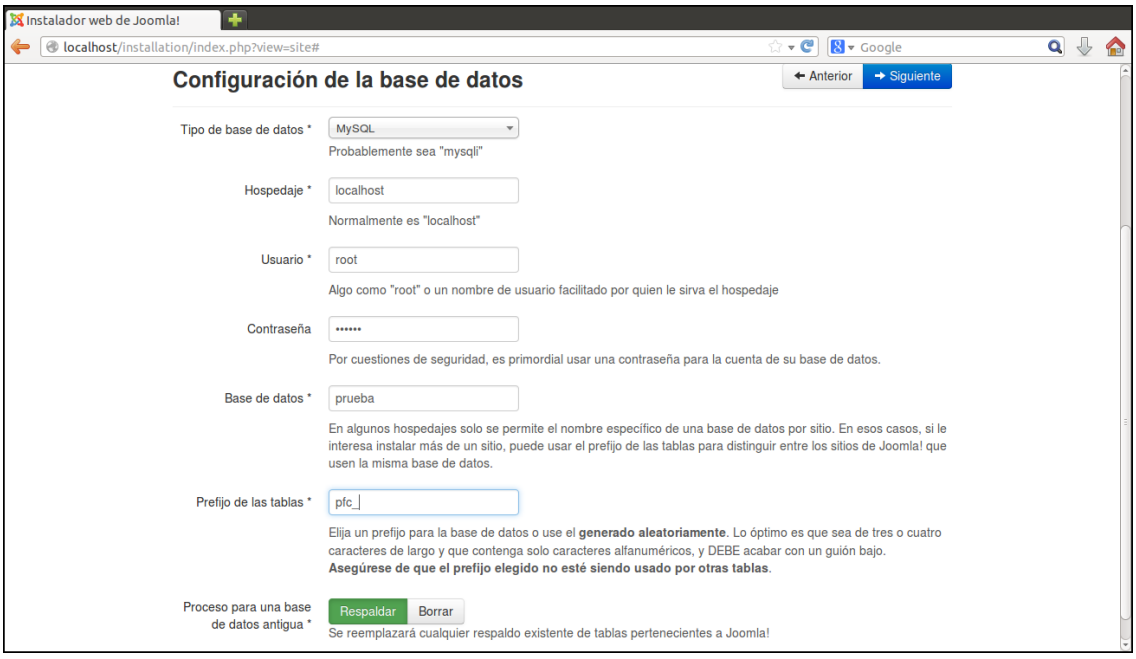

Figura A.6: Captura de pantalla de la instalación de Joomla™ para configurar la base de datos. En esta imagen se pueden observar los diferentes datos que se deben proporcionar para la configuración de la base de datos de Joomla™.

```
rm -R /var/www/installation
```

Cuadro A.14: Comando para eliminar archivos de instalación de Joomla™. Con este archivo se elimina la carpeta de instalación de Joomla en la que se encuentran los archivos que se utilizaron para su instalación.

Una vez eliminada esta carpeta, la instalación Joomla™ estaría completamente instalado. Para acceder a la configuración de la página web se debería acceder a través de un navegador web a "localhost", donde aparecerá la página web que se mostrará al público. Una vez en la página web se debe acceder al panel de administración, desde el cual se podrá comprobar y cambiar la configuración de los diferentes aspectos de la página web, así como su contenido.

Para más detalles acerca de Joomla™ se debe acceder a su página web oficial [8].

A.2.5. Creación de cuentas de usuario

Ya que el contenido de la página web se actualiza mediante una base de datos, es posible que sea administrada por diferentes usuarios y administradores con diferentes permisos.

En el caso de la página web, la creación de usuarios se realiza a través de la misma página web, utilizando el menú que se encuentra en la página principal. A través de este menú se crearán los diferentes usuarios y administradores.

Posteriormente, una vez se han creado los usuarios se debe gestionar los diferentes permisos que tendrá cada usuario. Para ello, se debe conectar a través de la página web con el usuario administrador de la misma y cambiar los diferentes permisos de los usuarios, ya sea a través de grupos o cambiando los permisos de un usuario concreto.

A.3. Servidor de correo

Como se indicó en la planificación de servicios, el servidor de correo cuenta de varios servicios que se debe implantar. Se eligió instalar estos servicios a través de Postfix y Dovecot™, llegando a proporcionar de esta manera el servicio SMTP, para enviar y recibir correos electrónicos, y POP3 e IMAP para la presentación de los correos electrónicos al usuario y su correcta recepción. Por tanto, habrá que instalar estos servicios.

A.3.1. Instalación de Postfix

Para la instalación de Postfix se utilizarán paquetes de las librerías de Ubuntu™, para ello se utilizará el comando del cuadro A.15.

```
apt-get install postfix
```

Cuadro A.15: Comando para instalar Postfix.

Al utilizar el comando se solicitan configurar las opciones de Postfix. Las opciones que se deben de

seleccionar son: “Internet Site”, como tipo de servidor, y “dominio.com” como *System mail name*. Esta opción de dominio será la que dictamine cuales son las direcciones de correo que debe aceptar el servidor, en este caso se utiliza un dominio hipotético, pero en caso de tratarse de un caso no hipotético se debería incluir el dominio registrado por la empresa. Estas opciones se pueden observar en las figuras A.7 y A.8.

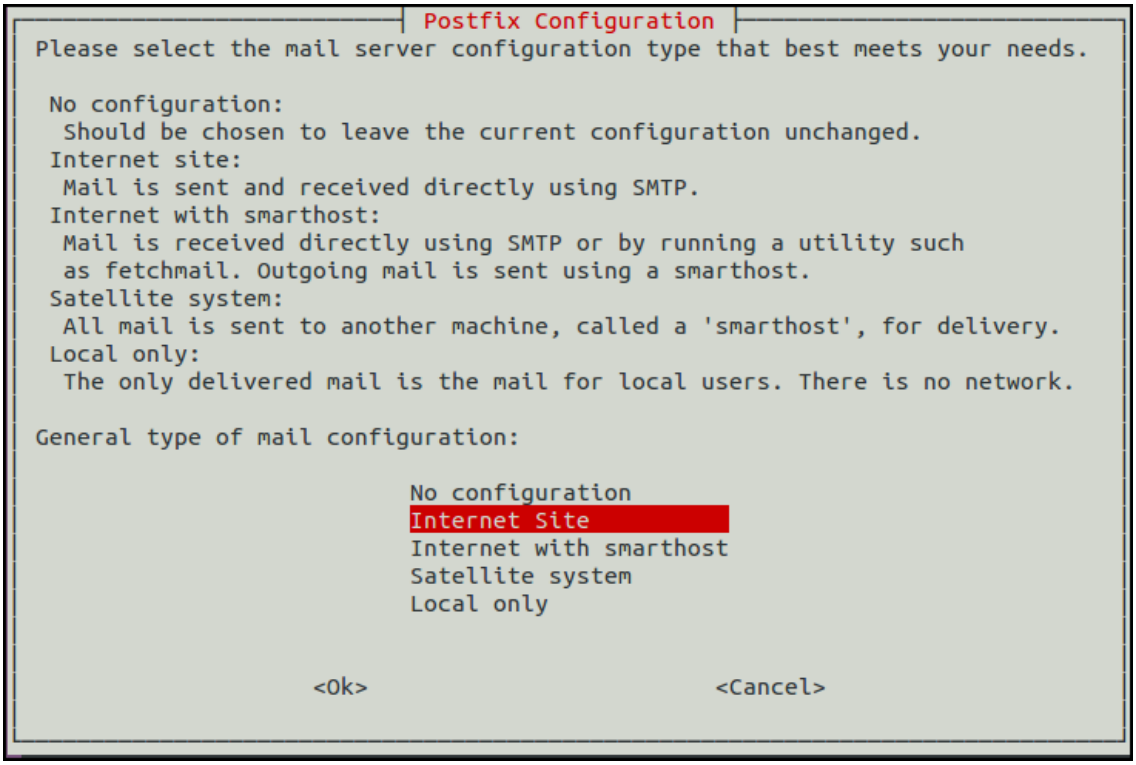

Figura A.7: Captura de pantalla con las opciones requeridas en la instalación de `Postfix`. En esta imagen se muestran las diferentes opciones a elegir en cuanto al tipo de servidor instalado, en este caso se seleccionará “Internet Site”.

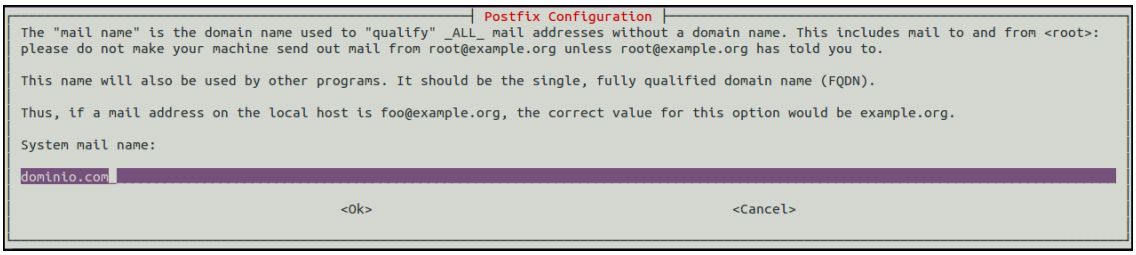

Figura A.8: Captura de pantalla con las opciones requeridas en la instalación de `Postfix`. En esta imagen se observa la opción que se debe introducir del dominio al que proveerá servicio `Postfix`, en este caso será “dominio.com”.

Posteriormente a su instalación se debe hacer una configuración básica del servidor. Para configurarlo se utilizará el comando indicado en el cuadro A.16.

Al utilizar el comando se solicitará que se introduzcan las opciones anteriores, pero también se solicitarán otras opciones como se pueden ver en las figuras A.9, A.10 y A.11.

En la opción que se muestra en la figura A.9 se establece que usuario será el que reciba los correos dirigidos hacia el administrador, es decir, hacia “postmaster@dominio.com”. De esta manera, se puede tener una dirección de correo de administrador sin necesidad de que el usuario que sea el administrador tenga que revisar dos

```
dpkg-reconfigure postfix
```

Cuadro A.16: Comando para configurar `Postfix`. Con este comando se inicia un proceso a través del cual se configura `Postfix` correctamente.

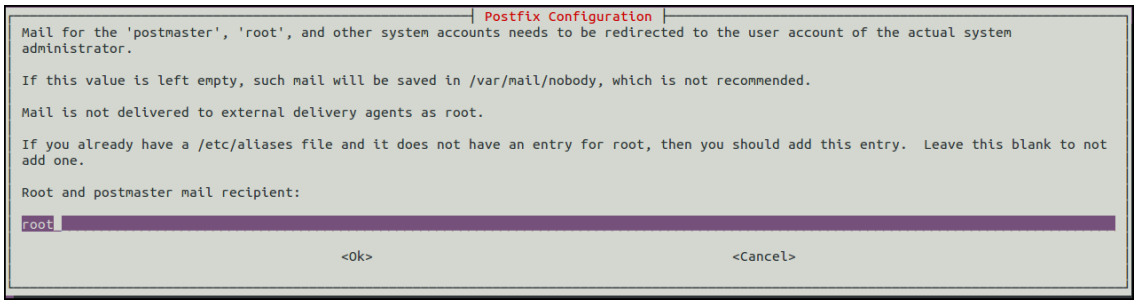

Figura A.9: Captura de pantalla con las opciones requeridas en la configuración de `Postfix`. En esta imagen se muestra la pantalla donde se solicita el usuario que actuará como postmaster del servidor, en este caso "root".

cuentas diferentes de correo.

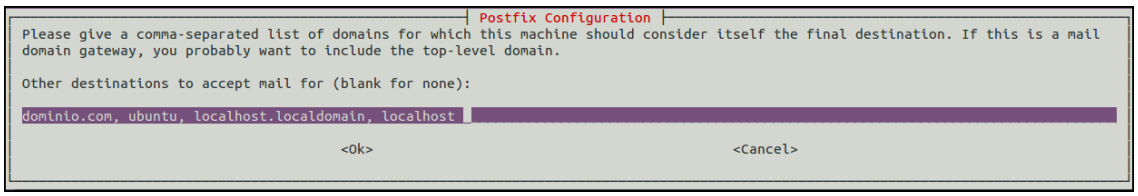

Figura A.10: Captura de pantalla con las opciones requeridas en la configuración de `Postfix`. En esta imagen se introducen los diferentes dominios para los cuales se recibirá correo, de esta manera se permite utilizar el mismo servidor para recibir correos de distintos dominios.

Con la opción de la figura A.10 se configura los destinos que debe aceptar el servidor de correo considerando que es el destinatario final. En este caso se utiliza la opción por defecto en la que ya se ha incluido el dominio que se está utilizando "dominio.com".

En la figura A.11 se muestra la configuración de *relay*. En esta configuración se debe añadir nuestro dominio para que se haga *relay*, es decir, para reenviar los correos recibidos. Para ello, se añadirán las dos redes propias, es decir, *192.168.1.0/24* y *192.168.2.0/24* en esta opción, dejando el resto de opciones por defecto.

Una vez cambiadas estas configuraciones el resto se dejaría el valor por defecto, ya que proporciona una buena configuración, y se tendría el servidor `Postfix` funcionando correctamente tras su reinicio. Para comprobar esto se puede hacer a través de `telnet` contactando con el servidor y enviando correos a alguna dirección existente mediante los diferentes comandos.

Para más detalles acerca de la configuración de `Postfix` o de su funcionamiento se puede consultar el libro correspondiente [24].

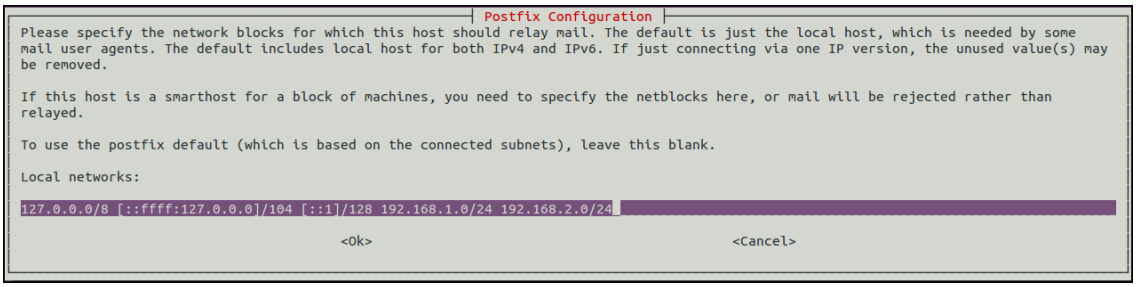

Figura A.11: Captura de pantalla con las opciones requeridas en la configuración de Postfix. En esta imagen se ve la interfaz a través de la cual se solicitan las diferentes redes para las cuales se hará *relay*.

A.3.2. Instalación de Dovecot™

Posteriormente se procede a la instalación de Dovecot™ para que proporciona los servicios de POP3 e IMAP. Para instalar Dovecot™ se utilizarán también los paquetes de las librerías de Ubuntu™, para ello se utiliza el comando del cuadro A.17.

```
apt-get install dovecot-imapd dovecot-pop3d
```

Cuadro A.17: Comando para instalar Dovecot. Con este comando se instala Dovecot™ para que funciona con POP3 e IMAP.

Una vez utilizado el comando del cuadro A.17 se dispondría del servicio de Dovecot™ instalado, por lo que se debe proceder a la configuración del mismo. Para ello habrá que realizar algunos cambios en los archivos de configuración. Los cambios a realizar son en diferentes archivos, siendo estos cambios:

- Se cambia la línea “listen=’*”” en el archivo “dovecot.conf” para que el servidor de correo escuche peticiones desde cualquier parte de la red, de esta manera permitimos el acceso al correo electrónico desde cualquier punto de la red.
- Se cambia la línea “disable_plaintext_auth=yes” en el archivo “10-auth.conf”, de esta manera se cancela la autenticación por texto plano, es decir, hay que cifrar las autenticaciones.
- Se cambia la línea “auth-verbose-passwords = sha1” en el archivo “10-logging.conf”, de esta manera al introducir una contraseña incorrecta se guarda en el log del sevidor codificada con sha1.
- Se cambia la línea “mail_location = mbox: /mail:INBOX/var/mail/ %u” en el archivo “10-mail.conf”, de esta manera se establece donde debe buscar los correos de los usuarios y donde debe guardar su información de correo.

Al realizar estos cambios se configura completamente el servidor Dovecot™ y ya estaría funcionando correctamente después de reiniciar el equipo para que se actualicen las configuraciones de todos los servicios. De esta manera, se tendría en funcionamiento tanto el servidor Postfix como Dovecot™, por lo que proporcionaríamos servicio SMTP, POP3 e IMAP, permitiendo a los usuarios elegir entre dos opciones para recibir su correo.

A.3.3. Creación de cuentas de usuario

Una vez se tiene instalado el servidor de correo con los servicios de SMTP, IMAP y POP3 funcionando, se deben de crear las diferentes cuentas de correo para que sean utilizadas por los usuarios.

En el servidor de correo, `Postfix` es el encargado de recibir los correos a través de SMTP, por lo que es el servicio que necesitará las cuentas de usuario para saber si existe la dirección de correo solicitada. Por lo tanto, las cuentas de usuario deberán ser creadas para `Postfix`.

El servidor `Postfix` utiliza como cuentas de correo las cunetas de los usuarios del sistema seguidas del dominio, es decir, los nombres de las cuentas de usuario seguidas de "@dominio.com". Por lo tanto, para crear las diferentes cuentas de correo destinadas a los usuarios solo se deben crear cuentas del sistema teniendo en cuenta que la dirección de correo final será "usuario@dominio.com".

Para crear un usuario, por lo tanto, se tendrán que utilizar los comandos indicados en los cuadros A.18 y A.19. De esta manera, se obtendrá una cuenta de correo para ese usuario, el cual deberá utilizar la misma contraseña, establecida en el sistema a partir de estos comandos, para acceder al servicio de correo.

```
useradd usuario -m
```

Cuadro A.18: Comando para crear un usuario en `Ubuntu`™.

```
passwd usuario
```

Cuadro A.19: Comando para establecer una contraseña a un usuario en `Ubuntu`™.

A.4. Base de datos interna

La base de datos interna se utilizará para que funcione el programa propio de la empresa, por lo tanto, deberá poder recibir conexiones de toda la red privada. Para esta base de datos se utilizará una base de datos SQL, más concretamente se utilizará una base de datos `PostgreSQL`™. La elección de `PostgreSQL` se debe a que se trata de una base de datos muy utilizada y que sigue en desarrollo, por lo que, en caso de detectarse errores o fallos de seguridad, existe una gran posibilidad de que sean corregidos en un corto espacio de tiempo.

A.4.1. Instalación de PostgreSQL™

Una vez seleccionado el tipo de base de datos que se utilizará y el servidor, se procede a la instalación.Para instalar esta base de datos se utilizarán las librerías de `Ubuntu`™, ya que, de esta manera, se asegura que se trata de software oficial que ha sido comprobado. Para ello se debe ejecutar el comando del cuadro A.20.

Al realizar este comando se instala la base de datos con una configuración predeterminada y un único usuario con todos los permisos, este usuario es `postgres`. Posteriormente, para evitar utilizar el usuario predeterminado se debe conectar con la base de datos y crear un nuevo usuario el cual utilizaremos para la gestión general de la base de datos. Para ello, utilizamos los comandos indicados en los cuadros A.21 y A.22.

```
apt-get install postgresql-9.1
```

Cuadro A.20: Comando para Instalar PostgreSQL™.

```
sudo -u postgres psql
```

Cuadro A.21: Comando para conectar con la base de datos PostgreSQL™.

Con estos comandos, se conecta con la base de datos y se crea un nuevo usuario, el cual utilizaremos para la gestión de la base de datos.

Una vez se ha creado el usuario se desconecta de la base de datos y se procede a crear una base de datos propia para la empresa. Esto es necesario debido a que durante la instalación solo se crean las bases de datos que se utilizan como plantillas para las nuevas bases de datos y, por lo tanto, no se deben utilizar para la empresa. Para crear una base de datos debemos especificar únicamente el nombre de la base de datos ya que el resto de características las copiará de la base de datos de plantilla. En este caso se creará una base de datos llamada *PFC*, para ello se debe ejecutar el comando del cuadro A.23.

Al realizar este comando se creará una base de datos vacía igual a la de la plantilla. Posteriormente se debe acceder a la base de datos para comenzar a gestionarla, así como configurar el servidor de manera correcta para que permita las conexiones necesarias.

A.4.2. Gestión de la base de datos

Para la gestión de la base de datos se utilizará una interfaz gráfica, en este caso se ha utilizado pgAdmin III. Se ha decidido utilizar esta interfaz debido a que se encuentra en las librerías propias de Ubuntu™ por lo que se habrá comprobado que no tendrá código malicioso. Además, se trata de una interfaz muy intuitiva que permite un gran control sobre la base de datos.

Instalación y configuración de pgAdmin III

Para instalar pgAdmin III se debe utilizar el comando del cuadro A.24.

Al ejecutar este comando se descargará e instalará la interfaz gráfica de pgAdmin III. Una vez instalada la interfaz gráfica se abre y se procede a la configuración de la conexión con la base de datos. Para ello se debe añadir un servidor donde se configurarán los detalles de la conexión. Los detalles de esta configuración se pueden observar en la figura A.12.

Como se puede observar en la figura se deben indicar diferentes datos de la conexión. En este caso, los

```
CREATE ROLE usuario LOGIN PASSWORD 'password' SUPERUSER;
```

Cuadro A.22: Comando para crear un usuario en PostgreSQL™. Con esta sentencia SQL se crea un usuario con los credenciales: *usuario/password*.

```
sudo -u postgres createdb PFC
```

Cuadro A.23: Comando para crear una base de datos en PostgreSQL™. Con este comando se crea una base de datos de nombre *PFC*.

```
apt-get install pgadmin3
```

Cuadro A.24: Comando para instalar pgAdmin III.

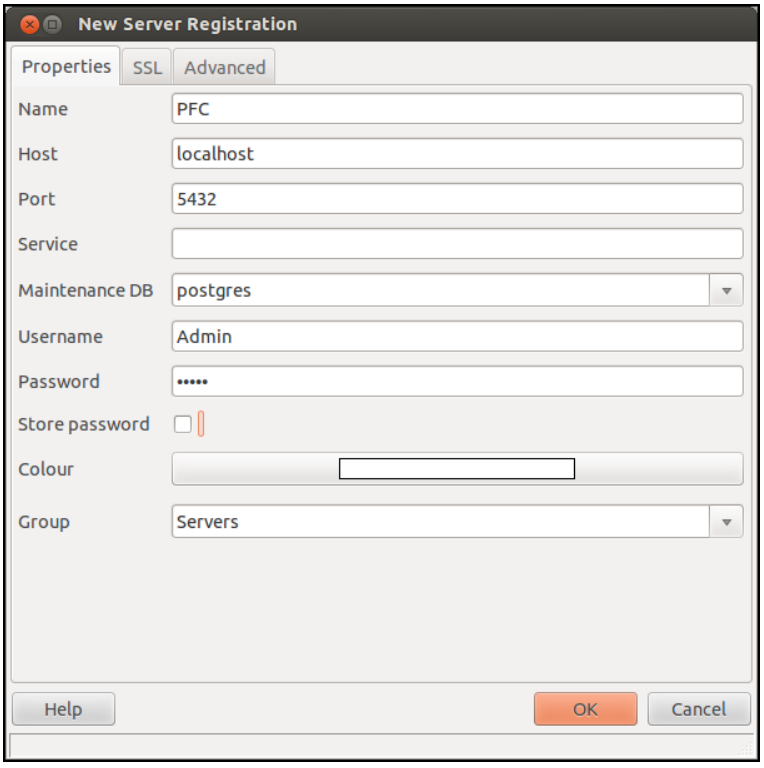

Figura A.12: Interfaz de creación de una conexión de pgAdmin III. En la imagen se pueden observar los diferentes parámetros que se deben rellenar para crear una conexión con una base de datos.

datos utilizados son:

Name: nombre que se quiere que se le adjudique a la conexión en la interfaz gráfica. Este parámetro no tiene importancia, ya que solo sirve para ayudar al usuario a identificar las conexiones, por lo que se podrá utilizar cualquier cosa.

Host: localhost. Este parámetro indica la dirección donde se encuentra el servidor PostgreSQL™. Debido a que la base de datos está instalada en el mismo equipo que la interfaz gráfica se utiliza "localhost".

Port: 5432. Puerto a través del cual se realizará la conexión con el servidor PostgreSQL™. Se deja el puerto por defecto, ya que no se ha modificado que la base de datos utilice otro puerto diferente.

Username y Password: deben ser los datos del usuario creado anteriormente con los comandos que se especificaron en los cuadros A.21 y A.22.

El resto de parámetros se dejarán por defecto. Una vez se conecta a PostgreSQL™ se pueden observar diferentes apartados como se muestra en la figura A.13. En estos apartados es donde se establecen los diferentes componentes del servidor PostgreSQL™. En el apartado "Databases" se encuentran las diferentes bases de datos que alberga el servidor, en este caso se encontrarán las base de datos de *PFC* y *postgres* siendo la primera la creada en el proyecto y la segunda la creada de forma predefinida. En el apartado "Group Roles" es donde se encontrarán los diferentes grupos de usuarios. Y en el apartado "Login Roles" es donde se encontrarán los diferentes usuarios con los que se puede conectar a la base de datos.

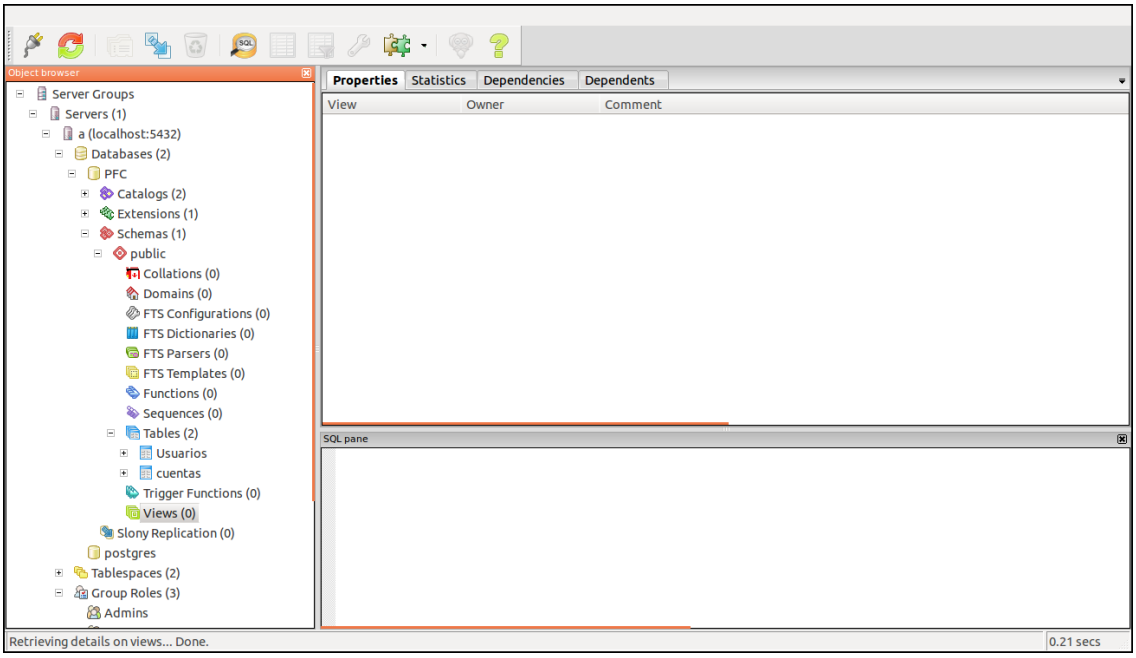

Figura A.13: Interfaz principal de pgAdmin III.

Creación de usuarios y grupos

Una vez que se tiene conexión con la base de datos se debe comenzar a crear los diferentes grupos y usuarios con sus correspondientes permisos, así como las diferentes tablas de la base de datos.

Debido al funcionamiento de PostgreSQL™ es posible definir grupos de usuarios en los que definimos sus permisos, para posteriormente añadir usuarios que pertenezcan a estos grupos y hereden sus permisos. Por lo tanto, se comenzará creando los diferentes grupos de usuarios con los diferentes permisos de acceso a la base de datos.

Para crear un usuario se deben pulsar con el botón derecho en “Group Roles” y se selecciona la opción de “New Group Role...”. Una vez se hace esto se abrirá una ventana donde se deberán poner las diferentes características, tal como se muestra en la figura A.14.

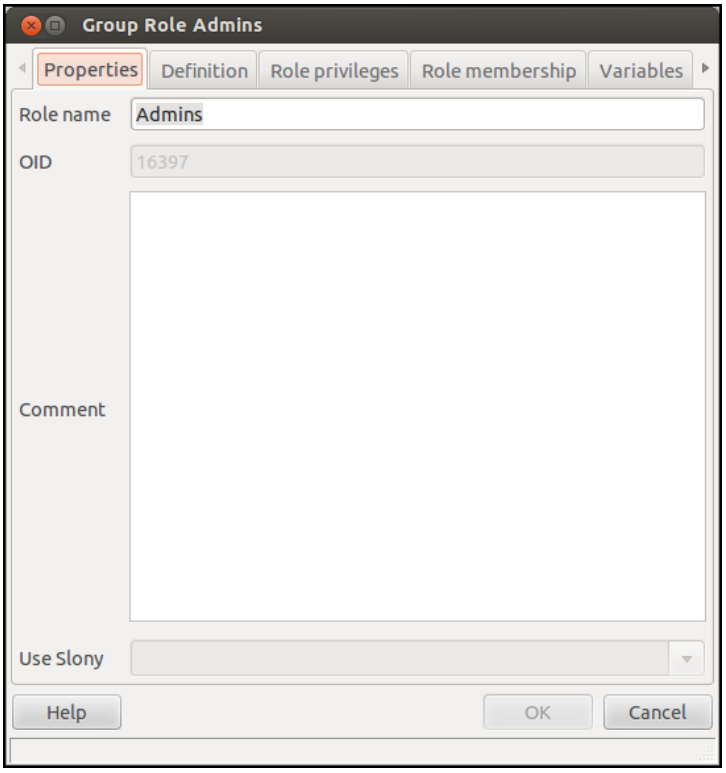

Figura A.14: Interfaz de creación de un grupo de `pgAdmin III`.

En esta ventana se encuentran diferentes pestañas en las cuales se deben configurar los diferentes aspectos del grupo que se está creando.

Properties:

Role name: nombre del grupo que se está creando.

Comment: comentarios del grupo de usuarios que se está creando.

Definition:

Password: contraseña del grupo que estamos creando. En este caso no se pondrá contraseña, ya que no se le proporcionarán permisos de conexión a la base de datos y por lo tanto no será necesaria.

Account expires: fecha en la que caduca el grupo, es decir, fecha en la que el grupo pierde todos sus permisos.

Connection Limit: número de conexiones simultáneas que se permiten de el grupo. Debido a que al grupo no se le añadirán permisos de conexión no será necesario establecer un límite.

Role Privileges: en esta pestaña es donde se establecen los privilegios del grupo. Existe la posibilidad de otorgarle desde permisos de superusuario, a permisos para crear usuarios.

Role Membership: en esta pestaña se encuentran los diferentes grupos a los que pertenece el grupo que estamos creando.
Esta opción permite crear grupos anidados, es decir, crear grupos que pertenezcan a grupos mayores, de forma que se puede organizar de una manera muy clara los permisos que tendrá cada grupo al heredarlos de los grupos a los que pertenece.

Variables: en esta pestaña se establecen diferentes variables para el grupo. En este caso se mantendrán las

variables por defecto, por lo que no se tendrá que realizar ninguna modificación.

SQL: en esta pestaña se puede observar el código SQL que crea ejecutará al finalizar la creación del grupo, es decir, el código SQL equivalente a todas las opciones seleccionadas en las diferentes pestañas.

Si se siguen estos pasos se crea un grupo con los diferentes permisos elegidos. Posteriormente se deben crear los diferentes usuarios que serán a través de los cuales se conectará a la base de datos para realizar las diferentes tareas.

Para crear un usuario se debe pulsar con el botón derecho en “login Roles” y seleccionar la opción de “New Login Role...”. De esta manera se abre una ventana igual a la que se utiliza para la creación de grupos, pero con pequeñas modificaciones en las opciones que se pueden seleccionar, por lo que se puede utilizar el mismo proceso que para crear un grupo pero teniendo en cuenta que se trata de la creación de un usuario.

En caso de una vez creado, tanto un grupo como un usuario, querer modificarlo es posible modificar todas las opciones, por lo que es mejor mantener unos permisos restringidos y añadir más permisos según sea necesario.

Posteriormente, se debe configurar las propiedades de la base de datos. Para ello se debe buscar la base de datos que se creó anteriormente, mediante el comando en la consola. Las diferentes bases de datos que existen se encuentran en la opción “Databases”, y para acceder a la configuración de una de ellas se debe pulsar con el botón derecho sobre ella y escoger la opción de “Properties...”. Al seleccionar esta opción se abrirá una ventana en la que se pueden seleccionar todas las propiedades de la base de datos a través de las diferentes pestañas, tal y como se muestra en la figura A.15.

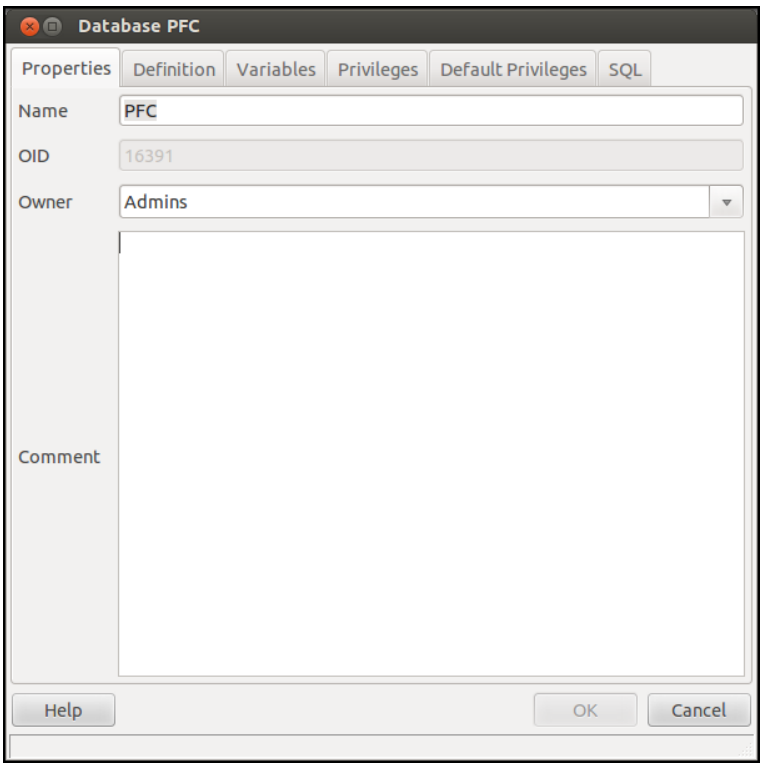

Figura A.15: Interfaz de modificación de una base de datos de `pgAdmin III`.

Debido a la gran cantidad de propiedades que tiene una tabla, solo se comentarán las más importantes que serán las que se modificarán en este caso. Las opciones a tener en cuenta son:

Owner: ésta es una opción de la pestaña inicial. Esta opción establece quien es el propietario de la base de datos, es decir, quien será el administrador de la misma.
Es posible asignar la propiedad de la base de datos tanto a un usuario como a un grupo. En este caso se

ha establecido al grupo de usuarios “Admins”, de forma que, para establecer un administrador de la base de datos, solo se tendría que añadir el usuario a este grupo.

Connection Limit: ésta es una opción de la ventana “Definition”. Esta propiedad establece el número de conexiones simultáneas máximas que se permiten a la base de datos. A través de esta opción se podría controlar que no hay demasiados usuarios accediendo a la base de datos, pero debido a que será una base de datos utilizada desde numerosos equipos se utilizará la opción “-1” que corresponde con conexiones ilimitadas permitidas.

Privileges: en esta pestaña se establecen los diferentes permisos que tendrán en la base de datos los grupos. Se permite establecer permisos para crear tablas nuevas, crear tablas permanentes y conectar con la base de datos, con la opción para cada uno de los permisos de que se puedan conceder los mismos a otros usuarios. A partir de estos parámetros se pueden establecer unos permisos iniciales que en caso de tener diferentes bases de datos en el mismo servidor permitirían separar los grupos de usuarios de ambas bases de datos a través de diferentes permisos.

Default Privileges: en esta pestaña se establecen los permisos por defecto que se establecen a crear tablas, secuencias o funciones en la base de datos.

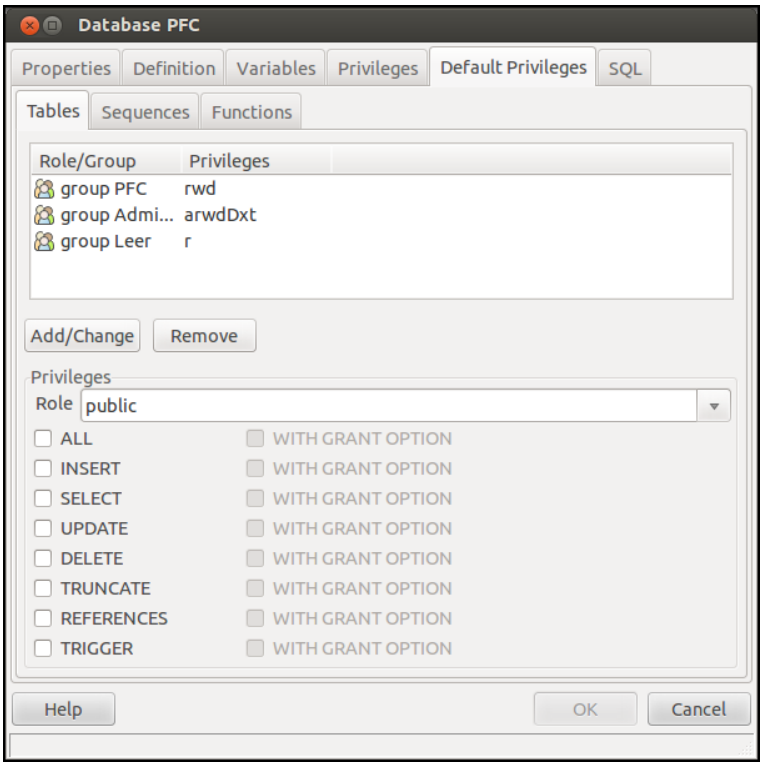

Figura A.16: Interfaz de "Default Privileges" de una base de datos de `pgAdmin III`. En esta interfaz es donde se establecen los diferentes privilegios por defecto que tendrán los elementos de la base de datos seleccionada.

Como se puede observar en la figura A.16, se pueden establecer diferentes permisos para cada usuario o grupo de usuarios, además de separar estos permisos en función del elemento al que se quiera establecer. Los permisos que se pueden configurar varían desde permisos de selección, para poder leer los datos de una tabla, hasta poder eliminar todos los datos de una tabla con la opción de que pueda conceder estos permisos a otro usuario al igual que en los privilegios de la base de datos.
A partir de estas opciones se pueden establecer unos permisos por defecto para todos los elementos de una base de datos, de esta manera al crear un nuevo elemento en la base de datos no se tendría que modificar los permisos excepto en casos especiales, ya que los permisos por defecto estarían establecidos en la configuración de la base de datos, permitiendo un control más sencillo de los permisos iniciales.

Una vez establecidas las diferentes propiedades de la base de datos se debe proceder a la creación de las diferentes tablas que contendrán toda la información que se quiere almacenar.

Para ello existen dos métodos muy diferentes, el primer método es a través de la utilización de código SQL. Para la utilización de código SQL se puede realizar una conexión con un cliente SQL a la base de datos y ejecutar directamente el código para crear las diferentes tablas, sin embargo, la interfaz gráfica que se está utilizando también permite la ejecución de sentencias SQL.

Para abrir este cliente se debe seleccionar la opción "Query tool" en el menú de herramientas de la interfaz. Al seleccionar esta herramienta se abre una nueva interfaz en la que se pueden escribir sentencias SQL para ser ejecutadas tal como se muestra en la figura A.17.

Además, en esta herramienta, también se permite la creación de diferentes sentencias a través de una pequeña interfaz que muestra las diferentes tablas pudiendo seleccionar de forma simple los campos que queremos seleccionar como se muestra en la figura A.18.

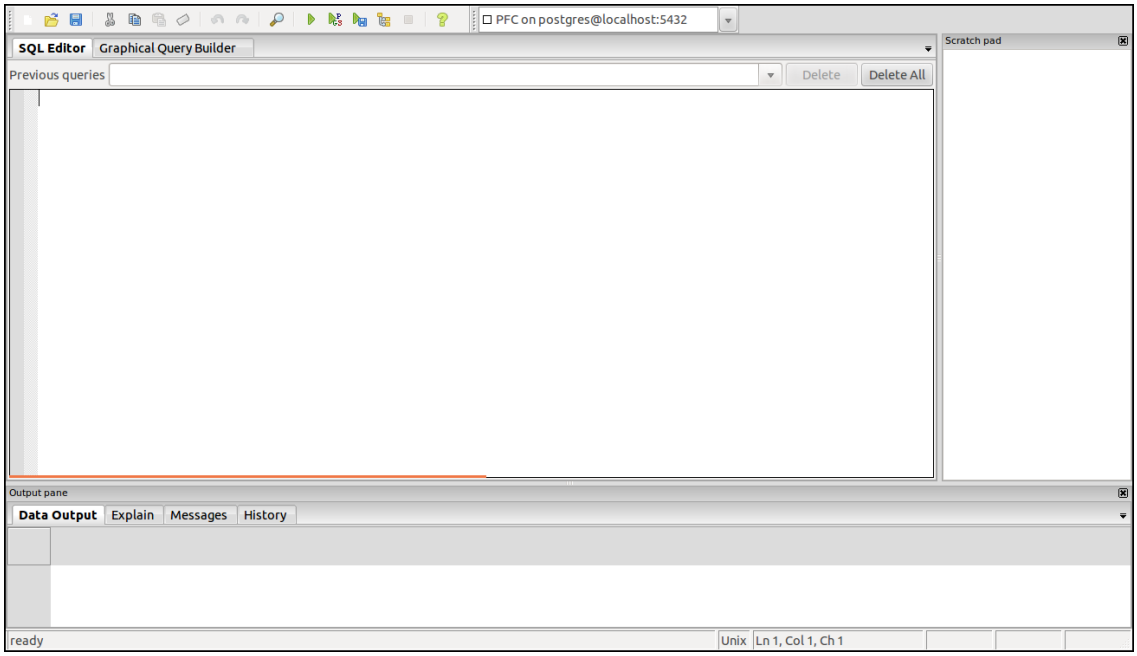

Figura A.17: Interfaz de ejecución de código SQL de `pgAdmin III`. A través de esta interfaz se pueden crear diferentes sentencias SQL para ser ejecutadas en la base de datos.

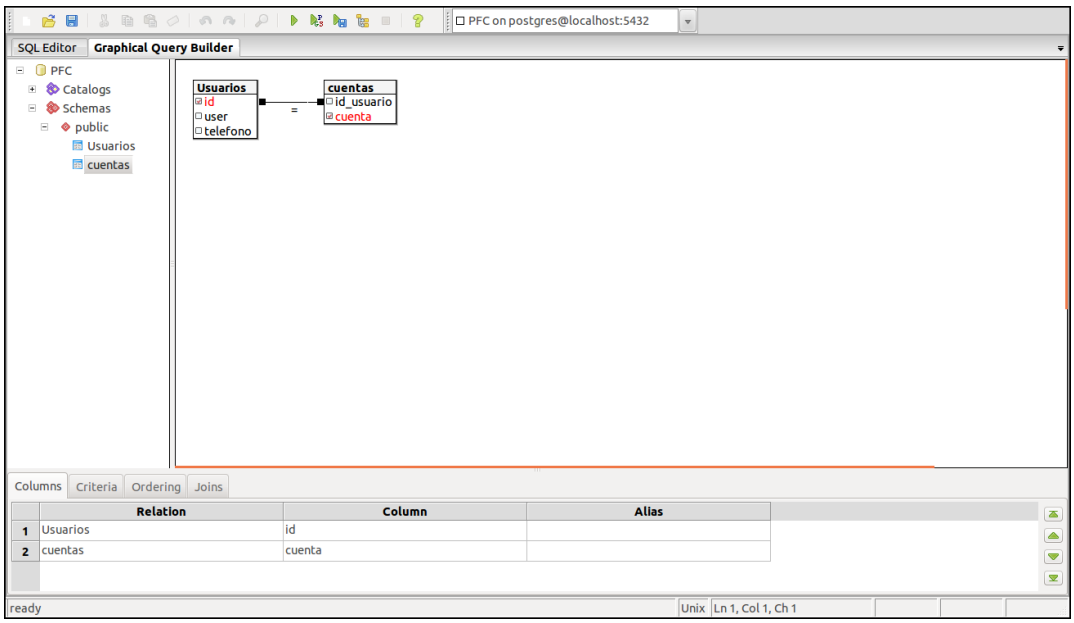

Figura A.18: Interfaz de creación de código SQL de `pgAdmin III`.

A.4.3. Configuración del servidor

Una vez se ha configurado el acceso a la base de datos correctamente, para que no pueda acceder un usuario no deseado, se debe permitir el acceso desde otros puntos de la red diferentes al del equipo donde está instalado el servidor.

Para ello se debe cambiar la configuración de acceso al servidor debiéndose realizar dos cambios en los archivos de configuración.

El primer cambio se debe realizar en el archivo indicado en el cuadro A.25.

```
/etc/postgresql/9.1/main/pg_hba.conf
```

Cuadro A.25: Ruta al archivo configuración credenciales PostgreSQL™ en Ubuntu™.

En este archivo se encuentra la configuración de los credenciales aceptados para las diferentes conexiones con el servidor PostgreSQL™. Inicialmente solo se permiten conexiones desde el propio equipo donde se instala el servidor, por lo que, para poder conectar desde otros equipos de la red, se debe añadir esta configuración. Para añadir esta configuración se debe tener un archivo con una configuración como en el cuadro de código A.2.

```
8  # IPv4 local connections:
9  host all all 127.0.0.1/32 md5
10 host all  all  192.168.1.0/24  md5
```

Código A.2: Código de configuración de PostgreSQL™.

En la línea 10, la cual se ha añadido, se especifica que se deben permitir conexiones para todas las bases de datos y todos los usuarios de la red *192.16.1.0/24* mientras que al conectar utilicen contraseñas con un cifrado *md5*.

De esta manera, se permiten conexiones a la red interna de la empresa, pero manteniendo una seguridad debido a que se necesita contraseña y la misma debe utilizar un sistema de cifrado, por lo que se reducirían los riesgos de seguridad.

El otro cambio en la configuración que se debe realizar es la configuración de donde debe escuchar conexiones el servidor. Esta configuración se encuentra en el archivo indicado en el cuadro A.26.

```
/etc/postgresql/9.1/main/postgresql.conf
```

Cuadro A.26: Ruta al archivo de configuración de PostgreSQL™ en Ubuntu™.

En este archivo se debe modificar la configuración para que se escuchen conexiones desde otras partes de la red, ya que de forma predeterminada el servidor solo escucha conexiones provenientes del propio equipo. Por lo tanto, se debe tener un archivo de configuración como el del cuadro de código A.3.

De esta manera, queda establecido que se escuchen conexiones desde cualquier dirección, permitiendo que se establezcan conexiones a través de la propia red utilizando los diferentes credenciales que se crearon en los pasos anteriores.

```
8  listen_addresses = '*'  # what IP address(es) to listen on;
```

Código A.3: Código de configuración de PostgreSQL™.

Al realizar estos cambios ya se podrían establecer conexiones con la base de datos desde otros equipos de la red, ya que el servidor escucha conexiones desde cualquier parte de la red y ,además, permite identificarse como usuario a los equipos que pertenezcan a la red interna de la empresa, por lo que se podría utilizar la base de datos correctamente.

Para más detalles acerca de la configuración de PostgreSQL™ o de su funcionamiento se puede consultar el libro correspondiente [28].

A.5. Servidor Samba

A.5.1. Instalación y configuración

Para la instalación del servidor Samba se utilizarán las librerías oficiales de Ubuntu™, ya que, de esta manera, se asegura que no se trata de software malicioso, además que permite una actualización muy simple, lo que produce que mantener el servidor seguro sea una tarea más sencilla.

Para instalar el servidor Samba utilizaremos el comando indicado en el cuadro A.27.

```
apt-get install samba
```

Cuadro A.27: Comando para instalar el servidor Samba.

Una vez instalado el servidor correctamente se debe realizar una configuración del mismo. Para cambiar la configuración se deben realizar los cambios necesarios en el archivo indicado en el cuadro A.28.

```
/etc/samba/smb.conf
```

Cuadro A.28: Ruta al archivo de configuración de Samba en Ubuntu™.

En este archivo se encuentra toda la configuración del servidor Samba, desde el grupo de trabajo que debe utilizar hasta las diferentes carpetas que se deben compartir. Debido a la gran cantidad de parámetros que contiene el servidor, solo se comentarán aquellos que son más importantes y los cuales será necesario cambiar. Estos parámetros son:

workgroup: éste será el grupo de trabajo al que conectará Samba. Es un parámetro necesario para que los clientes Windows™ puedan conectarse al servidor Samba correctamente, ya que para ello deben estar en el mismo grupo de trabajo.

netbios name: este parámetro se tendrá que añadir, ya que no existe de forma predeterminada en el archivo de configuración. Este parámetro indica cual será el nombre de el servidor Samba en la red, es decir, el nombre que el resto de equipos de la red verán.

De forma predeterminada se utiliza el nombre del equipo que puede ser modificado a través de otros archivos del sistema operativo, pero se decide realizar este cambio en la configuración de debido a que es más sencilla y además, no presenta problemas con otras configuraciones.

server string: este parámetro indica la descripción del servidor, se utilizará cuando se le solicite información al servidor sobre el mismo.

interfaces: en este parámetro se deben configurar aquellas redes o interfaces en las que se quiere que el servidor escuche conexiones. A través de este parámetro se puede establecer que escuche conexiones en nuestra red local. En este caso se ha configurado para que escuche conexiones en la red interna con el valor *192.168.1.0/24 eth0* para evitar conexiones desde otras redes.

bind interfaces only: este parámetro indica si únicamente se deben dejar establecer conexiones a los equipos que se conecten a través de las redes o interfaces especificados en el parámetro anterior de "interfaces".

Con este parámetro se puede limitar la conexión al servidor de equipos de fuera de la red si se configura correctamente para que únicamente escuche conexiones de la red interna y luego se establece este parámetro a "yes" para que solo permita conexiones desde esa red. En este caso se ha seguido esta configuración para limitar el acceso desde otros puntos de la red.

security: este parámetro indica que tipo de seguridad de conexión se establece en el servidor. En función de el parámetro de configuración que se establezca se tendrá un nivel de seguridad distinto. En este caso, se ha utilizado la opción de "user", esta opción establece que para que un usuario pueda establecer conexión con el servidor este debe tener una cuenta `Unix`™ en el servidor, es decir, que solo podrán conectar aquellos usuarios que tengan una cuenta en el propio equipo.

encrypt passwords: este parámetro establece si se codificarán las contraseñas para guardarlas. Debido a que se trata de establecer un servidor seguro se utiliza la opción "yes" que establece que las contraseñas deben codificarse antes de ser guardadas en un archivo. De esta manera se aumenta el nivel de seguridad, pero no es un parámetro que asegure la confidencialidad de las contraseñas, ya que pueden ser descodificadas con algunas herramientas.

map to guest: esta opción establece que se debe hacer cuando un usuario tiene un error al tratar de conectar con el servidor porque no proporciona unos datos de usuario y contraseña correctos. En esta opción se pueden establecer diferentes valores dependiendo del nivel de seguridad y de las funciones que se quieran establecer en el servidor.

En este caso se ha cambiado de la opción "bad user", que se utiliza por defecto y que establece las conexiones fallidas con un usuario anónimo, a la opción "never" que rechaza la conexión en caso de no utilizar unos credenciales válidos.

name resolve order: este parámetro indica el orden que se debe utilizar en el servidor para resolver los nombres de las conexiones.
Este parámetro es necesario que se configure de manera correcta, ya que en caso de no utilizar una configuración correcta produce problemas con los nombres para compartir carpetas, así como para establecer una visibilidad en la red del servidor correcta. En este ejemplo se utilizó la opción de "bcast host", con esta configuración se trata de resolver el nombre primero mediante su búsqueda en la red, y en caso de no ser posible trata de buscar en el propio equipo. Con esta configuración se asegura que no se provoquen problemas porque algún equipo pueda cambiar de dirección IP y pueda provocar problemas por tratar de resolver ese nombre inicialmente en el propio equipo, ya que se guarda información de las últimas conexiones en memoria y podría dar lugar a errores.

Además de estas opciones comentadas, existen muchas otras que permiten realizar muchos cambios en el servidor, tales como la integración del mismo con otros servicios como DNS o la compartición de impresoras.

En este caso se ha utilizado una configuración predeterminada para el resto de parámetros, ya que, de esta manera, se mantenían los servicios ofrecidos por `Samba` de forma correcta sin introducir nuevas brechas de seguridad por tener otros servicios configurados de manera incompleta.

Mediante este proceso se contaría con un servidor `Samba` funcionando correctamente, pero sin tener ningún directorio compartido. Para más detalles acerca de la configuración o funcionamiento de `Samba` se puede consultar el libro correspondiente [22].

A.5.2. Creación de zonas compartidas

Posteriormente, tras la configuración del servidor, se deben establecer las diferentes carpetas compartidas del sistema, así como cuales son los usuarios que podrán conectar a las mismas y sus permisos. Para ello, en el mismo archivo de configuración se deben establecer estas zonas de compartición, éstas llevan la estructura del cuadro de código A.4.

```
1  [public]
2      comment = Carpeta publica
3      path = /home/public
4      read only = no
5      create mask = 0744
6      valid users = @sambashare
```

Código A.4: Ejemplo de configuración de zona compartida en `Samba`.

Este sería un ejemplo utilizado para la compartición de una carpeta pública entre todos los usuarios. Los diferentes parámetros utilizados son:

Línea 1: esta línea indica el nombre que tendrá la carpeta compartida. Se puede utilizar cualquier nombre a excepción de unos pocos nombres especiales que serán comentados más adelante.

Línea 2: comentario acerca de la carpeta que será visible desde algunos exploradores de archivos.

Línea 3: ruta a la carpeta que va a ser compartida.

Línea 4: esta opción establece si esta carpeta será solo de lectura, valor por defecto, o si se podrá escribir.

Línea 5: este parámetro indica cual es la máscara que se utilizará para crear los archivos, esta máscara indica los permisos que tendrá el propietario, los usuarios del mismo grupo que el propietario y el administrador. En este caso el propietario tendría permisos de lectura, escritura y ejecución, mientras que los usuarios del mismo grupo que el propietario y el administrador tendrán permisos de lectura únicamente.

Línea 6: usuarios que tendrán acceso a esta carpeta compartida. Gracias a este parámetro se pueden crear diferentes carpetas compartidas para diferentes grupos de usuarios o usuarios específicos, ya que nos permite establecer quien podrá acceder a una carpeta concreta. En esta opción se deben especificar los nombres de usuarios separados por comas o, en caso de utilizarse grupos, se debe anteponer un "@" al nombre del grupo.

Además de estos parámetros existen muchos otros que permiten configurar cada carpeta compartida de samba de diferentes maneras. Por otro lado, como se dijo al explicar los parámetros utilizados en el ejemplo, hay algunos nombres especiales que no se pueden utilizar como nombres de carpetas compartidas. Estos nombres son:

global: este nombre es el utilizado por el servidor `Samba` para especificar toda la configuración global, es decir, la configuración que se utilizará en las carpetas compartidas en caso de no indicarse lo contrario.

Esta sección resulta muy útil cuando se requiere establecer una configuración en todas las carpetas compartidas que no se corresponde con la configuración por defecto, ya que de esta manera se evita tener que repetir la misma configuración en todas las zonas compartidas, reduciendo la probabilidad de que una carpeta quede mal configurada.

homes: este es utilizado por el servidor `Samba` para compartir de forma automática las carpetas personal de un usuario de forma automática.

Esta opción resulta muy útil cuando se requiere compartir la carpeta personal de todos los usuarios que utilizarán `Samba`, ya que con la utilización de esta etiqueta se permite configurar todas las carpetas de la misma manera, y será el servidor `Samba` el que automáticamente cuando un usuario conecte al servidor cree la compartición de su carpeta personal.

De esta manera, se evita tener que crear una zona para cada carpeta compartida de cada usuario y, además, evita que un usuario pueda ver cuales son los demás usuarios que tienen su carpeta compartida, ya que el servidor `Samba` solo comparte de forma automática la carpeta del usuario que se ha conectado con el servidor, dejando las de los demás usuarios sin compartir.

printers: este es utilizado por el servidor `Samba` para compartir las impresoras del equipo.

A través de este nombre `Samba` utiliza sus servicios para compartir las impresoras que tenga el equipo instaladas, permitiendo cambiar la configuración de la forma en la que las mismas se comparten, por lo que este nombre está reservado para este uso.

En este caso únicamente se ha utilizado la etiqueta de "global" para establecer la configuración global de las carpetas compartidas. No se ha utilizado la opción de compartir las impresoras conectadas al equipo, ya que este equipo actuará únicamente como servidor `Samba`, por lo que no tendrá ninguna impresora conectada y, por lo tanto, no se utilizará esta opción.

Por otro lado, la opción de "homes" es muy útil debido a que se requiere compartir las carpetas personales de los diferentes usuarios para que pueda mantener los archivos que consideren necesarios en el servidor para poder utilizarlos en diferentes puestos de trabajo o diferentes sistemas operativos sin necesidad de utilizar otras plataformas.

Sin embargo, esta opción causa muchos problemas debido a su funcionamiento para los clientes que utilizan `Ubuntu`™. Estos problemas de funcionamiento se debe a que los navegadores de archivos más utilizados en este sistema operativo funcionan de manera muy diferente a como funcionan el navegador de archivos de Windows™. Esta diferencia en el funcionamiento consiste básicamente en que el explorador de archivos de Windows™ una vez que comprueba que el servidor necesitará un usuario y una contraseña para conectar se los solicita al usuario, por lo que comprueba el contenido que se está compartiendo en el servidor habiéndose identificado previamente. Sin embargo, los navegadores de archivos de `Ubuntu`™ tienen un funcionamiento diferente, estos navegadores comprueban cual es el contenido que el servidor `Samba` tiene compartido, y cuando se trata de acceder a una carpeta pide los credenciales para conectar con el servidor y ver si se tienen los permisos necesarios para montar únicamente la carpeta solicitada.

Esta diferencia en el funcionamiento provoca que cuando se trata de ver las carpetas compartidas por el servidor Samba desde un cliente que utilice Ubuntu™, éste no es capaz de acceder a las carpetas personales de los usuarios aunque estén siendo compartidas a través del uso de la etiqueta “homes”, ya que el servidor Samba solo comparte la carpeta del usuario cuando conoce los credenciales del usuario y, sin embargo, los exploradores de archivos de Ubuntu™ nunca solicitan las carpetas compartidas identificándose primero.

De esta manera, no se utilizará la etiqueta de “homes” debido a que produciría problemas para acceder a las carpetas personales de los usuarios de forma correcta en clientes que utilicen Ubuntu™, por lo tanto, se utilizará una carpeta compartida para cada usuario creada de forma manual. Así, a pesar de ser un proceso más lento, se puede asegurar el correcto funcionamiento para ambos sistemas operativos.

A.5.3. Creación de cuentas de usuario

Una vez se ha terminado con la configuración del servidor Samba y sus carpetas compartidas, se deben crear las diferentes cuentas para acceder al mismo. Al igual que otros servicios, Samba utiliza las cuentas de los usuarios del propio equipo como cuentas del servidor, con la excepción de que solo se pueden utilizar si se les añade una contraseña propia del servicio. Por lo tanto, para crear nuevos usuarios se deben realizar las siguientes acciones:

1.– Se crea un usuario en el equipo de Samba que posea su propia carpeta personal. Para ello, utilizando un usuario con permisos de administrador se utiliza el comando del cuadro A.29.

```
useradd ''usuario'' -m
```

Cuadro A.29: Comando para crear un usuario en Ubuntu™.

Se utiliza la opción de “-m” para que se cree de forma automática la carpeta personal para poder compartirla posteriormente.

2.– Posteriormente se le añadirá una contraseña a la cuenta, este paso no es necesario para el funcionamiento de Samba, sin embargo, tener un usuario sin contraseña en el sistema puede dar lugar a grandes problemas de seguridad, por lo que se le añadirá una contraseña a cada usuario. Para ello se utilizará el comando del cuadro A.30.

```
passwd ''usuario''
```

Cuadro A.30: Comando para establecer una contraseña a un usuario en Ubuntu™.

3.– Una vez creado el usuario y se ha establecido una contraseña en el sistema es necesario establecer la contraseña para el servicio Samba. Esto es necesario debido a que el servidor Samba utiliza sus propias contraseñas para la autenticación de usuarios, por lo que la contraseña del sistema no sería la utilizada para conectar con el servidor Samba. Para establecer la contraseña del usuario se utiliza el comando del cuadro A.31.

```
smbpasswd -a ''usuario''
```

Cuadro A.31: Comando para establecer una contraseña a un usuario en Samba.

Al utilizar este comando se solicitará que se escriba una contraseña que será la utilizada para conectar con el servidor Samba.

4.– Posteriormente, si se quiere que el usuario tenga acceso a alguna carpeta compartida únicamente a algún grupo, se debe añadir este usuario al grupo. Para ello se debe utilizar el comando del cuadro A.32.

```
adduser ‘‘usuario’’ ‘‘grupo’’
```

Cuadro A.32: Comando para añadir un usuario a un grupo en Ubuntu™.

Al realizar este procedimiento se creará un usuario con el que se podrá acceder al servidor Samba, pero como se ha explicado anteriormente, será necesario modificar el archivo de configuración de Samba añadir la compartición de su carpeta personal. Para ello se añadirá una nueva zona siguiendo la configuración establecida en el capítulo de “Creación de zonas compartidas”.

A.6. Servidor de impresión Linux

Para proporcionar el servicio de servidor de impresión Linux se ha elegido utilizar CUPS debido a su gran utilización en estos entornos. Para la instalación de CUPS se utilizarán las bibliotecas de paquetes oficiales de Ubuntu™, para garantizar que se trata de software confiable y que se trata de la última versión disponible. Posteriormente a su instalación, se debe realizar la implantación de las diferentes impresoras en el sistema para su correcta utilización.

En esta red se ha utilizado para realizar las pruebas tanto una impresora virtual como una impresora modelo *HP Deskjet D2400 series*, esta impresora se conectará al servidor CUPS a través de un puerto USB (Universal Serial Bus) y será instalada siguiendo los pasos indicados en el capítulo A.6.2, seleccionando el propio modelo en la lista de *drivers*.

A.6.1. Instalación de CUPS

Para la instalación de CUPS se debe ejecutar el comando del cuadro A.33.

```
apt-get install cups cups-pdf
```

Cuadro A.33: Comando para instalar CUPS.

Al ejecutar este comando se instalará el servidor CUPS con una configuración predeterminada. Además, se ha decidido instalar una impresora PDF (Portable Document Format) virtual, es decir, una impresora que en lugar de imprimir en un medio físico exportará los documentos que se impriman como archivos PDF guardándolos en el equipo del servidor CUPS.

Una vez que se ha realizado la instalación, se utilizará la interfaz web para configurar el servidor, esto se debe a que la configuración de las diferentes impresoras a través del archivo de configuración puede ser muy complicada, mientras que a través de la interfaz web es un proceso muy simple.

Para que se pueda tener acceso al servidor CUPS mediante la página web es necesario realizar unos cambios en el archivo de configuración, ya que inicialmente el servidor CUPS solo acepta conexiones a través de la interfaz web del propio equipo, pero al instalarse en un equipo con Ubuntu Server™ no se dispone de

interfaz gráfica por lo que será necesario acceder desde otro equipo. Los cambios necesarios se deben realizar en el archivo de configuración que es el especificado en el cuadro A.34.

```
/etc/cups/cupsd.conf
```

Cuadro A.34: Ruta al archivo de configuración de CUPS en Ubuntu™.

En este archivo, entre otros parámetros, se encuentra la configuración de acceso al servidor a través de la interfaz web, que será la parte que se modificará. Para poder acceder correctamente se tendrá que localizar parte del archivo que se indica en el cuadro de código A.5 añadiendo las líneas 19, 23, 24 y 30 para que se permita una conexión desde otros equipos de la red interna.

```
14  WebInterface Yes
15  <Location />
16    # Allow shared printing...
17    Order allow,deny
18    Allow @LOCAL
19    Allow 192.168.10.0/24
20  </Location>
21  <Location /admin>
22    Order allow,deny
23    Require user @SYSTEM
24    Allow 192.168.10.0/24
25  </Location>
26  <Location /admin/conf>
27    AuthType Default
28    Require user @SYSTEM
29    Order allow,deny
30    Allow 192.168.10.0/24
31  </Location>
```

Código A.5: Código de configuración de CUPS.

Al realizar estos cambios se permite el acceso a la interfaz web a través de equipos que se encuentren en la red interna de la empresa, pero en caso de querer acceder a la zona de administración del servidor o a la zona de configuración del mismo, se solicitará al usuario que proporcione los datos del usuario y contraseña del administrador del equipo donde está el servidor CUPS instalado.

De esta manera, a pesar de que se pueda acceder a la interfaz web de CUPS desde otros equipos, solo se permite acceder a la parte de configuración o administración del mismo si se conoce el usuario administrador del servidor. Asimismo, al limitar el acceso al servidor desde únicamente la red interna de la empresa se minimiza el riesgo creado al permitir estas conexiones.

Una vez configurado el acceso web de forma correcta se debe puede acceder al mismo. Para ello, se debe abrir un navegador web y acceder a la dirección indicada en el cuadro A.35.

```
https://direccion_ip_servidor:631
```

Cuadro A.35: Dirección para acceder a CUPS.

Una vez se acceda a la interfaz web de forma correcta se mostrará la interfaz de la figura A.19.

Figura A.19: Interfaz principal del acceso web de CUPS.

Desde esta interfaz se puede acceder a la pestaña de administración, para lo cual se pedirá un usuario y una contraseña. Este usuario y contraseña deben ser los correspondientes al usuario y contraseña del administrador del equipo donde esté instalado el servidor CUPS.

Una vez introducidos los datos correctamente se mostrará la interfaz de la figura A.20 en la que se muestran las diferentes opciones de configuración más comunes y los accesos a los menús de impresoras y los diferentes archivos del servidor, tanto archivos de configuración como archivos de registro.

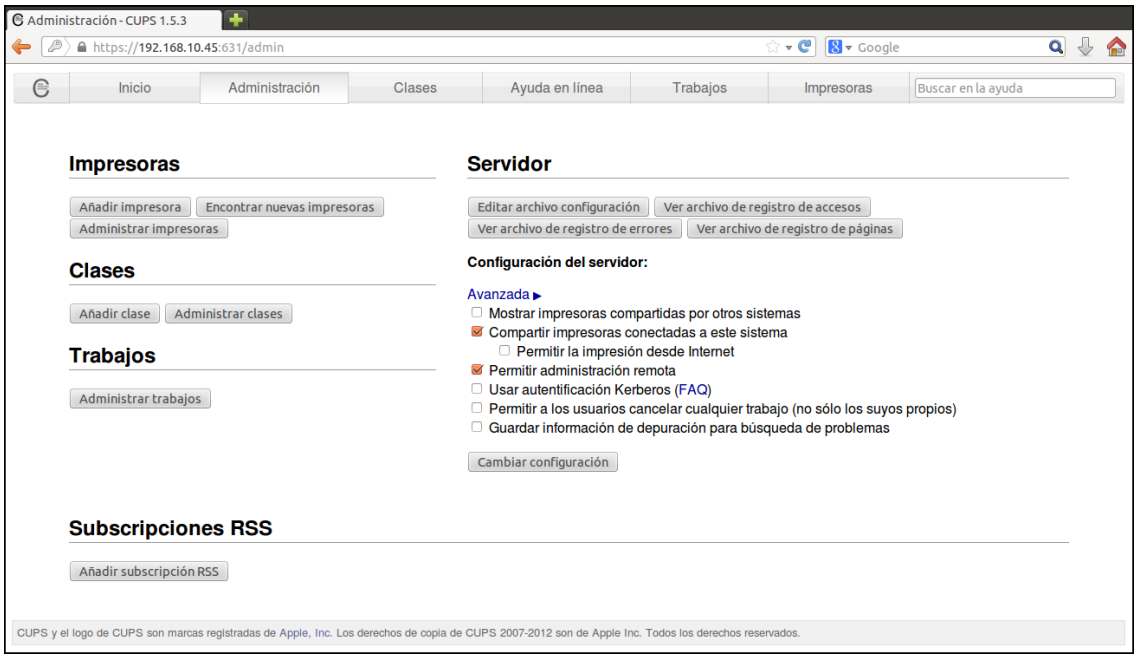

Figura A.20: Interfaz de administración del acceso web de CUPS.

Desde esta interfaz se podrá, por lo tanto, modificar toda la configuración de CUPS a través de las diferentes opciones y archivos que se muestran en la interfaz.

A.6.2. Configuración de las impresoras

Una vez se ha finalizado la configuración del servidor CUPS por completo, se deben instalar las diferentes impresoras para su utilización.

Para añadir una impresora al servidor se debe seleccionar la opción de “Añadir impresora”. Una vez seleccionada, aparecerá la interfaz de la figura A.21, donde se mostrarán las impresoras que se detecten conectadas al equipo del servidor CUPS. También se da la opción de elegir algunos protocolos de compartición de impresoras a través de internet, para poder integrarlas en el servidor CUPS en caso de ser necesario y, debido a que se realizó la instalación de la impresora PDF virtual, también aparece esta opción para seleccionarla.

Una vez se ha seleccionado una impresora aparecerá una nueva interfaz como la que se muestra en la figura A.22, en la que se deben se deben introducir datos de la impresora para que se pueda identificar, como nombre de la impresora y su localización.

Posteriormente, también se debe seleccionar el modelo de la impresora, esto se debe a que a través de esta selección CUPS selecciona el driver que tendrá que utilizar para enviarle los documentos a imprimir a esa impresora, de forma que no se produzcan errores de formato. Esta selección del modelo de la impresora se hace a través de una nueva interfaz como la que se muestra en la figura A.23.

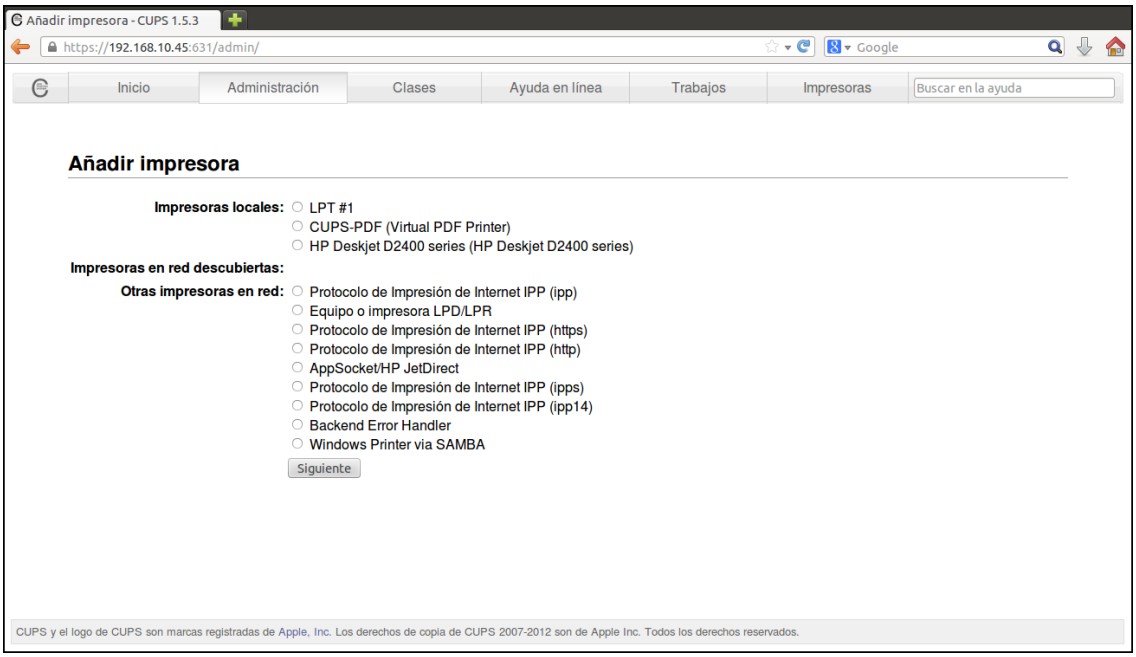

Figura A.21: Interfaz de añadir impresoras del acceso web de CUPS.

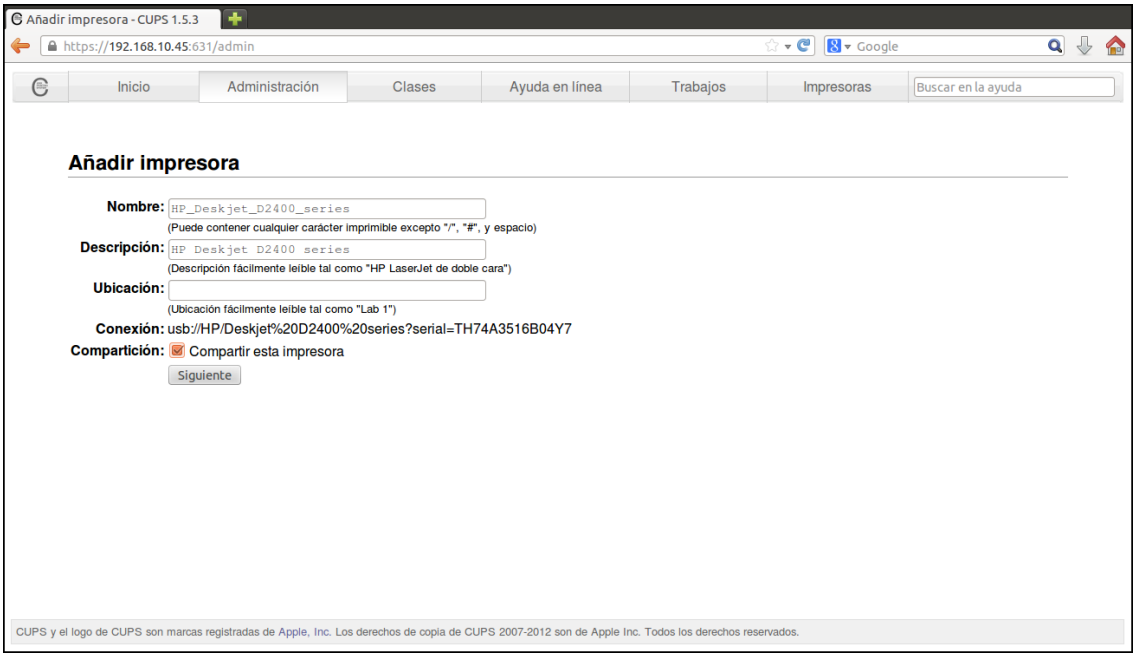

Figura A.22: Interfaz de datos para una impresora del acceso web de CUPS.

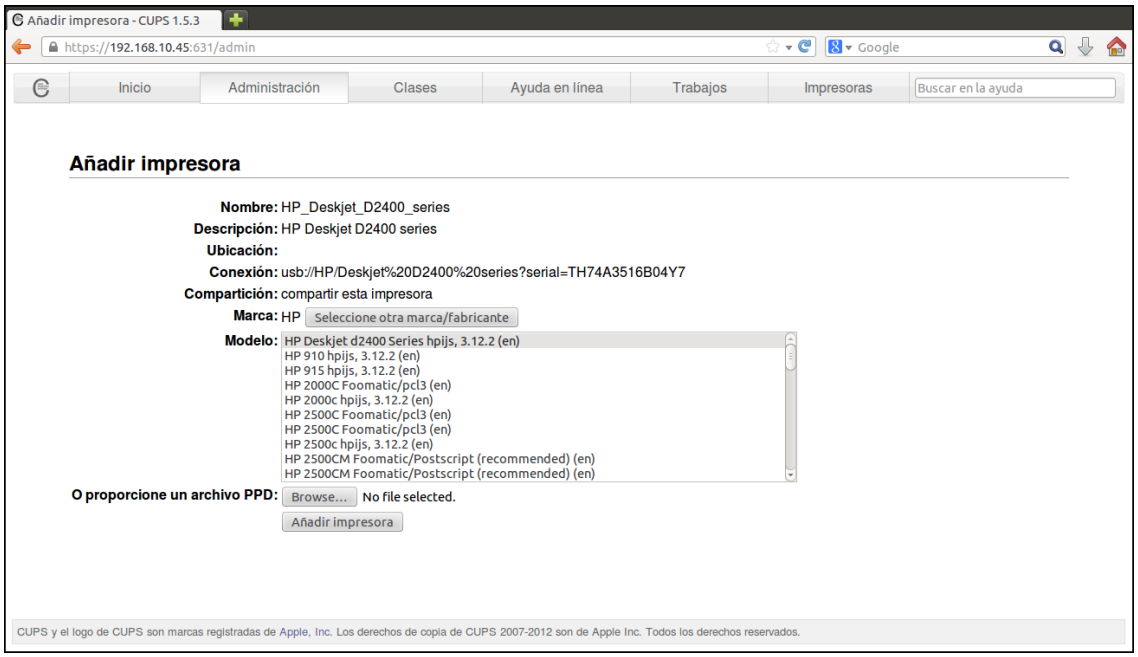

Figura A.23: Interfaz de selección de drivers del acceso web de CUPS.

A.6.3. Configuración impresora PDF virtual

Al igual que con el resto de impresoras, para la instalación de la impresora PDF virtual, se debe realizar el proceso de instalación en el servidor CUPS a través de la interfaz web. Sin embargo, a diferencia del resto de impresoras, en el caso de la impresora PDF virtual, la configuración de la misma está especificada en un archivo de configuración.

El archivo de configuración para la impresora PDF virtual es el indicado en el cuadro A.36.

```
/etc/cups/cups-pdf.conf
```

Cuadro A.36: Archivo de configuración de CUPS-PDF.

En este archivo se encuentra la configuración de como se deben tratar los diferentes documentos que sean impresos con la impresora virtual PDF. En este caso se ha utilizado la configuración por defecto, ya que mantiene una buena configuración en la que los documentos se guardan con el nombre del archivo que se ha mandado imprimir, utilizando, además, un código numérico para evitar que se sobrescriban documentos con el mismo nombre. Estos documentos se guardan en la carpeta personal del usuario en caso de ser un usuario del sistema o, en caso de no ser un usuario del sistema, se guardan en el directorio indicado en el cuadro de código A.6.

```
3 AnonDirName /var/spool/cups-pdf/ANONYMOUS
```

Código A.6: Código de configuración de CUPS-PDF.

A.7. Configuración de clientes

Para que los diferentes equipos de la red funcionen correctamente se deben realizar algunos ajustes en los mismos. Esto se debe a que los diferentes servicios prestados no están instalados en los diferentes equipos de forma predeterminada. Además, debido a que se ha creado una red propia, no hay posibilidad de utilizar un servicio de DNS, por lo que para un correcto funcionamiento de algunos servicios será necesario que se añadan algunas entradas al archivo de DNS de cada equipo.

A.7.1. Clientes Ubuntu™

Para que funcionen correctamente todos los servicios se tendrá que instalar algunos paquetes.

Para que funcione el servicio de FTP interno es necesario la utilización de cifrado SSL, y éste servicio no existe de forma predeterminada en los equipos con Ubuntu™. Para que se pueda conectar al servicio de FTP interno se deberá por tanto instalar el servicio de ftp-ssl. Para ello se debe ejecutar el comando del cuadro A.37.

```
apt-get install ftp-ssl
```

Cuadro A.37: Comando para instalar FTP-SSL en Ubuntu™.

Con este comando se instalará la extensión de FTP para usar cifrado SSL, por lo que se podrá conectar con el servidor de FTP interno correctamente.

Además, para que el cliente pueda conectar con la base de datos será necesario que se instale un cliente de PostgreSQL para que conecte con la misma. Por lo tanto, se tendrá que ejecutar el comando del cuadro A.38.

```
apt-get install postgresql-client-9.1
```

Cuadro A.38: Comano para instalar el cliente de PostgreSQL en Ubuntu™.

Con este comando se instalará el cliente de PostgreSQL permitiendo conectar con la base de datos correctamente.

Posteriormente, para que el servidor Samba funcione correctamente se debe modificar su archivo de configuración. Este se debe a lo comentado en el capítulo A.5 de que si no se configura correctamente, debido al funcionamiento de los navegadores de archivos de Ubuntu™, el servicio de Samba no funcionará bien. La configuración necesaria es la establecida en el cuadro de código A.7.

```
6 name resolve order = bcast host
```

Código A.7: Código de configuración de Samba.

Por otro lado, se tendrá que instalar las diferentes impresoras que se quieran utilizar en el equipo. Para ello se debe utilizar la interfaz propia de Ubuntu™ para instalar una impresora. Para ello, se seleccionará la opción de “Buscar impresora en la red” estableciendo la dirección IP del servidor CUPS. De esta manera, se buscarán las impresoras compartidas por el servidor CUPS permitiendo instalar la impresora que se quiera.

Por último, para que funcionen correctamente los servicios de correo electrónico y la página web, es necesario añadir diferentes entradas en el DNS del equipo. Para ello, se debe modificar el archivo indicado en el cuadro A.39.

```
/etc/hosts
```

Cuadro A.39: Archivo de DNS en Ubuntu™.

En este archivo se debe dejar una configuración como la que se establece en el cuadro de código A.8. Donde *192.168.2.6* es la dirección IP del equipo donde se ha instalado el servidor de correo, y *192.168.2.7* es la dirección IP del servidor web. De esta manera, al acceder a una de estas direcciones se obtendrá la dirección IP correcta funcionando correctamente.

```
1 127.0.0.1 localhost
2 127.0.1.1 ubuntu
3 192.168.2.6 smtp.dominio.com
4 192.168.2.6 pop3.dominio.com
5 192.168.2.6 imap.dominio.com
6 192.168.2.7 dominio.com
```

Código A.8: Código de configuración de DNS en Ubuntu™.

A.7.2. Clientes Windows™

Al igual que con los clientes Ubuntu™, en los clientes Windows™ también es necesario realizar algunos cambios e instalaciones.

La primera instalación a realizar será el cliente necesario para que funcione el servidor FTP interno correctamente. El cliente a instalar será el programa Filezilla™. Para ello, se debe descargar el cliente desde la página indicada en el cuadro A.40.

```
https://filezilla-project.org/download.php
```

Cuadro A.40: Página de descarga de Filezilla™.

Una vez se ha instalado el cliente se debe configurar la conexión con el servidor FTP. Para ello, se debe acceder al menú de “Gestor de sitios...”, una vez en este menú se deben introducir las características de la conexión. Un ejemplo de esta ventana con la configuración de una conexión se puede observar en la figura A.24.

Posteriormente, para que funcione correctamente el servicio de Samba, se debe comprobar el grupo de trabajo y asegurarse de que se utiliza el mismo grupo de trabajo que en el servidor Samba.

Para comprobar el grupo de trabajo del cliente Windows™ se deben seguir los siguientes pasos:

1.– Click en Inicio.

2.– Click con el botón derecho en Equipo.

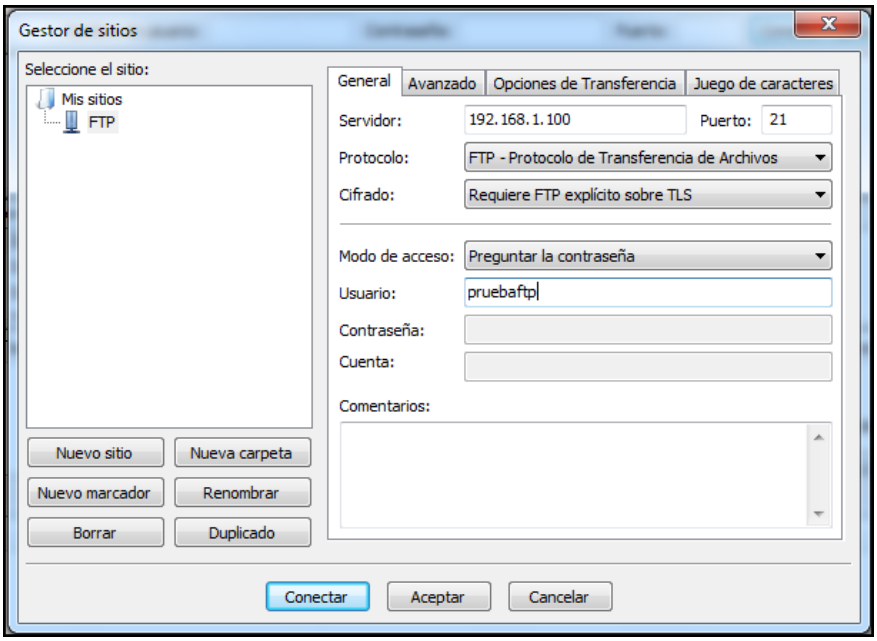

Figura A.24: Interfaz de conexión de `Filezilla`™.

3.– Comprobar en la parte inferior de la ventana que se abre el grupo de trabajo. En caso de querer cambiarlo pulsar en “Cambiar configuración”.

Por último, al igual que en los clientes `Ubuntu`™ se tendrá que modificar el archivo de DNS del equipo. Para ello, se deberá modificar el archivo indicado en el cuadro A.41.

```
C:/Windows/System32/drivers/etc/hosts
```

Cuadro A.41: Archivo de DNS en Windows™.

Al igual que en el archivo de DNS en `Ubuntu`™, se deberán realizar algunos cambios. Estos están indicados en el cuadro de código A.9.

```
22 192.168.2.6 smtp.dominio.com
23 192.168.2.6 pop3.dominio.com
24 192.168.2.6 imap.dominio.com
25 192.168.2.7 dominio.com
```

Código A.9: Código de DNS en Windows™.

B

Herramientas de la auditoría

B.1. Kali™

Kali™ es una distribución de GNU/Linux™ creada específicamente para la realización de *Test de Penetración*. Es una distribución basada en Debian pero que utiliza repositorios propios para las actualizaciones.

La gran ventaja de utilizar Kali™ frente a otros sistemas operativos, es que, al haber sido creado específicamente para realizar *Test de Penetración*, tiene un gran número de herramientas para este propósito.

Además, Kali™ tiene una configuración por defecto que evita acciones que podrían incluir entradas en los registros de una red a la que se conectara, como por ejemplo se desactiva las peticiones DHCP para evitar aparecer en el log del mismo.

Para obtener Kali™ se debe acceder a su página web oficial [9] en la que se pueden obtener diferentes distribuciones, como imágenes de máquinas virtuales, o imágenes para montar en una memoria USB.

Para más detalles acerca del funcionamiento de Kali™ o de sus características, se puede acceder también a su página web oficial [9].

B.2. Nessus™

Nessus™ es un programa de escáner de vulnerabilidades creado por *Tenable*. Es una herramienta muy útil, ya que cuenta con una gran base de datos con más de 60.000 vulnerabilidades que está en constante actualización por expertos de *Tenable*.

B.2.1. Instalación

Para la instalación de Nessus™ se debe acceder a la página oficial de descarga, que se muestra en el cuadro B.1 y seleccionar el paquete acorde con el sistema operativo que se utilice.

http://www.tenable.com/products/nessus/select-your-operating-system

Cuadro B.1: Página de descarga de Nessus™.

Una vez descargado el paquete se procede a su instalación. Para ello se debe utilizar el comando del cuadro B.2.

```
dpkg -i Nessus-5.2.1-debian6_amd64.deb
```

Cuadro B.2: Comando para instalar Nessus™.

Una vez utilizado el comando se tiene Nessus™ instalado. Para acceder a el se debe introducir en un navegador web la dirección del cuadro B.3.

```
https://127.0.0.1:8834
```

Cuadro B.3: Página para acceder a Nessus™.

Una vez accedido a Nessus™ se den introducir los datos solicitados, para poder cumplimentar correctamente todos los campos, se debe contar con un usuario de Tenable, por lo que una vez registrado en la página se completan estos datos accediendo a Nessus™.

B.2.2. Utilización

Para realizar escáneres de vulnerabilidades con Nessus™ se utilizará su interfaz web, la cual se utilizó en la última parte de la instalación. Para acceder a ella se debe introducir la dirección del cuadro B.3 en un navegador web e introducir los datos solicitados.

Una vez en la interfaz principal de Nessus™, la cual se puede observar en la imagen B.1, se deben introducir los datos de acceso del usuario. Una vez hecho esto, se debe acceder a la pestaña de *Scan*, la cual se puede observar en la imagen. En ella se selecciona la opción de *New Scan*.

Al realizar esta selección se abre la interfaz donde se debe establecer el objetivo del escáner, ya sea un equipo o una red, la política del escáner y un nombre para poder identificarlo. Una vez seleccionados estos datos se comienza el escáner y, una vez finalizado el mismo, podremos ver el resultado seleccionando el análisis desde la pestaña de *Scan*. Las diferentes interfaces recorridas a lo largo de este proceso son las que se pueden observar en las figuras B.2 y B.3.

B.3. Metasploit™

Metasploit™ es un software de *Test de Penetración*. Este programa incluye una base de datos con un gran número de errores de seguridad junto con pequeños *scripts* que sirven para vulnerar estos fallos.

Por lo tanto, al usar esta herramienta junto con un informe de vulnerabilidades de una red, se pueden comprobar si las vulnerabilidades que hay en el informe existen realmente o si son falsos positivos, es decir, que aunque se hallan detectado no existan.

B.3.1. Instalación

Puesto que se utilizará Kali™ no será necesario instalar Metasploit™ puesto que viene incorporado en esta distribución de Linux™.

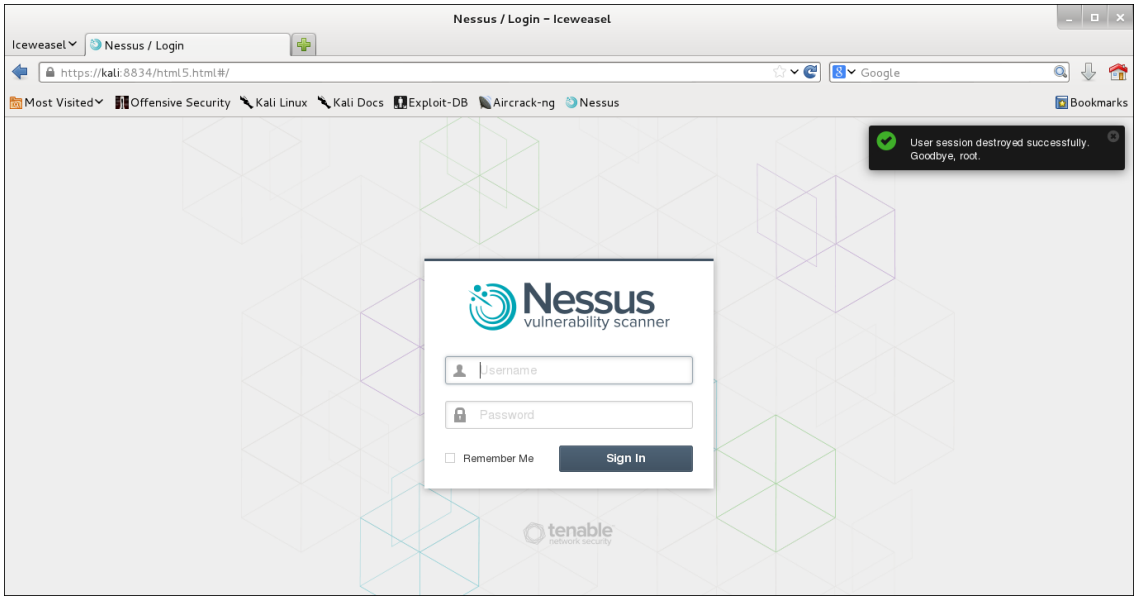

Figura B.1: Pantalla inicial de Nessus™.

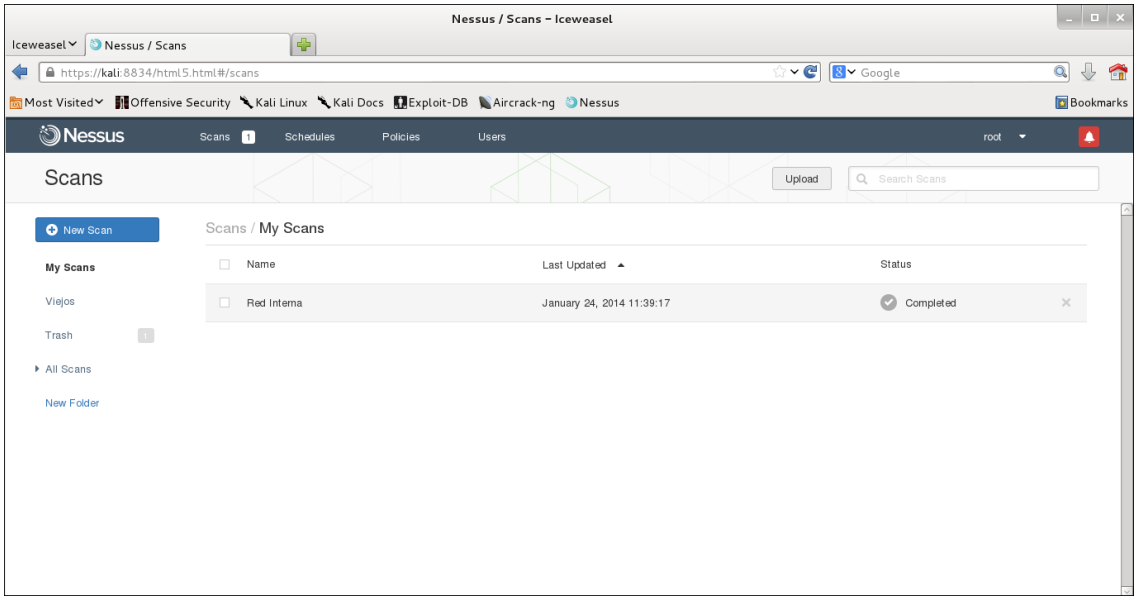

Figura B.2: Pestaña de *Scan* de Nessus™.

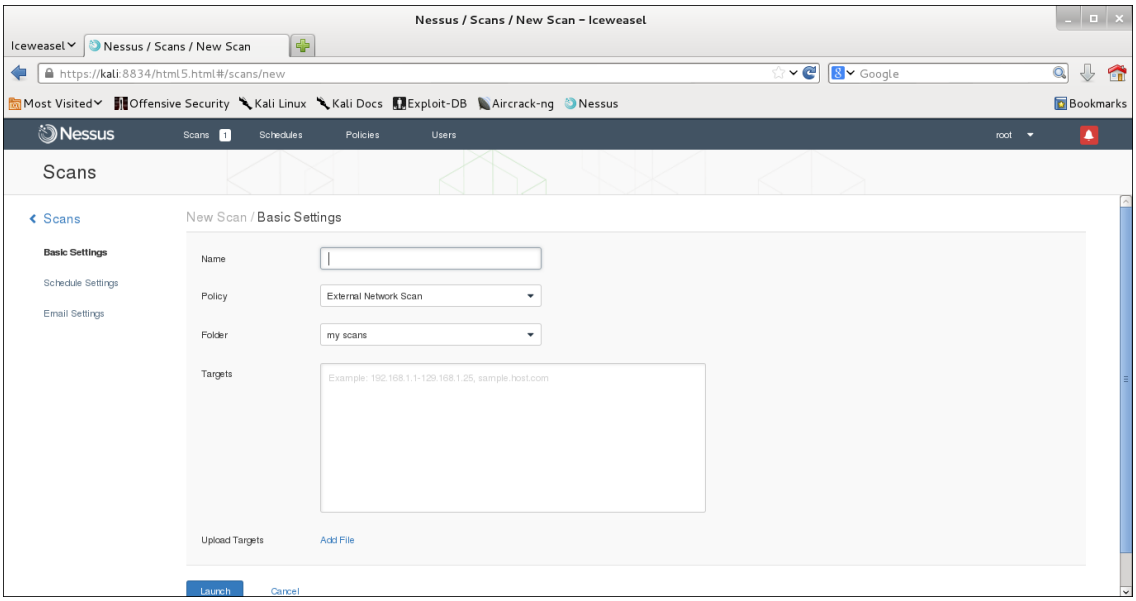

Figura B.3: Interfaz de configuración de análisis de Nessus™.

Sin embargo, será necesario actualizar el software puesto que las diferentes vulnerabilidades existentes cambian rápidamente. Para actualizar el sistema hay que utilizar el comando del cuadro B.4, con el cual se actualiza la base de datos de vulnerabilidades del programa.

```
msfupdate
```

Cuadro B.4: Comando para actualizar Metasploit™.

B.3.2. Utilización

Para utilizar Metasploit™ existen diferentes interfaces. Sin embargo, la interfaz más utilizada, y la que se utilizará para la realización del proyecto, es a través de la consola del sistema. Para abrir Metasploit™ en una consola se debe utilizar el comando del cuadro B.5.

```
msfconsole
```

Cuadro B.5: Comando para abrir Metasploit™.

Una vez abierta la consola de Metasploit™ se pueden utilizar diferentes comandos para navegar, para ver los diferentes comandos se puede utilizar la ayuda propia del programa o se pueden utilizar los manuales de su página web oficial [11]. Sin embargo, en su utilización habitual solo se utilizan unos pocos comandos, algunos de ellos son los del cuadro B.6.

El primer comando del cuadro sirve para buscar vulnerabilidad a partir de sus descripciones. El segundo se utiliza para, una vez localizado la vulnerabilidad a usar, seleccionarla para su utilización. Por último, el último comando del cuadro se utiliza para mostrar las diferentes cargas que puede llevar la vulnerabilidad seleccionada

```
search ''vulnerabilidad''
use ''ruta vulnerabilidad''
show payloads
```

Cuadro B.6: Comandos para buscar y usar vulnerabilidades, y mostrar las cargas de una vulnerabilidad en Metasploit™.

para su utilización.

B.4. Otros

B.4.1. Traceroute

Traceroute es un programa incluido en Kali™ que se utiliza para averiguar cuáles son los diferentes *routers* que atraviesa un paquete antes de llegar a su destino. Para ello, el programa envía paquetes al destino pero que solo pueden atravesar un número determinado de *routers*. De esta manera, iniciando el número de *routers* a atravesar indicado por el TTL (Time To Live), se puede controlar por donde viaja el paquete comprobando quien devuelve el paquete enviado.

Para su utilización se debe utilizar la consola, en la cual se debe introducir el comando que se muestra en el cuadro B.7. Una vez introducido ese comando, a continuación se muestran las direcciones IP de los diferentes *router* que atraviesan los paquetes antes de llegar al destino indicado.

```
traceroute destino
```

Cuadro B.7: Comando Traceroute.

B.4.2. Hydra

Hydra es un programa incluido en Kali™ cuya función es la realización de ataques por fuera bruta. Este tipo de ataques consisten en la prueba de diferentes credenciales de usuario hasta encontrar con uno correcto. Para ello usualmente se utilizan diccionarios, estos son un conjunto de usuarios o contraseñas comunes, los cuales son probados por el programa como credenciales de usuario.

Para su utilización se debe utilizar la consola de comandos de Kali™. Para utilizarlo se utilizan comandos en los que se indican tanto los diccionarios a utilizar como el objetivo a atacar. La estructura de los comandos es la que se muestra en el cuadro B.8.

```
hydra -L dicc_usuarios -P dicc_contraseñas IP_objetivo
servicio
```

Cuadro B.8: Estructura de comando de Hydra.

Como se puede observar en el cuadro, se debe introducir tanto el diccionario de usuarios y contraseñas como el objetivo y el protocolo a utilizar. Para el protocolo existen un gran número de opciones entre los que se encuentran FTP y `Samba`.

Un ejemplo de uso de `Hydra` sería el mostrado en el cuadro B.9. En este ejemplo se utilizan los archivos *usuarios.txt* y *password.txt* como diccionarios de usuarios y contraseñas respectivamente, el objetivo a atacar es el equipo con dirección IP *192.168.2.6* y se tratará de averiguar los credenciales de usuario del servicio FTP.

```
hydra -L usuarios.txt -P password.txt 192.168.1.6 ftps
```

Cuadro B.9: Ejemplo de comando de `Hydra`.

Para más información acerca de los servicios que `Hydra` puede atacar o acerca de su funcionamiento se puede consultar su página de manual [10].

C

Archivos de configuración

En esta parte del proyecto se presentarán los diferentes archivos de configuración de los diferentes servicios. De esta forma, se puede consultar la configuración completa de los diferentes servicios.

C.1. FTP

C.1.1. FTP Interno

proftpd.conf

```
# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6     on
# If set on you can experience a longer connection delay in many cases.
IdentLookups    off

ServerName    "Debian"
ServerType    standalone
DeferWelcome    off

MultilineRFC2228  on
DefaultServer    on
ShowSymlinks    on

TimeoutNoTransfer  600
TimeoutStalled    600
TimeoutIdle    1200

DisplayLogin welcome.msg
DisplayChdir  .message true
ListOptions  "-l"

DenyFilter    \*.*/

# Use this to jail all users in their homes
 DefaultRoot    ~
# Port 21 is the standard FTP port.
Port     21

<IfModule mod_dynmasq.c>
# DynMasqRefresh 28800
</IfModule>

# To prevent DoS attacks, set the maximum number of child processes
# to 30.
```

```
MaxInstances    30

# Set the user and group that the server normally runs at.
User    proftpd
Group    nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask    022 022
# Normally, we want files to be overwriteable.
AllowOverwrite    on

TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log

<IfModule mod_quotatab.c>
QuotaEngine off
</IfModule>

<IfModule mod_ratio.c>
Ratios off
</IfModule>

<IfModule mod_delay.c>
DelayEngine on
</IfModule>

<IfModule mod_ctrls.c>
ControlsEngine off
ControlsMaxClients 2
ControlsLog /var/log/proftpd/controls.log
ControlsInterval 5
ControlsSocket /var/run/proftpd/proftpd.sock
</IfModule>

<IfModule mod_ctrls_admin.c>
AdminControlsEngine off
</IfModule>

# Alternative authentication frameworks

# This is used for FTPS connections
Include /etc/proftpd/tls.conf

# Include other custom configuration files
Include /etc/proftpd/conf.d/
```

tls.conf

```
<IfModule mod_tls.c>
TLSEngine on
TLSLog /var/log/proftpd/tls.log
TLSProtocol SSLv23

# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.

TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key

# Authenticate clients that want to use FTP over TLS?

TLSVerifyClient off

# Are clients required to use FTP over TLS when talking to this server?

TLSRequired on
</IfModule>
```

C.1.2. FTP Externo

proftpd.conf

```
# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6    on
# If set on you can experience a longer connection delay in many cases.
IdentLookups    off

ServerName    "Debian"
ServerType    standalone
DeferWelcome    off

MultilineRFC2228  on
DefaultServer    on
ShowSymlinks    on

TimeoutNoTransfer  600
TimeoutStalled    600
TimeoutIdle    1200

DisplayLogin welcome.msg
DisplayChdir  .message true
ListOptions  "-l"

DenyFilter    \*.*/

# Use this to jail all users in their homes
 DefaultRoot    ~
# Port 21 is the standard FTP port.
Port    21
```

```
# To prevent DoS attacks, set the maximum number of child processes
# to 30.

MaxInstances    30

# Set the user and group that the server normally runs at.
User    proftpd
Group    nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask    022 022
# Normally, we want files to be overwriteable.
AllowOverwrite    on

TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log

<IfModule mod_quotatab.c>
QuotaEngine off
</IfModule>

<IfModule mod_ratio.c>
Ratios off
</IfModule>

<IfModule mod_delay.c>
DelayEngine on
</IfModule>

<IfModule mod_ctrls.c>
ControlsEngine off
ControlsMaxClients 2
ControlsLog /var/log/proftpd/controls.log
ControlsInterval 5
ControlsSocket /var/run/proftpd/proftpd.sock
</IfModule>

<IfModule mod_ctrls_admin.c>
AdminControlsEngine off
</IfModule>

# This is used for FTPS connections
Include /etc/proftpd/tls.conf

# Useful to keep VirtualHost/VirtualRoot directives separated
#Include /etc/proftpd/virtuals.con

# A basic anonymous configuration, no upload directories.

 <Anonymous ~ftp>
   User    ftp
   Group    nogroup
   # We want clients to be able to login with "anonymous" as well as "ftp"
   UserAlias    anonymous ftp
   # Cosmetic changes, all files belongs to ftp user
   DirFakeUser on ftp
   DirFakeGroup on ftp

   RequireValidShell  off

   # Limit the maximum number of anonymous logins
   MaxClients    10

   # We want `welcome.msg` displayed at login, and `.message` displayed
   # in each newly chdired directory.
   DisplayLogin    welcome.msg
   DisplayChdir    .message
```

```
    # Limit WRITE everywhere in the anonymous chroot
    <Directory *>
      <Limit WRITE>
        Allow 192.168.1.*
        DenyAll
      </Limit>
    </Directory>

  </Anonymous>

# Include other custom configuration files
Include /etc/proftpd/conf.d/
```

tls.conf

```
<IfModule mod_tls.c>
TLSEngine on
TLSLog /var/log/proftpd/tls.log
TLSProtocol SSLv23

# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.

TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key

# Authenticate clients that want to use FTP over TLS?

TLSVerifyClient off

# Are clients required to use FTP over TLS when talking to this server?

TLSRequired on
</IfModule>
```

C.2. Servidor de correo

10-auth.conf

```
# Authentication processes

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
disable_plaintext_auth = yes
```

10-logging.conf

```
# Log destination.

# In case of password mismatches, log the attempted password. Valid values are
# no, plain and sha1. sha1 can be useful for detecting brute force password
# attempts vs. user simply trying the same password over and over again.
auth_verbose_passwords = sha1
```

10-mail.conf

```
# Mailbox locations and namespaces

# Location for users' mailboxes.
# If you're using mbox, giving a path to the INBOX file (eg. /var/mail/%u)
# isn't enough. You'll also need to tell Dovecot where the other mailboxes are
# kept. This is called the "root mail directory", and it must be the first
# path given in the mail_location setting.

mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

20-imap.conf

```
# IMAP specific settings

protocol imap {
  # Maximum IMAP command line length.
  imap_max_line_length = 64k

  # Maximum number of IMAP connections allowed for a user from each IP address.
  mail_max_userip_connections = 10

  # Space separated list of plugins to load (default is global mail_plugins).
  mail_plugins = $mail_plugins
}
```

dovecot.conf

```
## Dovecot configuration file

# Enable installed protocols
!include_try /usr/share/dovecot/protocols.d/*.protocol

# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
listen = *, ::

# Most of the actual configuration gets included below. The filenames are
# first sorted by their ASCII value and parsed in that order. The 00-prefixes
# in filenames are intended to make it easier to understand the ordering.
!include conf.d/*.conf

# A config file can also tried to be included without giving an error if
# it's not found:
!include_try local.conf
```

main.cf

```
smtpd_banner = myhostnameESMTPmail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

readme_directory = no

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database =
    btree:data_directory/smtpd_scachesmtp_tls_session_cache_database = btree :
    {data_directory}/smtp_scache

myhostname = ubuntu
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = dominio.com, ubuntu, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24
mailbox_size_limit = 51200000
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

C.3. Base de datos interna

pg_hba.conf

```
# PostgreSQL Client Authentication Configuration File
# Database administrative login by Unix domain socket
local all postgres peer

# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all peer
# IPv4 local connections:
host all all 127.0.0.1/32 md5
host all  all  192.168.1.0/24  md5
# IPv6 local connections:
host all all ::1/128 md5
```

postgresql.conf

```
# PostgreSQL configuration file

data_directory = '/var/lib/postgresql/9.1/main'  # use data in another directory
hba_file = '/etc/postgresql/9.1/main/pg_hba.conf' # host-based authentication file
ident_file = '/etc/postgresql/9.1/main/pg_ident.conf' # ident configuration file
external_pid_file = '/var/run/postgresql/9.1-main.pid'  # write an extra PID file

listen_addresses = '*'  # what IP address(es) to listen on;
port = 5432    # (change requires restart)
max_connections = 100   # (change requires restart)
unix_socket_directory = '/var/run/postgresql'  # (change requires restart)

# - Security and Authentication -
ssl = true    # (change requires restart)

shared_buffers = 24MB   # min 128kB
log_line_prefix = '%t '   # %t = timestamp without milliseconds

# These settings are initialized by initdb, but they can be changed.
lc_messages = 'en_US.UTF-8'   # locale for system error message
                      # strings
lc_monetary = 'en_US.UTF-8'   # locale for monetary formatting
lc_numeric = 'en_US.UTF-8'   # locale for number formatting
lc_time = 'en_US.UTF-8'    # locale for time formatting

# default configuration for text search
default_text_search_config = 'pg_catalog.english'
```

C.4. Servidor Samba

smb.conf

```
[global]
    workgroup = WORKGROUP
    netbios name = SAMBA
    server string = %h server (Samba, Ubuntu)
    dns proxy = no
    name resolve order = bcast host

    interfaces = 192.168.1.0/24 eth0
    bind interfaces only = yes

    log file = /var/log/samba/log.%m
    max log size = 1000
    syslog = 1

    panic action = /usr/share/samba/panic-action %d
    security = user
    encrypt passwords = true
    passdb backend = tdbsam
    obey pam restrictions = yes
    unix password sync = yes
    passwd program = /usr/bin/passwd %u
    passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
        *password\supdated\ssuccessfully* .
    pam password change = yes
    map to guest = never
    usershare allow guests = no

[public]
     comment = Carpeta publica
     path = /home/public
     read only = no
     create mask = 0744
     valid users = @sambashare

[sambamalo]
     comment = Carpeta de Sambamalo
     path = /home/sambamalo
     valid users = sambamalo
     read only = no

[sambamedio]
     comment = Carpeta de Sambamedio
     path = /home/sambamedio
     valid users = sambamedio
     read only = no

[sambabueno]
     comment = Carpeta de Sambabueno
     path = /home/sambabueno
     valid users = sambabueno
     read only = no
```

C.5. Servidor de impresión Linux

cupsd.conf

```
LogLevel warn
MaxLogSize 1m
SystemGroup lpadmin
# Allow remote access
Port 631
Listen /var/run/cups/cups.sock
# Share local printers on the local network.
Browsing On
BrowseOrder allow,deny
BrowseRemoteProtocols
BrowseAddress @LOCAL
BrowseLocalProtocols CUPS dnssd
DefaultAuthType Basic
WebInterface Yes
<Location />
  # Allow shared printing...
  Order allow,deny
  Allow @LOCAL
  Allow 192.168.10.0/24
</Location>
<Location /admin>
  Order allow,deny
  Require user @SYSTEM
  Allow 192.168.10.0/24
</Location>
<Location /admin/conf>
  AuthType Default
  Require user @SYSTEM
  Order allow,deny
  Allow 192.168.10.0/24
</Location>
<Policy default>
  JobPrivateAccess default
  JobPrivateValues default
  SubscriptionPrivateAccess default
  SubscriptionPrivateValues default
  <Limit Create-Job Print-Job Print-URI Validate-Job>
    Order deny,allow
  </Limit>
  <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job Purge-Jobs
      Set-Job-Attributes Create-Job-Subscription Renew-Subscription Cancel-Subscription
      Get-Notifications Reprocess-Job Cancel-Current-Job Suspend-Current-Job
      Resume-Job Cancel-My-Jobs Close-Job CUPS-Move-Job CUPS-Get-Document>
    Require user @OWNER @SYSTEM
    Order deny,allow
  </Limit>
  <Limit CUPS-Add-Modify-Printer CUPS-Delete-Printer CUPS-Add-Modify-Class
      CUPS-Delete-Class CUPS-Set-Default CUPS-Get-Devices>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
  </Limit>
```

```
  <Limit Pause-Printer Resume-Printer Enable-Printer Disable-Printer
      Pause-Printer-After-Current-Job Hold-New-Jobs Release-Held-New-Jobs
      Deactivate-Printer Activate-Printer Restart-Printer Shutdown-Printer Startup-Printer
      Promote-Job Schedule-Job-After Cancel-Jobs CUPS-Accept-Jobs
      CUPS-Reject-Jobs>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
  </Limit>
  <Limit Cancel-Job CUPS-Authenticate-Job>
    Require user @OWNER @SYSTEM
    Order deny,allow
  </Limit>
  <Limit All>
    Order deny,allow
  </Limit>
</Policy>
<Policy authenticated>
  JobPrivateAccess default
  JobPrivateValues default
  SubscriptionPrivateAccess default
  SubscriptionPrivateValues default
  <Limit Create-Job Print-Job Print-URI Validate-Job>
    AuthType Default
    Order deny,allow
  </Limit>
  <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job Purge-Jobs
      Set-Job-Attributes Create-Job-Subscription Renew-Subscription Cancel-Subscription
      Get-Notifications Reprocess-Job Cancel-Current-Job Suspend-Current-Job
      Resume-Job Cancel-My-Jobs Close-Job CUPS-Move-Job CUPS-Get-Document>
    AuthType Default
    Require user @OWNER @SYSTEM
    Order deny,allow
  </Limit>
  <Limit CUPS-Add-Modify-Printer CUPS-Delete-Printer CUPS-Add-Modify-Class
      CUPS-Delete-Class CUPS-Set-Default>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
  </Limit>
  <Limit Pause-Printer Resume-Printer Enable-Printer Disable-Printer
      Pause-Printer-After-Current-Job Hold-New-Jobs Release-Held-New-Jobs
      Deactivate-Printer Activate-Printer Restart-Printer Shutdown-Printer Startup-Printer
      Promote-Job Schedule-Job-After Cancel-Jobs CUPS-Accept-Jobs
      CUPS-Reject-Jobs>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
  </Limit>
  <Limit Cancel-Job CUPS-Authenticate-Job>
    AuthType Default
    Require user @OWNER @SYSTEM
    Order deny,allow
  </Limit>
  <Limit All>
    Order deny,allow
  </Limit>
</Policy>
```

cups-pdf.conf

```
Out ${HOME}/PDF

AnonDirName /var/spool/cups-pdf/ANONYMOUS

### Key: Label
## label all jobs with a unique job-id in order to avoid overwriting old
## files in case new ones with identical names are created; always true for
## untitled documents
## 0: label untitled documents only
## 1: label all documents with a preceeding "job_#-"
## 2: label all documents with a tailing "-job_#"
### Default: 0

Label 2

### Key: Grp
## group cups-pdf is supposed to run as - this will also be the gid for all
## created directories and log files
### Default: lp

Grp lpadmin

### Key: DecodeHexStrings
## this option will try to decode hex strings in the title to allow
## internationalized titles
## (have a look at contrib/pstitleconv for a suitable filter for data
## from Windows clients)
## 0: disable, 1: enable
### Default: 0

DecodeHexStrings 1
```

printers.conf

```
# Printer configuration file for CUPS v1.5.3
# Written by cupsd
# DO NOT EDIT THIS FILE WHEN CUPSD IS RUNNING
<Printer prueba>
UUID urn:uuid:a6eb3811-3a21-3cf9-50bd-ab102b10ab57
Info Virtual PDF Printer
Location asd
MakeModel Generic CUPS-PDF Printer
DeviceURI cups-pdf:/
State Idle
StateTime 1384339803
Type 8450124
Accepting Yes
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
```

```
ErrorPolicy retry-job
</Printer>
<DefaultPrinter HP_Deskjet_D2400_series>
UUID urn:uuid:1f603646-ea2a-37cc-63ab-7d8ad927d4cb
Info HP Deskjet D2400 series
Location Servidor CUPS
MakeModel HP Deskjet d2400 Series hpijs, 3.12.2
DeviceURI usb://HP/Deskjet%20D2400%20series?serial=TH74A3516B04Y7
State Idle
StateTime 1384339665
Type 8425484
Accepting Yes
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy retry-job
</Printer>
<Printer Virtual_PDF_Printer>
UUID urn:uuid:4f710428-b33a-354a-5b20-bbf553a200a0
Info Virtual PDF Printer
Location
MakeModel Generic CUPS-PDF Printer
DeviceURI cups-pdf:/
State Idle
StateTime 1382195125
Type 8450124
Accepting Yes
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy retry-job
</Printer>
```

D

Resultados análisis de vulnerabilidades

A continuación se presentan los informes técnicos de los análisis de vulnerabilidades realizados a la red. Estos informes son generados de forma automática por Nessus™, seleccionando únicamente los módulos a incluir en el informe. Debido a esto, la numeración de las páginas no corresponde con al numeración del proyecto, sino que corresponde con la numeración del propio informe.

D.1. Análisis desde el exterior de la red

El informe presentado a continuación corresponde con el informe automático generado por Nessus™ tras la realización del análisis desde el exterior de la red.

Con este análisis se pueden observar las diferentes vulnerabilidades que podría explotar cualquier usuario, puesto que se tratan de las accesibles desde internet.

Las vulnerabilidades que aparecen en este análisis son muy importantes, puesto que, como se ha comentado, cualquier usuario podría explotarlas.

El informe consiste en un resumen ejecutivo de las diferentes vulnerabilidades existentes. En este resumen se presentan las diferentes vulnerabilidades existentes en cada equipo, ordenadas según un código de color en función de la severidad de la misma. De esta manera, de cada vulnerabilidad se presenta: su severidad, el código de la vulnerabilidad y una breve descripción.

No se han añadido los detalles de las vulnerabilidades puesto que las presentes en este informe aparecen también en el informe realizado desde la red privada, por lo que si se quiere ver en detalle alguna vulnerabilidad se puede consultar el mismo.

192.168.2.5

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	19506	Nessus Scan Information

192.168.2.6

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	20	24

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12218	mDNS Detection (Remote Network)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10185	POP Server Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11414	IMAP Service Banner Retrieval
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	42085	IMAP Service STARTTLS Command Support
Info	42087	POP3 Service STLS Command Support
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

192.168.2.7

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	21	25

Details

Severity	Plugin Id	Name
Medium (5.0)	12218	mDNS Detection (Remote Network)
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (4.3)	69280	Joomla! libraries/idna_convert/example.php lang Parameter XSS
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10662	Web mirroring
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21142	Joomla! Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39521	Backported Security Patch Detection (WWW)
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	49704	External URLs
Info	54615	Device Type
Info	66334	Patch Report

192.168.2.105

Summary

Critical	High	Medium	Low	Info	Total
4	5	5	5	50	69

Details

Severity	Plugin Id	Name
Critical (10.0)	25216	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow
Critical (10.0)	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Critical (10.0)	33850	Unsupported Unix Operating System
Critical (10.0)	34970	Apache Tomcat Manager Common Administrative Credentials
High (7.8)	55976	Apache HTTP Server Byte Range DoS
High (7.5)	17210	TWiki ImageGalleryPlugin Shell Command Injection
High (7.5)	19704	TWiki rev Parameter Arbitrary Command Execution
High (7.5)	34460	Unsupported Web Server Detection
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (5.0)	11229	Web Server info.php / phpinfo.php Detection
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	35806	Tomcat Sample App cal2.jsp time Parameter XSS (CVE-2009-0781)
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Low (2.6)	34850	Web Server Uses Basic Authentication Without HTTPS
Low (2.6)	42263	Unencrypted Telnet Server
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10028	DNS Server BIND version Directive Remote Version Disclosure
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10267	SSH Server Type and Version Information
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information

Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10662	Web mirroring
Info	10719	MySQL Server Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10881	SSH Protocol Versions Supported
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11032	Web Server Directory Enumeration
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11419	Web Server Office File Inventory
Info	11422	Web Server Unconfigured - Default Install Page Present
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	19941	TWiki Detection
Info	20108	Web Server / Application favicon.ico Vendor Fingerprinting
Info	22964	Service Detection
Info	24004	WebDAV Directory Enumeration
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	25240	Samba Server Detection
Info	26024	PostgreSQL Server Detection
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	39446	Apache Tomcat Default Error Page Version Detection
Info	39520	Backported Security Patch Detection (SSH)

Info	39521	Backported Security Patch Detection (WWW)
Info	40984	Browsable Web Directories
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	49704	External URLs
Info	49705	Web Server Harvested Email Addresses
Info	54615	Device Type
Info	60119	Microsoft Windows SMB Share Permissions Enumeration
Info	66334	Patch Report
Info	70657	SSH Algorithms and Languages Supported

D.2. Análisis desde la zona pública de la red

El informe presentado a continuación corresponde con el informe automático generado por Nessus™ tras la realización del análisis desde la zona pública de la red.

Con este análisis se pueden observar las diferentes vulnerabilidades que podría explotar un empleado. Éstas no son tan accesibles, por lo que no existe un gran número de usuarios que pueda explotarlas. Sin embargo, puesto que existen vulnerabilidades en los servicios mas importantes de la red, cobran una gran importancia.

El informe consiste en un resumen ejecutivo de las diferentes vulnerabilidades existentes. En este resumen se presentan las diferentes vulnerabilidades existentes en cada equipo, ordenadas según un código de color en función de la severidad de la misma. De esta manera, de cada vulnerabilidad se presenta: su severidad, el código de la vulnerabilidad y una breve descripción.

No se han añadido los detalles de las vulnerabilidades puesto que las presentes en este informe aparecen también en el informe realizado desde la red privada, por lo que si se quiere ver en detalle alguna vulnerabilidad se puede consultar el mismo.

192.168.2.5

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	3	21	29

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	10079	Anonymous FTP Enabled
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	34324	FTP Supports Clear Text Authentication
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10092	FTP Server Detection
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39519	Backported Security Patch Detection (FTP)
Info	42149	FTP Service AUTH TLS Command Support
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported

Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

192.168.2.6

Summary

Critical	High	Medium	Low	Info	Total
0	0	4	2	26	32

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10185	POP Server Detection
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11414	IMAP Service Banner Retrieval
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42085	IMAP Service STARTTLS Command Support
Info	42087	POP3 Service STLS Command Support
Info	42088	SMTP Service STARTTLS Command Support
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported

Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66717	mDNS Detection (Local Network)
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

192.168.2.7

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	1	24	27

Details

Severity	Plugin Id	Name
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (4.3)	69280	Joomla! libraries/idna_convert/example.php lang Parameter XSS
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10662	Web mirroring
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21142	Joomla! Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39521	Backported Security Patch Detection (WWW)
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	49704	External URLs
Info	54615	Device Type
Info	66334	Patch Report

Info	66717	mDNS Detection (Local Network)

192.168.2.105

Summary

Critical	High	Medium	Low	Info	Total
3	5	15	8	60	91

Details

Severity	Plugin Id	Name
Critical (10.0)	25216	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow
Critical (10.0)	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Critical (10.0)	33850	Unsupported Unix Operating System
High (9.4)	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
High (7.8)	55976	Apache HTTP Server Byte Range DoS
High (7.5)	17210	TWiki ImageGalleryPlugin Shell Command Injection
High (7.5)	19704	TWiki rev Parameter Arbitrary Command Execution
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	11229	Web Server info.php / phpinfo.php Detection
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 (v2) Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
Medium (4.3)	51893	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Ciphersuite Disabled Cipher Issue
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
Medium (4.0)	52611	SMTP Service STARTTLS Plaintext Command Injection
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported

Low (2.6)	34324	FTP Supports Clear Text Authentication
Low (2.6)	42263	Unencrypted Telnet Server
Low (2.6)	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10028	DNS Server BIND version Directive Remote Version Disclosure
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10662	Web mirroring
Info	10719	MySQL Server Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11032	Web Server Directory Enumeration
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification

Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	19941	TWiki Detection
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	25240	Samba Server Detection
Info	26024	PostgreSQL Server Detection
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	35716	Ethernet Card Manufacturer Detection
Info	39519	Backported Security Patch Detection (FTP)
Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	40984	Browsable Web Directories
Info	42057	Web Server Allows Password Auto-Completion
Info	42088	SMTP Service STARTTLS Command Support
Info	43111	HTTP Methods Allowed (per directory)
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	49704	External URLs
Info	49705	Web Server Harvested Email Addresses
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	58768	SSL Resume With Different Cipher Issue
Info	60119	Microsoft Windows SMB Share Permissions Enumeration

Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported

D.3. Análisis desde la zona privada de la red

El informe presentado a continuación corresponde con el informe automático generado por Nessus™ tras la realización del análisis desde la zona privada de la red.

Con este análisis se pueden observar las diferentes vulnerabilidades que podría explotar cualquier usuario invitado que se conectara a la red pública, de esta manera, son importantes. Sin embargo, puesto que existe cierto control de quien puede conectarse a la zona de la red pública, no tienen tanta importancia como las vulnerabilidades que aparecen en el informe realizado desde el exterior de la red.

El informe consiste en un resumen ejecutivo de las diferentes vulnerabilidades existentes junto con una explicación en detalle de las mismas. En el resumen se presentan las diferentes vulnerabilidades existentes en cada equipo, ordenadas según un código de color en función de la severidad de la misma. De esta manera, de cada vulnerabilidad se presenta: su severidad, el código de la vulnerabilidad y una breve descripción. Por otro lado, en la explicación en detalle de las vulnerabilidades se pueden encontrar mas detalles como: una explicación detallada del alcance de la vulnerabilidad, los módulos de algunos programas con los cuales explotarlas o como corregirlas entre otros.

192.168.1.1

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	2	3

Details

Severity	Plugin Id	Name
Low (3.3)	10663	DHCP Server Detection
Info	19506	Nessus Scan Information
Info	35716	Ethernet Card Manufacturer Detection

192.168.1.5

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	20	21

Details

Severity	Plugin Id	Name
Medium (5.0)	57608	SMB Signing Disabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	11011	Microsoft Windows SMB Service Detection
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	25220	TCP/IP Timestamps Supported
Info	25240	Samba Server Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	60119	Microsoft Windows SMB Share Permissions Enumeration

192.168.1.6

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	19	19

Details

Severity	Plugin Id	Name
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39519	Backported Security Patch Detection (FTP)
Info	42149	FTP Service AUTH TLS Command Support
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	66717	mDNS Detection (Local Network)

192.168.1.7

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	12	12

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	25220	TCP/IP Timestamps Supported
Info	26024	PostgreSQL Server Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	66717	mDNS Detection (Local Network)

192.168.1.25

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	3	4

Details

Severity	Plugin Id	Name
Low (3.2)	50686	IP Forwarding Enabled
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	35716	Ethernet Card Manufacturer Detection

192.168.1.109

Summary

Critical	High	Medium	Low	Info	Total
1	0	0	0	12	13

Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type

192.168.1.113

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	7	7

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	66717	mDNS Detection (Local Network)

192.168.2.5

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	3	19	27

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	10079	Anonymous FTP Enabled
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	34324	FTP Supports Clear Text Authentication
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10092	FTP Server Detection
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	39519	Backported Security Patch Detection (FTP)
Info	42149	FTP Service AUTH TLS Command Support
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported

Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

192.168.2.6

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	2	23	30

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12218	mDNS Detection (Remote Network)
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10185	POP Server Detection
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11414	IMAP Service Banner Retrieval
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	42085	IMAP Service STARTTLS Command Support
Info	42087	POP3 Service STLS Command Support
Info	42088	SMTP Service STARTTLS Command Support
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type

Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

192.168.2.7

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	21	25

Details

Severity	Plugin Id	Name
Medium (5.0)	12218	mDNS Detection (Remote Network)
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (4.3)	69280	Joomla! libraries/idna_convert/example.php lang Parameter XSS
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10662	Web mirroring
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21142	Joomla! Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39521	Backported Security Patch Detection (WWW)
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	49704	External URLs
Info	54615	Device Type
Info	66334	Patch Report

192.168.2.105

Summary

Critical	High	Medium	Low	Info	Total
3	3	15	7	55	83

Details

Severity	Plugin Id	Name
Critical (10.0)	25216	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow
Critical (10.0)	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Critical (10.0)	33850	Unsupported Unix Operating System
High (9.4)	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
High (7.8)	55976	Apache HTTP Server Byte Range DoS
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	11229	Web Server info.php / phpinfo.php Detection
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 (v2) Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
Medium (4.3)	51893	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Ciphersuite Disabled Cipher Issue
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
Medium (4.0)	52611	SMTP Service STARTTLS Plaintext Command Injection
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported
Low (2.6)	42263	Unencrypted Telnet Server
Low (2.6)	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10028	DNS Server BIND version Directive Remote Version Disclosure
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10662	Web mirroring
Info	10719	MySQL Server Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11032	Web Server Directory Enumeration
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported

Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	25240	Samba Server Detection
Info	26024	PostgreSQL Server Detection
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	40984	Browsable Web Directories
Info	42057	Web Server Allows Password Auto-Completion
Info	42088	SMTP Service STARTTLS Command Support
Info	43111	HTTP Methods Allowed (per directory)
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	49704	External URLs
Info	49705	Web Server Harvested Email Addresses
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	58768	SSL Resume With Different Cipher Issue
Info	60119	Microsoft Windows SMB Share Permissions Enumeration
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported

Vulnerabilities By Host

192.168.1.1

Scan Information

Start time: Mon Jan 6 08:02:18 2014

End time: Mon Jan 6 08:10:35 2014

Host Information

IP: 192.168.1.1

MAC Address: 00:13:8f:3f:67:cf

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	2	3

Results Details

0/tcp

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Ports

tcp/0

```
The following card manufacturers were identified :

00:13:8f:3f:67:cf : Asiarock Incorporation
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel

- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 493 sec
```

67/udp

10663 - DHCP Server Detection

Synopsis

The remote DHCP server may expose information about the associated network.

Description

This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.
Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.
It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.

Solution

Apply filtering to keep this information off the network and remove any options that are not in use.

Risk Factor

Low

CVSS Base Score

3.3 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2001/05/05, Modification date: 2013/01/25

Ports

udp/67

```
Nessus gathered the following information from the remote DHCP server :
```

```
Master DHCP server of this network : 192.168.1.1
IP address the DHCP server would attribute us : 192.168.1.121
DHCP server(s) identifier : 192.168.1.1
Netmask : 255.255.255.0
Router : 192.168.1.1
Domain name server(s) : 80.58.0.33 , 80.58.32.97
Domain name : dominio.com
Broadcast address : 192.168.1.255
```

192.168.1.5

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:56:08 2014

Host Information

Netbios Name:	SAMBA
IP:	192.168.1.5
MAC Address:	00:50:56:22:d0:a0
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	21	22

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is -14076 seconds.
```

0/tcp

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

20094 - VMware Virtual Machine Detection

Synopsis

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2011/03/27

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:22:d0:a0 : VMware, Inc.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.2
Linux Kernel 3.3
Confidence Level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.2
Linux Kernel 3.3
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports

tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:linux:linux_kernel:3.2
  cpe:/o:linux:linux_kernel:3.3

Following application CPE matched on the remote system :

  cpe:/a:samba:samba:3.6.3 -> Samba 3.6.3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 3230 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.1.5 :
192.168.1.121
192.168.1.5
```

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2013/01/16

Ports

udp/137

```
The following 7 NetBIOS names have been gathered :

 SAMBA            = Computer name
 SAMBA            = Messenger Service
 SAMBA            = File Server Service
 __MSBROWSE__     = Master Browser
 WORKGROUP        = Master Browser
 WORKGROUP        = Browser Service Elections
 WORKGROUP        = Workgroup / Domain name

This SMB server seems to be a Samba server - its MAC address is NULL.
```

139/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2012/01/31

Ports

tcp/139

```
An SMB server is running on this port.
```

445/tcp

57608 - SMB Signing Disabled

Synopsis

Signing is disabled on the remote SMB server.

Description

Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

See Also

http://support.microsoft.com/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information:

Publication date: 2012/01/19, Modification date: 2013/10/24

Ports

tcp/445

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2012/01/31

Ports

tcp/445

```
A CIFS server is running on this port.
```

25240 - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

http://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2013/01/07

Ports

tcp/445

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It is possible to obtain information about the remote operating system.

Description

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2013/06/25

Ports

tcp/445

```
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.6.3
The remote SMB Domain Name is : SAMBA
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It is possible to log into the remote host.

Description

The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :
- NULL session
- Guest account
- Given Credentials

See Also

http://support.microsoft.com/kb/143474

http://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2000/05/09, Modification date: 2013/04/23

Ports

tcp/445

```
- NULL sessions are enabled on the remote host
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).
The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information:

Publication date: 2002/02/13, Modification date: 2012/08/10

Ports

tcp/445

```
The remote host SID value is :

1-5-21-264684740-4009281998-452950973

The value of 'RestrictAnonymous' setting is : unknown
```

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

It is possible to enumerate local users.

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/02/13, Modification date: 2012/08/10

Ports

tcp/445

```
  - nobody (id 501, Guest account)
  - sambamalo (id 1000)
  - sambamedio (id 1001)
  - sambabueno (id 1002)

Note that, in addition to the Administrator and Guest accounts, Nessus
has enumerated only those local users with IDs between 1000 and 1200.
```

```
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2012/11/29

Ports

tcp/445

```
Here are the SMB shares available on the remote host when logged as a NULL session:

  - IPC$
  - sambabueno
  - sambamedio
  - sambamalo
  - public
```

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It is possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

http://technet.microsoft.com/en-us/library/bb456988.aspx

http://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/07/25, Modification date: 2012/07/25

Ports

tcp/445

```
Share path : \\SAMBA\IPC$
Local path : C:\tmp
Comment : IPC Service (ubuntu server (Samba, Ubuntu))
Allow ACE for Everyone : Read, Write

Share path : \\SAMBA\sambabueno
Local path : C:\home\sambabueno
Comment : Carpeta de Sambabueno
Allow ACE for Everyone : Read, Write

Share path : \\SAMBA\sambamedio
Local path : C:\home\sambamedio
Comment : Carpeta de Sambamedio
```

```
Allow ACE for Everyone : Read, Write

Share path : \\SAMBA\sambamalo
Local path : C:\home\sambamalo
Comment : Carpeta de Sambamalo
Allow ACE for Everyone : Read, Write

Share path : \\SAMBA\public
Local path : C:\home\public
Comment : Carpeta publica
Allow ACE for Everyone : Read, Write
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2011/03/04

Ports

tcp/445

```
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF OSVDB:300

Plugin Information:

Publication date: 2000/05/09, Modification date: 2011/09/14

Ports

tcp/445

```
Here is the browse list of the remote host :

ASUSN53SV ( os : 0.0 )
```

```
SAMBA ( os : 0.0 )
```

192.168.1.6

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:59:34 2014

Host Information

IP:	192.168.1.6
MAC Address:	00:50:56:33:41:9d
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	21	21

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is -14082 seconds.
```

0/tcp

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

20094 - VMware Virtual Machine Detection

Synopsis

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2011/03/27

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:33:41:9d : VMware, Inc.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.2
Linux Kernel 3.3
Confidence Level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.2
Linux Kernel 3.3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports
tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:linux:linux_kernel:3.2
  cpe:/o:linux:linux_kernel:3.3
```

19506 - Nessus Scan Information
Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports
tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 3436 sec
```

0/udp

10287 - Traceroute Information
Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.1.6 :
192.168.1.121
192.168.1.6
```

21/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/21

```
Port 21/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/21

```
An FTP server is running on this port.
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on this port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2013/03/08

Ports

tcp/21

```
The remote FTP banner is :

220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.1.6]
550 SSL/TLS required on the control channel
500 Invalid command: try being more creative
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a plaintext to an encrypted communications channel.

See Also

http://en.wikipedia.org/wiki/STARTTLS

http://tools.ietf.org/html/rfc4217

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/15, Modification date: 2011/03/11

Ports

tcp/21

```
Here is the FTP server's SSL certificate that Nessus was able to
collect after sending a 'AUTH TLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Issuer Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Serial Number: 00 E7 EC 34 2E 20 2E EF 1B
```

```
Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 19 11:07:15 2013 GMT
Not Valid After: Oct 19 11:07:15 2014 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 C2 02 96 4A 98 8A EC 5E E5 62 9C 7D 47 34 73 6D DF 7B 46
            0C 6E 3C 2C 29 B7 74 62 D4 BC 83 45 EF DF 2F 26 02 B2 65 3F
            DF C9 A1 80 B0 7E FD A6 26 13 16 E4 1D B5 B2 F5 C8 E5 35 9E
            46 D5 68 53 94 50 5A 59 12 07 A3 17 8F 7A AE 9C F0 BE 29 26
            CB 04 8B 87 D7 5A E9 06 76 A8 5B 07 60 48 E5 7E CF CE F2 46
            C6 8C 69 4B BD FF B2 B4 96 89 B1 66 63 47 97 A9 9C 4B B8 1F
            68 98 DD DD 35 EE CC DA 6D
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 35 DD 48 73 2A 3D F2 B8 AB 59 A5 9C D7 34 0E 93 82 DC F8
           01 7C 9D 10 2C 99 47 2A 3E 62 1B 63 C1 02 6A 23 17 84 41 74
           4A 87 D2 0D 83 86 DA C9 66 1E BF E1 12 73 16 A6 04 A6 56 A2
           DC 50 67 FD 61 1F B8 7D 24 55 2B 1B 85 1B E2 E2 94 16 C2 9C
           E3 EB F1 30 9D CE C4 06 8D F6 6B 73 54 60 21 13 EC 75 63 7C
           84 91 00 38 58 0F 7F 54 70 2C D2 4F 7F 40 15 77 44 E3 18 C8
           09 8B 2F 71 1D 1E 4E 11 8A

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 57 8D AF 7E 71 BB 51 69 80 FA 81 7A 18 04 70 4B AE 76 59 C7


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 57 8D AF 7E 71 BB 51 69 80 FA 81 7A 18 04 70 4B AE 76 59 C7


Extension: Basic Co [...]
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports

tcp/21

```
This port supports TLSv1.0/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports

tcp/21

```
Subject Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Issuer Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Serial Number: 00 E7 EC 34 2E 20 2E EF 1B

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 19 11:07:15 2013 GMT
Not Valid After: Oct 19 11:07:15 2014 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 C2 02 96 4A 98 8A EC 5E E5 62 9C 7D 47 34 73 6D DF 7B 46
            0C 6E 3C 2C 29 B7 74 62 D4 BC 83 45 EF DF 2F 26 02 B2 65 3F
            DF C9 A1 80 B0 7E FD A6 26 13 16 E4 1D B5 B2 F5 C8 E5 35 9E
            46 D5 68 53 94 50 5A 59 12 07 A3 17 8F 7A AE 9C F0 BE 29 26
            CB 04 8B 87 D7 5A E9 06 76 A8 5B 07 60 48 E5 7E CF CE F2 46
            C6 8C 69 4B BD FF B2 B4 96 89 B1 66 63 47 97 A9 9C 4B B8 1F
            68 98 DD DD 35 EE CC DA 6D
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 35 DD 48 73 2A 3D F2 B8 AB 59 A5 9C D7 34 0E 93 82 DC F8
           01 7C 9D 10 2C 99 47 2A 3E 62 1B 63 C1 02 6A 23 17 84 41 74
           4A 87 D2 0D 83 86 DA C9 66 1E BF E1 12 73 16 A6 04 A6 56 A2
           DC 50 67 FD 61 1F B8 7D 24 55 2B 1B 85 1B E2 E2 94 16 C2 9C
           E3 EB F1 30 9D CE C4 06 8D F6 6B 73 54 60 21 13 EC 75 63 7C
           84 91 00 38 58 0F 7F 54 70 2C D2 4F 7F 40 15 77 44 E3 18 C8
           09 8B 2F 71 1D 1E 4E 11 8A

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 57 8D AF 7E 71 BB 51 69 80 FA 81 7A 18 04 70 4B AE 76 59 C7


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 57 8D AF 7E 71 BB 51 69 80 FA 81 7A 18 04 70 4B AE 76 59 C7


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE
```

39519 - Backported Security Patch Detection (FTP)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote FTP server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/04/03

Ports

tcp/21

```
Give Nessus credentials to perform local checks.
```

631/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/631

```
Port 631/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports
tcp/631

```
A web server is running on this port.
```

10107 - HTTP Server Type and Version
Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2013/12/03

Ports
tcp/631

```
The remote web server type is :

CUPS/1.5
```

43111 - HTTP Methods Allowed (per directory)
Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports
tcp/631

```
Based on the response to an OPTIONS request :

  - HTTP methods  HEAD  OPTIONS  POST  PUT GET are allowed on :

    /
```

5353/udp
66717 - mDNS Detection (Local Network)
Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/31, Modification date: 2013/05/31

Ports

udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : ubuntu.local.

  - Advertised services :
    o Service name      : ubuntu [00:50:56:33:41:9d]._workstation._tcp.local.
      Port number       : 9
    o Service name      : HP Deskjet D2400 series @ ubuntu._ipp._tcp.local.
      Port number       : 631
    o Service name      : Virtual PDF Printer @ ubuntu._ipp._tcp.local.
      Port number       : 631

  - CPU type            : X86_64
  - OS                  : LINUX
```

192.168.1.7

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:53:24 2014

Host Information

IP:	192.168.1.7
MAC Address:	00:50:56:37:79:4f
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	12	12

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 6633 seconds.
```

0/tcp

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

20094 - VMware Virtual Machine Detection

Synopsis

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2011/03/27

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:37:79:4f : VMware, Inc.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.2
Linux Kernel 3.3
Confidence Level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.2
Linux Kernel 3.3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports
tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:linux:linux_kernel:3.2
  cpe:/o:linux:linux_kernel:3.3
```

19506 - Nessus Scan Information
Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports
tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 3066 sec
```

0/udp

10287 - Traceroute Information
Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.1.7 :
192.168.1.121
192.168.1.7
```

5353/udp

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/31, Modification date: 2013/05/31

Ports

udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : ubuntu-2.local.

  - Advertised services :
    o Service name      : ubuntu-2 [00:50:56:37:79:4f]._workstation._tcp.local.
      Port number       : 9
    o Service name      : ubuntu-2._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : X86_64
  - OS                  : LINUX
```

5432/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/5432

```
Port 5432/tcp was found to be open
```

26024 - PostgreSQL Server Detection

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

http://www.postgresql.org/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Publication date: 2007/09/14, Modification date: 2013/02/14

Ports

tcp/5432

192.168.1.25

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:10:43 2014

Host Information

IP:	192.168.1.25
MAC Address:	00:50:56:29:5d:12

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	3	4

Results Details

0/tcp

50686 - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker may use this flaw to route packets through this host and potentially bypass some firewalls / routers / NAC filtering.
Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :
echo 0 > /proc/sys/net/ipv4/ip_forward
On Windows, set the key 'IPEnableRouter' to 0 under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameter
On Mac OS X, you can disable IP forwarding by executing the command :
sysctl -w net.inet.ip.forwarding=0
For other systems, check with your vendor.

Risk Factor

Low

CVSS Base Score

3.2 (CVSS2#AV:A/AC:H/Au:N/C:P/I:P/A:N)

References

CVE	CVE-1999-0511
XREF	OSVDB:8114

Plugin Information:

Publication date: 2010/11/23, Modification date: 2013/12/10

Ports

tcp/0

20094 - VMware Virtual Machine Detection

Synopsis

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2011/03/27

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:29:5d:12 : VMware, Inc.
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 501 sec
```

192.168.1.109

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:10:45 2014

Host Information

Netbios Name:	WIN-IS8I702L4F5
IP:	192.168.1.109
MAC Address:	00:50:56:32:13:82
OS:	Microsoft Windows Server 2003, Microsoft Windows Vista, Microsoft Windows Server 2008, Microsoft Windows 7, Microsoft Windows Server 2008 R2

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	0	0	12	13

Results Details

0/tcp

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

20094 - VMware Virtual Machine Detection

Synopsis

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2011/03/27

Ports
tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Ports
tcp/0

```
The following card manufacturers were identified :

00:50:56:32:13:82 : VMware, Inc.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports
tcp/0

```
Remote operating system : Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Windows Server 2008
Microsoft Windows 7
Microsoft Windows Server 2008 R2
Confidence Level : 70
Method : HTTP


The remote host is running one of these operating systems :
Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Windows Server 2008
Microsoft Windows 7
Microsoft Windows Server 2008 R2
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 70
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports

tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:microsoft:windows_2003_server
  cpe:/o:microsoft:windows_vista
  cpe:/o:microsoft:windows_server_2008
  cpe:/o:microsoft:windows_7
  cpe:/o:microsoft:windows_server_2008:r2 -> Microsoft Windows Server 2008 R2
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible

- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 503 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.1.109 :
192.168.1.121
192.168.1.109
```

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2013/01/16

Ports

udp/137

```
The following 3 NetBIOS names have been gathered :

 WIN-IS8I702L4F5  = File Server Service
 WIN-IS8I702L4F5  = Computer name
 WORKGROUP        = Workgroup / Domain name

The remote host has the following MAC address on its adapter :

   00:50:56:32:13:82
```

5355/udp

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.
Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-030

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

BID	47242
CVE	CVE-2011-0657
XREF	OSVDB:71780
XREF	IAVA:2011-A-0039

XREF MSFT:MS11-030

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2011/04/21, Modification date: 2013/11/03

Ports

udp/5355

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?85beb421

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2011/04/21, Modification date: 2012/03/05

Ports

udp/5355

```
According to LLMNR, the name of the remote host is 'WIN-IS8I702L4F5'.
```

5357/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/5357

```
Port 5357/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/5357

```
A web server is running on this port.
```

192.168.1.113

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:10:44 2014

Host Information

IP:	192.168.1.113
MAC Address:	00:50:56:3e:44:fd
OS:	Linux Kernel

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	7	7

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is -14058 seconds.
```

0/tcp

20094 - VMware Virtual Machine Detection

Synopsis

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2011/03/27

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:3e:44:fd : VMware, Inc.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel
Confidence Level : 30
Method : mDNS


The remote host is running Linux Kernel
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 506 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports
udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.1.113 :
192.168.1.121
192.168.1.113
```

5353/udp
66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/31, Modification date: 2013/05/31

Ports
udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : ubuntu-3.local.

  - Advertised services :
    o Service name      : ubuntu-3 [00:50:56:3e:44:fd]._workstation._tcp.local.
      Port number       : 9
    o Service name      : ubuntu-3._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : X86_64
  - OS                  : LINUX
```

192.168.2.5

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:10:22 2014

Host Information

IP:	192.168.2.5
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	3	19	27

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is -14049 seconds.
```

0/tcp

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.2
Linux Kernel 3.3
Confidence Level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.2
Linux Kernel 3.3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports

tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:linux:linux_kernel:3.2
  cpe:/o:linux:linux_kernel:3.3
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
```

```
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 484 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.2.5 :
192.168.1.121
?
192.168.2.5
```

21/tcp

10079 - Anonymous FTP Enabled

Synopsis

Anonymous logins are allowed on the remote FTP server.

Description

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Solution

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0497
XREF	OSVDB:69

Plugin Information:

Publication date: 1999/06/22, Modification date: 2013/01/25

Ports

tcp/21

```
The contents of the remote FTP root are :
-rw-r--r--   1 ftp      ftp             0 Jan 16 17:13 ftpraro
```

```
-rw-r--r--   1 ftp      ftp           170 Dec 16  2011 welcome.msg
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Ports

tcp/21

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=SP/ST=Madrid/L=Madrid/O=PFC/CN=dominio.com/E=postmaster@dominio.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer.
Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2012/10/25

Ports

tcp/21

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : C=SP/ST=Madrid/L=Madrid/O=PFC/CN=dominio.com/E=postmaster@dominio.com
|-Issuer  : C=SP/ST=Madrid/L=Madrid/O=PFC/CN=dominio.com/E=postmaster@dominio.com
```

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:327
XREF	CWE:326
XREF	CWE:753
XREF	CWE:803
XREF	CWE:720

Plugin Information:

Publication date: 2007/10/08, Modification date: 2013/08/30

Ports

tcp/21

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)      Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)      Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2009/11/23, Modification date: 2012/04/02

Ports

tcp/21

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

34324 - FTP Supports Clear Text Authentication

Synopsis

Authentication credentials might be intercepted.

Description

The remote FTP server allows the user's name and password to be transmitted in clear text, which could be intercepted by a network sniffer or a man-in-the-middle attack.

Solution

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523

Plugin Information:

Publication date: 2008/10/01, Modification date: 2013/01/25

Ports
tcp/21

```
Although this FTP server supports 'AUTH TLS', it is not mandatory
and USER and PASS may be sent without switching to TLS.
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.
Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.
Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates it signed.

Risk Factor

Low

Plugin Information:

Publication date: 2013/09/03, Modification date: 2013/09/30

Ports
tcp/21

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak.

|-Subject        : C=SP/ST=Madrid/L=Madrid/O=PFC/CN=dominio.com/E=postmaster@dominio.com
|-RSA Key Length : 1024 bits
```

65821 - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/12/11

Ports

tcp/21

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      RC4-MD5                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=SHA1

    TLSv1
      RC4-MD5                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/21

```
Port 21/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/21

```
An FTP server is running on this port.
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on this port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2013/03/08

Ports

tcp/21

```
The remote FTP banner is :

220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.2.5]
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a plaintext to an encrypted communications channel.

See Also

http://en.wikipedia.org/wiki/STARTTLS

http://tools.ietf.org/html/rfc4217

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/15, Modification date: 2011/03/11

Ports

tcp/21

```
Here is the FTP server's SSL certificate that Nessus was able to
```

```
collect after sending a 'AUTH TLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Issuer Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Serial Number: 00 EE 0C 56 14 33 B0 C6 F5

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 19 15:55:21 2013 GMT
Not Valid After: Oct 19 15:55:21 2014 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D1 1F 63 02 20 50 1B 83 AD BA DD 2D 21 29 E6 B2 8A 69 12
            E4 80 93 A8 E1 49 67 B7 7E E3 9E 33 A6 B6 E2 AD F9 F1 3A 14
            CB 65 43 4A C7 B0 19 D1 13 4A 91 CC CE 06 66 0F 19 0C 39 01
            1A 25 BC 2A 07 88 39 61 8C A4 0E 13 14 3A 4D 05 4F 3D FC 59
            DB 80 A4 8D C8 A4 54 FC 6F 3D 3A 75 D8 05 14 DF 57 4B 99 98
            39 28 4D FB D1 85 84 F7 96 BA 45 CD 65 B9 11 00 8A 29 95 73
            CE D9 03 FF 50 84 CA D3 E1
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 80 86 82 01 21 00 86 A6 81 F4 7C C0 73 4F 62 79 26 48 A1
           13 64 46 64 04 CF 4F A1 04 89 EE 40 22 B1 C7 A8 A4 AF 37 9F
           81 3F 6F 83 64 CC F1 EA D6 62 0C 67 F5 35 3C FA DB 5A D5 18
           35 1E FD D2 57 37 72 18 2C 40 46 C7 6F BF 54 04 32 5B EC 37
           FB CC 2E 92 17 AD 52 3D 02 E8 B2 7D D2 09 57 67 1D A4 86 E6
           2A C3 14 06 02 E7 F5 AF 0E 59 97 61 E2 0A 5F 45 50 8B D6 6D
           A5 EC 18 25 7C 41 F0 39 58

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4A E8 B4 67 E0 78 8D 27 30 67 5D 4F 79 CF A6 06 93 11 B7 87


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4A E8 B4 67 E0 78 8D 27 30 67 5D 4F 79 CF A6 06 93 11 B7 87


Extension: Basic Co [...]
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports

tcp/21

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports

tcp/21

```
Subject Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Issuer Name:

Country: SP
State/Province: Madrid
Locality: Madrid
Organization: PFC
Common Name: dominio.com
Email Address: postmaster@dominio.com

Serial Number: 00 EE 0C 56 14 33 B0 C6 F5

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 19 15:55:21 2013 GMT
Not Valid After: Oct 19 15:55:21 2014 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D1 1F 63 02 20 50 1B 83 AD BA DD 2D 21 29 E6 B2 8A 69 12
            E4 80 93 A8 E1 49 67 B7 7E E3 9E 33 A6 B6 E2 AD F9 F1 3A 14
            CB 65 43 4A C7 B0 19 D1 13 4A 91 CC CE 06 66 0F 19 0C 39 01
            1A 25 BC 2A 07 88 39 61 8C A4 0E 13 14 3A 4D 05 4F 3D FC 59
            DB 80 A4 8D C8 A4 54 FC 6F 3D 3A 75 D8 05 14 DF 57 4B 99 98
            39 28 4D FB D1 85 84 F7 96 BA 45 CD 65 B9 11 00 8A 29 95 73
            CE D9 03 FF 50 84 CA D3 E1
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 80 86 82 01 21 00 86 A6 81 F4 7C C0 73 4F 62 79 26 48 A1
```

```
            13 64 46 64 04 CF 4F A1 04 89 EE 40 22 B1 C7 A8 A4 AF 37 9F
            81 3F 6F 83 64 CC F1 EA D6 62 0C 67 F5 35 3C FA DB 5A D5 18
            35 1E FD D2 57 37 72 18 2C 40 46 C7 6F BF 54 04 32 5B EC 37
            FB CC 2E 92 17 AD 52 3D 02 E8 B2 7D D2 09 57 67 1D A4 86 E6
            2A C3 14 06 02 E7 F5 AF 0E 59 97 61 E2 0A 5F 45 50 8B D6 6D
            A5 EC 18 25 7C 41 F0 39 58

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4A E8 B4 67 E0 78 8D 27 30 67 5D 4F 79 CF A6 06 93 11 B7 87


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4A E8 B4 67 E0 78 8D 27 30 67 5D 4F 79 CF A6 06 93 11 B7 87


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports

tcp/21

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/21

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2013/10/18

Ports

tcp/21

```
Here is the list of SSL ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES(168)            Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
```

```
    DES-CBC3-SHA                Kx=RSA      Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1
    AES128-SHA                  Kx=RSA      Au=RSA      Enc=AES-CBC( [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/21

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      CAMELLIA128-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      CAMELLIA256-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      SEED-SHA                     Kx=RSA         Au=RSA      Enc=SEED-CBC(128)   [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/21

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

39519 - Backported Security Patch Detection (FTP)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote FTP server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/04/03

Ports

tcp/21

```
Give Nessus credentials to perform local checks.
```

192.168.2.6

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:09:31 2014

Host Information

IP:	192.168.2.6
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	13	6	63	82

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is -4924 seconds.
```

0/tcp

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.2
Linux Kernel 3.3
Confidence Level : 59
Method : SinFP

Not all fingerprints could give a match.  If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org.  Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

mDNS:LINUX
SinFP:
   P1:B10113:F0x12:W14600:O0204ffff:M1460:
   P2:B10113:F0x12:W14480:O0204ffff0402080affffffff4445414401030306:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:5202_7_p=110R
SMTP:!:220 ubuntu ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntui/O:Dovecot mail serveri/OU:ubuntus/CN:ubuntus/O:Dovecot mail servers/
OU:ubuntu
4e7c4036c58db7aead46e82910d26b7e77f13e4e
i/CN:ubuntui/O:Dovecot mail serveri/OU:ubuntus/CN:ubuntus/O:Dovecot mail servers/OU:ubuntu
4e7c4036c58db7aead46e82910d26b7e77f13e4e



The remote host is running one of these operating systems :
Linux Kernel 3.2
Linux Kernel 3.3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports

tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:linux:linux_kernel:3.2
  cpe:/o:linux:linux_kernel:3.3
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 433 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.2.6 :
192.168.1.121
?
192.168.2.6
```

25/tcp

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Ports

tcp/25

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=ubuntu
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2012/10/25

Ports

tcp/25

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : CN=ubuntu
|-Issuer  : CN=ubuntu
```

42873 - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2009/11/23, Modification date: 2012/04/02

Ports

tcp/25

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      ADH-DES-CBC-SHA              Kx=DH          Au=None      Enc=DES-CBC(56)          Mac=SHA1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA       Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA       Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA       Enc=DES-CBC(56)          Mac=SHA1
      ADH-DES-CBC-SHA              Kx=DH          Au=None      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA       Enc=DES-CBC(56)          Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:327
XREF	CWE:326
XREF	CWE:753

XREF CWE:803

XREF CWE:720

Plugin Information:

Publication date: 2007/10/08, Modification date: 2013/08/30

Ports

tcp/25

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2(40)              Mac=MD5
export
      EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
      EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
      EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/12/11

Ports

tcp/25

```
Here is the list of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-ADH-RC4-MD5             Kx=DH(512)     Au=None     Enc=RC4(40)             Mac=MD5
 export
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
 export

    TLSv1
      EXP-ADH-RC4-MD5             Kx=DH(512)     Au=None     Enc=RC4(40)             Mac=MD5
 export
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
 export

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      ADH-RC4-MD5                 Kx=DH          Au=None     Enc=RC4(128)            Mac=MD5
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

    TLSv1
      ADH-RC4-MD5                 Kx=DH          Au=None     Enc=RC4(128)            Mac=MD5
      ECDHE-RSA-RC4-SHA           Kx=ECDH        Au=RSA      Enc=RC4(128)            Mac=SHA1
      AECDH-RC4-SHA               Kx=ECDH        Au=None     Enc=RC4(128)            Mac=SHA1
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	28482
CVE	CVE-2007-1858
XREF	OSVDB:34882

Plugin Information:

Publication date: 2008/03/28, Modification date: 2013/07/18

Ports

tcp/25

```
Here is the list of SSL anonymous ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export

    TLSv1
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      ADH-DES-CBC3-SHA             Kx=DH          Au=None     Enc=3DES-CBC(168)        Mac=SHA1
      ADH-RC4-MD5                  Kx=DH          Au=None     Enc=RC4(128)             Mac=MD5

    TLSv1
      ADH-DES-CBC3-SHA             Kx=DH          Au=None     Enc=3DES-CBC(168)        Mac=SHA1
      ADH-AES128-SHA               Kx=DH          Au=None     Enc=AES-CBC(128)         Mac=SHA1
      ADH-AES256-SHA               Kx=DH          Au=None     Enc=AES-CBC(256)         Mac=SHA1
      ADH-CAMELLIA128-SHA          Kx=DH          Au=None     Enc=Camellia-CBC(128)    Mac=SHA1
      ADH-CAMELLIA256-SHA          Kx=DH          Au=None     Enc=Camellia-CBC(256)    Mac=SHA1
      ADH-RC4-MD5                  Kx=DH          Au=None     Enc=RC4(128)             Mac=MD5
```

```
ADH-SEED-SHA                  Kx=DH          Au=None     Enc=SEED-CBC(128)       Mac=SHA1
AECDH-DES-CBC3-SHA            Kx=ECDH        Au=None     Enc=3DES-CBC(168)       Mac=SHA1
AECDH-AES128-SHA              Kx=ECDH        Au=None     Enc=AES-CBC(128)        Mac=SHA1
AECDH-AES256-SHA              Kx=ECDH [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/25

```
Port 25/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/25

```
An SMTP server is running on this port.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.
Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/25

```
Remote SMTP server banner :

220 ubuntu ESMTP Postfix (Ubuntu)
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a plaintext to an encrypted communications channel.

See Also

http://en.wikipedia.org/wiki/STARTTLS

http://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/09, Modification date: 2011/12/14

Ports

tcp/25

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Common Name: ubuntu

Issuer Name:

Common Name: ubuntu

Serial Number: 00 B2 C9 DA B6 95 3F 7B D0

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 14 18:47:59 2013 GMT
Not Valid After: Jul 12 18:47:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 26 5A 7C EE 50 AA 6E A4 51 E8 BD 9A 44 84 2C F3 A8 B3
            1E 9F 44 AF 63 7D CE E4 0B 11 CE B0 F6 4E 09 58 6C BB BB 6E
            F1 E9 EB F1 DD 1E B2 23 56 E0 72 30 C9 84 3B 98 AF 69 9B 97
            1F 1A ED 03 DC 04 AC EB BB FB 98 17 32 C4 5D 15 F4 C0 6A 1D
            A7 C7 9A 6B 62 9E 43 CA 88 66 B8 74 E7 9C AB 45 EC 54 BA E5
            66 0C 42 90 3E B5 84 74 64 77 59 29 00 55 3D 75 AE B1 A0 1B
            AC BC B9 36 E5 BD FD E9 A7 74 47 EA DA 5E 0A 23 84 57 B8 64
            01 50 17 42 19 48 E1 23 90 D0 26 17 EC 2C 32 95 37 61 CD FA
            57 86 72 21 7A F0 68 BE 48 70 53 B3 32 B2 A2 B2 8D FF 20 D7
            2F D8 9E 3F A7 70 F6 10 01 51 5D 6A E8 C2 62 C2 71 93 8B 7B
            F4 7E 08 C4 8A 4B B3 EB 39 5B 7F 55 1E 6A 3B 0C B8 6C 98 F6
            EB B3 05 A3 FC EA E3 F1 A2 40 6D 1A E9 6A 21 3C 72 19 CC 9F
            FB B4 CD 05 D3 01 E1 86 29 C3 89 3E 91 B5 2A 4B DF
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
```

```
Signature: 00 B2 8A D7 13 BB 54 B3 53 0A 0F 66 7C 59 FC 3E 59 D6 10 9A
           61 2B 71 ED D6 60 F4 82 1F 16 38 F4 A9 D7 9F 35 D9 F3 F7 59
           F2 00 42 32 F0 0E 09 21 D2 7C D2 7D 87 A1 86 69 E9 41 1D D6
           7D 99 A1 59 3A DF 05 C0 89 70 F1 EC 47 FF 6A 48 1E DB EC 55
           27 27 58 2B 66 D5 29 34 77 89 08 53 EF 7F 0B 38 AE 5A CA D0
           76 01 D4 EF A4 3F 6B 0B 1F 71 E9 2E B3 1D 20 6D E3 69 F9 8D
           6E F9 1F A7 C8 E2 90 08 66 13 C8 8C 72 AC CA E5 24 0E 0F 44
           BD E0 CB 2D C5 0B 9F A [...]
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports

tcp/25

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports

tcp/25

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports

tcp/25

```
Subject Name:

Common Name: ubuntu

Issuer Name:

Common Name: ubuntu

Serial Number: 00 B2 C9 DA B6 95 3F 7B D0

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 14 18:47:59 2013 GMT
Not Valid After: Jul 12 18:47:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 26 5A 7C EE 50 AA 6E A4 51 E8 BD 9A 44 84 2C F3 A8 B3
            1E 9F 44 AF 63 7D CE E4 0B 11 CE B0 F6 4E 09 58 6C BB BB 6E
            F1 E9 EB F1 DD 1E B2 23 56 E0 72 30 C9 84 3B 98 AF 69 9B 97
            1F 1A ED 03 DC 04 AC EB BB FB 98 17 32 C4 5D 15 F4 C0 6A 1D
            A7 C7 9A 6B 62 9E 43 CA 88 66 B8 74 E7 9C AB 45 EC 54 BA E5
            66 0C 42 90 3E B5 84 74 64 77 59 29 00 55 3D 75 AE B1 A0 1B
            AC BC B9 36 E5 BD FD E9 A7 74 47 EA DA 5E 0A 23 84 57 B8 64
            01 50 17 42 19 48 E1 23 90 D0 26 17 EC 2C 32 95 37 61 CD FA
            57 86 72 21 7A F0 68 BE 48 70 53 B3 32 B2 A2 B2 8D FF 20 D7
            2F D8 9E 3F A7 70 F6 10 01 51 5D 6A E8 C2 62 C2 71 93 8B 7B
            F4 7E 08 C4 8A 4B B3 EB 39 5B 7F 55 1E 6A 3B 0C B8 6C 98 F6
            EB B3 05 A3 FC EA E3 F1 A2 40 6D 1A E9 6A 21 3C 72 19 CC 9F
            FB B4 CD 05 D3 01 E1 86 29 C3 89 3E 91 B5 2A 4B DF
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 B2 8A D7 13 BB 54 B3 53 0A 0F 66 7C 59 FC 3E 59 D6 10 9A
           61 2B 71 ED D6 60 F4 82 1F 16 38 F4 A9 D7 9F 35 D9 F3 F7 59
           F2 00 42 32 F0 0E 09 21 D2 7C D2 7D 87 A1 86 69 E9 41 1D D6
           7D 99 A1 59 3A DF 05 C0 89 70 F1 EC 47 FF 6A 48 1E DB EC 55
           27 27 58 2B 66 D5 29 34 77 89 08 53 EF 7F 0B 38 AE 5A CA D0
           76 01 D4 EF A4 3F 6B 0B 1F 71 E9 2E B3 1D 20 6D E3 69 F9 8D
           6E F9 1F A7 C8 E2 90 08 66 13 C8 8C 72 AC CA E5 24 0E 0F 44
           BD E0 CB 2D C5 0B 9F A2 89 91 76 19 53 46 9A 9A 03 DC 98 19
           E6 60 44 91 F7 40 D4 8C CC 33 26 A7 CB 08 7E 61 66 E8 67 7E
           A1 16 34 C5 60 7B B4 0B 39 3E 41 7E F7 67 65 69 ED 65 51 A7 [...]
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/25

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2013/10/18

Ports

tcp/25

```
Here is the list of SSL ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2(40)              Mac=MD5
export
      EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
      EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
      EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
```

```
    SSLv3
      ADH-DES-CBC-SHA             Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
      EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      ADH-DES-CBC-SHA             Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA           [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/25

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-ADH-DES-CBC-SHA         Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-DES-CBC-SHA             Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-ADH-DES-CBC-SHA         Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-DES-CBC-SHA             Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      ADH-DES-CBC-SHA             Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
      EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      ADH-DES-CBC-SHA             Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
```

```
    DES-CBC-SHA                 Kx=RSA          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      ADH-DES-CBC3-SHA          Kx=DH           Au=None     Enc=3DES-CBC(168)        Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA      Kx=DH           Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA        Kx=DH           Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA        Kx=DH           Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-C [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/25

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA   Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA   Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC-SHA       Kx=DH           Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA       Kx=DH           Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA      Kx=DH           Au=RSA      Enc=3DES(168)            Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA      Kx=DH           Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA        Kx=DH           Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA        Kx=DH           Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA   Kx=DH           Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
```

```
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
      ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      ECDHE-RSA-RC4-SHA            Kx=ECDH        Au=RSA      Enc=RC4(128)             Mac=SHA1
      n/a                          Kx=ECDHE       Au=RSA      Enc=AES-CBC(128)         Mac=SHA256

      n/a                          Kx=ECDHE       Au=RSA      Enc=AES-CBC(256)         Mac=SHA384


  The fields above are :

    {OpenSSL ciphername}
    Kx={key exchange}
   [...]
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports

tcp/25

```
  This port supports resuming SSLv3 sessions.
```

110/tcp

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Ports

tcp/110

```
  The following certificate was found at the top of the certificate
```

```
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2012/10/25

Ports

tcp/110

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
|-Issuer  : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

65821 - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/12/11

Ports

tcp/110

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      RC4-MD5                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=SHA1

    TLSv1
      RC4-MD5                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/110

```
Port 110/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/110

```
A POP3 server is running on this port.
```

42087 - POP3 Service STLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote POP3 service supports the use of the 'STLS' command to switch from a plaintext to an encrypted communications channel.

See Also

http://en.wikipedia.org/wiki/STARTTLS

http://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/09, Modification date: 2011/03/10

Ports

tcp/110

```
Here is the POP3 server's SSL certificate that Nessus was able to
collect after sending a 'STLS' command :

------------------------------ snip ------------------------------
Subject Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Issuer Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Serial Number: 00 C0 72 11 13 D3 B0 7C 71

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 18 16:21:17 2013 GMT
```

```
Not Valid After: Oct 18 16:21:17 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BC 3B 40 F0 74 E3 4C F5 5D 81 B8 3B D6 E3 E0 FE 61 85 AE
            E7 68 54 56 A0 F5 FB BE 8D 38 9D 65 A7 B4 0F 5B DF 78 00 FE
            DA 03 87 F7 0B 93 9C 7B 6A 5C FD B4 56 2D 4C F9 D5 BF 83 4A
            83 31 C4 A2 9F 9F BB AF 59 A4 D3 99 4B 75 9E 54 31 2B D2 AA
            81 0B B4 D1 83 C1 4E 6D 8C CB 5F CC ED 58 F4 B9 8E 31 ED DB
            9A 03 F5 FE 72 35 14 5B 85 38 FD 60 75 4B F0 DB 16 84 14 36
            16 AD 48 5E 96 A6 93 C2 83 B8 2D EC 94 58 F8 7D C4 F6 F4 6B
            17 C1 47 14 ED 8F DD 1C 46 E8 84 5F E2 81 43 FF 01 A7 E9 23
            D0 BA FC CA 1A B7 90 DD 10 BC 90 1E 64 47 BE E4 5A 18 E2 43
            48 5E 31 72 89 6A 14 74 54 72 5A 9F 44 AA 6C 3A F1 5C 90 4C
            CB 7F E5 F9 89 7A 08 92 51 43 F4 83 A4 1C 79 AE 0D E2 D1 D1
            62 BB 36 0C 69 90 B3 0B 35 65 53 7B D1 B7 32 03 E8 44 2C F6
            8A 92 A9 C0 00 29 A8 2C DE 33 68 DB 28 A6 85 5A 23
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 45 91 E1 C2 10 F7 3C 7D 0B DC AC BB 49 F2 6C E8 FB 90 CC
           23 D7 6A E7 59 2C 1E 95 D1 AD F7 45 E8 0C 93 E5 DF C9 2A D0
           83 FF 69 1A 16 C0 75 A5 6D B7 E7 6C A5 34 7C AB 74 C0 63 18
           64 4C 4B D9 A4 6D 7F AE 97 24 03 A6 E2 4A FF 93 4D 08 8B 82
           CC DF CC 5A 1D 1A 5C A0 5D 2C C1 D6 E9 B4 D1 34 B3 01 9D B1 [...]
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

http://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/110

```
Remote POP server banner :

+OK Dovecot ready.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports
tcp/110

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports
tcp/110

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports
tcp/110

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Issuer Name:
```

```
Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Serial Number: 00 C0 72 11 13 D3 B0 7C 71

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 18 16:21:17 2013 GMT
Not Valid After: Oct 18 16:21:17 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BC 3B 40 F0 74 E3 4C F5 5D 81 B8 3B D6 E3 E0 FE 61 85 AE
            E7 68 54 56 A0 F5 FB BE 8D 38 9D 65 A7 B4 0F 5B DF 78 00 FE
            DA 03 87 F7 0B 93 9C 7B 6A 5C FD B4 56 2D 4C F9 D5 BF 83 4A
            83 31 C4 A2 9F 9F BB AF 59 A4 D3 99 4B 75 9E 54 31 2B D2 AA
            81 0B B4 D1 83 C1 4E 6D 8C CB 5F CC ED 58 F4 B9 8E 31 ED DB
            9A 03 F5 FE 72 35 14 5B 85 38 FD 60 75 4B F0 DB 16 84 14 36
            16 AD 48 5E 96 A6 93 C2 83 B8 2D EC 94 58 F8 7D C4 F6 F4 6B
            17 C1 47 14 ED 8F DD 1C 46 E8 84 5F E2 81 43 FF 01 A7 E9 23
            D0 BA FC CA 1A B7 90 DD 10 BC 90 1E 64 47 BE E4 5A 18 E2 43
            48 5E 31 72 89 6A 14 74 54 72 5A 9F 44 AA 6C 3A F1 5C 90 4C
            CB 7F E5 F9 89 7A 08 92 51 43 F4 83 A4 1C 79 AE 0D E2 D1 D1
            62 BB 36 0C 69 90 B3 0B 35 65 53 7B D1 B7 32 03 E8 44 2C F6
            8A 92 A9 C0 00 29 A8 2C DE 33 68 DB 28 A6 85 5A 23
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 45 91 E1 C2 10 F7 3C 7D 0B DC AC BB 49 F2 6C E8 FB 90 CC
           23 D7 6A E7 59 2C 1E 95 D1 AD F7 45 E8 0C 93 E5 DF C9 2A D0
           83 FF 69 1A 16 C0 75 A5 6D B7 E7 6C A5 34 7C AB 74 C0 63 18
           64 4C 4B D9 A4 6D 7F AE 97 24 03 A6 E2 4A FF 93 4D 08 8B 82
           CC DF CC 5A 1D 1A 5C A0 5D 2C C1 D6 E9 B4 D1 34 B3 01 9D B1
           C8 AE 6E 4A 92 09 30 B4 B8 02 CD 76 F3 F9 80 E4 24 76 D2 40
           F0 94 DF A0 DA 34 4F 70 B0 1B 3B FD AB 1F 3A 1C 10 4F 34 E6
           FE DE 4A 1F E2 EA F [...]
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/110

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2013/10/18

Ports

tcp/110

```
Here is the list of SSL ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES(168)            Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      CAMELLIA128-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      CAMELLIA256-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
      RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1
      SEED-SHA                     Kx=RSA         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={mess [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/110

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      CAMELLIA128-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      CAMELLIA256-SHA              Kx=RSA         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      SEED-SHA                     Kx=RSA         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/110

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)
```

```
    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

143/tcp

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Ports

tcp/143

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer.

Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2012/10/25

Ports

tcp/143

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
|-Issuer  : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

65821 - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/12/11

Ports
tcp/143

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      RC4-MD5                    Kx=RSA         Au=RSA       Enc=RC4(128)              Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA       Enc=RC4(128)              Mac=SHA1

    TLSv1
      RC4-MD5                    Kx=RSA         Au=RSA       Enc=RC4(128)              Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA       Enc=RC4(128)              Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports
tcp/143

```
Port 143/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports
tcp/143

```
An IMAP server is running on this port.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/03/18, Modification date: 2011/03/16

Ports

tcp/143

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED]
 Dovecot ready.
```

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote IMAP service supports the use of the 'STARTTLS' command to switch from a plaintext to an encrypted communications channel.

See Also

http://en.wikipedia.org/wiki/STARTTLS

http://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/09, Modification date: 2011/03/10

Ports

tcp/143

```
Here is the IMAP server's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Issuer Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Serial Number: 00 C0 72 11 13 D3 B0 7C 71

Version: 3
```

```
Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 18 16:21:17 2013 GMT
Not Valid After: Oct 18 16:21:17 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BC 3B 40 F0 74 E3 4C F5 5D 81 B8 3B D6 E3 E0 FE 61 85 AE
            E7 68 54 56 A0 F5 FB BE 8D 38 9D 65 A7 B4 0F 5B DF 78 00 FE
            DA 03 87 F7 0B 93 9C 7B 6A 5C FD B4 56 2D 4C F9 D5 BF 83 4A
            83 31 C4 A2 9F 9F BB AF 59 A4 D3 99 4B 75 9E 54 31 2B D2 AA
            81 0B B4 D1 83 C1 4E 6D 8C CB 5F CC ED 58 F4 B9 8E 31 ED DB
            9A 03 F5 FE 72 35 14 5B 85 38 FD 60 75 4B F0 DB 16 84 14 36
            16 AD 48 5E 96 A6 93 C2 83 B8 2D EC 94 58 F8 7D C4 F6 F4 6B
            17 C1 47 14 ED 8F DD 1C 46 E8 84 5F E2 81 43 FF 01 A7 E9 23
            D0 BA FC CA 1A B7 90 DD 10 BC 90 1E 64 47 BE E4 5A 18 E2 43
            48 5E 31 72 89 6A 14 74 54 72 5A 9F 44 AA 6C 3A F1 5C 90 4C
            CB 7F E5 F9 89 7A 08 92 51 43 F4 83 A4 1C 79 AE 0D E2 D1 D1
            62 BB 36 0C 69 90 B3 0B 35 65 53 7B D1 B7 32 03 E8 44 2C F6
            8A 92 A9 C0 00 29 A8 2C DE 33 68 DB 28 A6 85 5A 23
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 45 91 E1 C2 10 F7 3C 7D 0B DC AC BB 49 F2 6C E8 FB 90 CC
           23 D7 6A E7 59 2C 1E 95 D1 AD F7 45 E8 0C 93 E5 DF C9 2A D0
           83 FF 69 1A 16 C0 75 A5 6D B7 E7 6C A5 34 7C AB 74 C0 63 18
           64 4C 4B D9 A4 6D 7F AE 97 24 03 A6 E2 4A FF 93 4D 08 8B 82
           CC DF CC 5A 1D 1A 5C A0 5D 2C C1 D6 E9 B4 D1 34 B3 01 9 [...]
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports

tcp/143

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports

tcp/143

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports

tcp/143

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Issuer Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Serial Number: 00 C0 72 11 13 D3 B0 7C 71

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 18 16:21:17 2013 GMT
Not Valid After: Oct 18 16:21:17 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BC 3B 40 F0 74 E3 4C F5 5D 81 B8 3B D6 E3 E0 FE 61 85 AE
            E7 68 54 56 A0 F5 FB BE 8D 38 9D 65 A7 B4 0F 5B DF 78 00 FE
            DA 03 87 F7 0B 93 9C 7B 6A 5C FD B4 56 2D 4C F9 D5 BF 83 4A
            83 31 C4 A2 9F 9F BB AF 59 A4 D3 99 4B 75 9E 54 31 2B D2 AA
            81 0B B4 D1 83 C1 4E 6D 8C CB 5F CC ED 58 F4 B9 8E 31 ED DB
            9A 03 F5 FE 72 35 14 5B 85 38 FD 60 75 4B F0 DB 16 84 14 36
            16 AD 48 5E 96 A6 93 C2 83 B8 2D EC 94 58 F8 7D C4 F6 F4 6B
            17 C1 47 14 ED 8F DD 1C 46 E8 84 5F E2 81 43 FF 01 A7 E9 23
            D0 BA FC CA 1A B7 90 DD 10 BC 90 1E 64 47 BE E4 5A 18 E2 43
```

```
            48 5E 31 72 89 6A 14 74 54 72 5A 9F 44 AA 6C 3A F1 5C 90 4C
            CB 7F E5 F9 89 7A 08 92 51 43 F4 83 A4 1C 79 AE 0D E2 D1 D1
            62 BB 36 0C 69 90 B3 0B 35 65 53 7B D1 B7 32 03 E8 44 2C F6
            8A 92 A9 C0 00 29 A8 2C DE 33 68 DB 28 A6 85 5A 23
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 45 91 E1 C2 10 F7 3C 7D 0B DC AC BB 49 F2 6C E8 FB 90 CC
           23 D7 6A E7 59 2C 1E 95 D1 AD F7 45 E8 0C 93 E5 DF C9 2A D0
           83 FF 69 1A 16 C0 75 A5 6D B7 E7 6C A5 34 7C AB 74 C0 63 18
           64 4C 4B D9 A4 6D 7F AE 97 24 03 A6 E2 4A FF 93 4D 08 8B 82
           CC DF CC 5A 1D 1A 5C A0 5D 2C C1 D6 E9 B4 D1 34 B3 01 9D B1
           C8 AE 6E 4A 92 09 30 B4 B8 02 CD 76 F3 F9 80 E4 24 76 D2 40
           F0 94 DF A0 DA 34 4F 70 B0 1B 3B FD AB 1F 3A 1C 10 4F 34 E6
           FE DE 4A 1F E2 EA F [...]
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/143

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2013/10/18

Ports

tcp/143

```
Here is the list of SSL ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1
```

```
    DES-CBC3-SHA                Kx=RSA      Au=RSA      Enc=3DES(168)           Mac=SHA1
    RC4-MD5                     Kx=RSA      Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-SHA                     Kx=RSA      Au=RSA      Enc=RC4(128)            Mac=SHA1

  TLSv1
    EDH-RSA-DES-CBC3-SHA        Kx=DH       Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1
    DHE-RSA-AES128-SHA          Kx=DH       Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
    DHE-RSA-AES256-SHA          Kx=DH       Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
    DHE-RSA-CAMELLIA128-SHA     Kx=DH       Au=RSA      Enc=Camellia-CBC(128)   Mac=SHA1
    DHE-RSA-CAMELLIA256-SHA     Kx=DH       Au=RSA      Enc=Camellia-CBC(256)   Mac=SHA1
    DHE-RSA-SEED-SHA            Kx=DH       Au=RSA      Enc=SEED-CBC(128)       Mac=SHA1
    DES-CBC3-SHA                Kx=RSA      Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1
    AES128-SHA                  Kx=RSA      Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
    AES256-SHA                  Kx=RSA      Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
    CAMELLIA128-SHA             Kx=RSA      Au=RSA      Enc=Camellia-CBC(128)   Mac=SHA1
    CAMELLIA256-SHA             Kx=RSA      Au=RSA      Enc=Camellia-CBC(256)   Mac=SHA1
    RC4-MD5                     Kx=RSA      Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-SHA                     Kx=RSA      Au=RSA      Enc=RC4(128)            Mac=SHA1
    SEED-SHA                    Kx=RSA      Au=RSA      Enc=SEED-CBC(128)       Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={mess [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/143

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

  TLSv1
    EDH-RSA-DES-CBC3-SHA        Kx=DH       Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1
    DHE-RSA-AES128-SHA          Kx=DH       Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
    DHE-RSA-AES256-SHA          Kx=DH       Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
    DHE-RSA-CAMELLIA128-SHA     Kx=DH       Au=RSA      Enc=Camellia-CBC(128)   Mac=SHA1
    DHE-RSA-CAMELLIA256-SHA     Kx=DH       Au=RSA      Enc=Camellia-CBC(256)   Mac=SHA1
    DHE-RSA-SEED-SHA            Kx=DH       Au=RSA      Enc=SEED-CBC(128)       Mac=SHA1
    DES-CBC3-SHA                Kx=RSA      Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1
    AES128-SHA                  Kx=RSA      Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
    AES256-SHA                  Kx=RSA      Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
```

```
      CAMELLIA128-SHA             Kx=RSA        Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      CAMELLIA256-SHA             Kx=RSA        Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      SEED-SHA                    Kx=RSA        Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/143

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA        Kx=DH         Au=RSA      Enc=3DES(168)            Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA        Kx=DH         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA          Kx=DH         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA          Kx=DH         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA     Kx=DH         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA     Kx=DH         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA            Kx=DH         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

993/tcp

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Ports

tcp/993

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer.
Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2012/10/25

Ports

tcp/993

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :
```

```
|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
|-Issuer  : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

65821 - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/12/11

Ports

tcp/993

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

    TLSv1
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/993

```
Port 993/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/993

```
A TLSv1 server answered on this port.
```

tcp/993

```
An IMAP server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/993

```
A TLSv1 server answered on this port.
```

tcp/993

```
An IMAP server is running on this port through TLSv1.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/03/18, Modification date: 2011/03/16

Ports

tcp/993

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot
 ready.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports

tcp/993

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports

tcp/993

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports

tcp/993

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Issuer Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Serial Number: 00 C0 72 11 13 D3 B0 7C 71

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 18 16:21:17 2013 GMT
Not Valid After: Oct 18 16:21:17 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BC 3B 40 F0 74 E3 4C F5 5D 81 B8 3B D6 E3 E0 FE 61 85 AE
            E7 68 54 56 A0 F5 FB BE 8D 38 9D 65 A7 B4 0F 5B DF 78 00 FE
            DA 03 87 F7 0B 93 9C 7B 6A 5C FD B4 56 2D 4C F9 D5 BF 83 4A
            83 31 C4 A2 9F 9F BB AF 59 A4 D3 99 4B 75 9E 54 31 2B D2 AA
            81 0B B4 D1 83 C1 4E 6D 8C CB 5F CC ED 58 F4 B9 8E 31 ED DB
            9A 03 F5 FE 72 35 14 5B 85 38 FD 60 75 4B F0 DB 16 84 14 36
            16 AD 48 5E 96 A6 93 C2 83 B8 2D EC 94 58 F8 7D C4 F6 F4 6B
            17 C1 47 14 ED 8F DD 1C 46 E8 84 5F E2 81 43 FF 01 A7 E9 23
            D0 BA FC CA 1A B7 90 DD 10 BC 90 1E 64 47 BE E4 5A 18 E2 43
            48 5E 31 72 89 6A 14 74 54 72 5A 9F 44 AA 6C 3A F1 5C 90 4C
            CB 7F E5 F9 89 7A 08 92 51 43 F4 83 A4 1C 79 AE 0D E2 D1 D1
            62 BB 36 0C 69 90 B3 0B 35 65 53 7B D1 B7 32 03 E8 44 2C F6
            8A 92 A9 C0 00 29 A8 2C DE 33 68 DB 28 A6 85 5A 23
```

```
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 45 91 E1 C2 10 F7 3C 7D 0B DC AC BB 49 F2 6C E8 FB 90 CC
           23 D7 6A E7 59 2C 1E 95 D1 AD F7 45 E8 0C 93 E5 DF C9 2A D0
           83 FF 69 1A 16 C0 75 A5 6D B7 E7 6C A5 34 7C AB 74 C0 63 18
           64 4C 4B D9 A4 6D 7F AE 97 24 03 A6 E2 4A FF 93 4D 08 8B 82
           CC DF CC 5A 1D 1A 5C A0 5D 2C C1 D6 E9 B4 D1 34 B3 01 9D B1
           C8 AE 6E 4A 92 09 30 B4 B8 02 CD 76 F3 F9 80 E4 24 76 D2 40
           F0 94 DF A0 DA 34 4F 70 B0 1B 3B FD AB 1F 3A 1C 10 4F 34 E6
           FE DE 4A 1F E2 EA F [...]
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/993

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2013/10/18

Ports

tcp/993

```
Here is the list of SSL ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH         Au=RSA      Enc=3DES(168)          Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA        Au=RSA      Enc=3DES(168)          Mac=SHA1
      RC4-MD5                      Kx=RSA        Au=RSA      Enc=RC4(128)           Mac=MD5
      RC4-SHA                      Kx=RSA        Au=RSA      Enc=RC4(128)           Mac=SHA1
```

```
    TLSv1
      EDH-RSA-DES-CBC3-SHA          Kx=DH         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA            Kx=DH         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA            Kx=DH         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA       Kx=DH         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA       Kx=DH         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA              Kx=DH         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
      DES-CBC3-SHA                  Kx=RSA        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      AES128-SHA                    Kx=RSA        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      AES256-SHA                    Kx=RSA        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      CAMELLIA128-SHA               Kx=RSA        Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      CAMELLIA256-SHA               Kx=RSA        Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      RC4-MD5                       Kx=RSA        Au=RSA      Enc=RC4(128)             Mac=MD5
      RC4-SHA                       Kx=RSA        Au=RSA      Enc=RC4(128)             Mac=SHA1
      SEED-SHA                      Kx=RSA        Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

  The fields above are :

    {OpenSSL ciphername}
    Kx={key exchange}
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={mess [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/993

```
  Here is the list of SSL CBC ciphers supported by the remote server :

    High Strength Ciphers (>= 112-bit key)

      TLSv1
        EDH-RSA-DES-CBC3-SHA          Kx=DH         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
        DHE-RSA-AES128-SHA            Kx=DH         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
        DHE-RSA-AES256-SHA            Kx=DH         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
        DHE-RSA-CAMELLIA128-SHA       Kx=DH         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
        DHE-RSA-CAMELLIA256-SHA       Kx=DH         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
        DHE-RSA-SEED-SHA              Kx=DH         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
        DES-CBC3-SHA                  Kx=RSA        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
        AES128-SHA                    Kx=RSA        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
        AES256-SHA                    Kx=RSA        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
        CAMELLIA128-SHA               Kx=RSA        Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
        CAMELLIA256-SHA               Kx=RSA        Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
        SEED-SHA                      Kx=RSA        Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/993

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

995/tcp

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Ports

tcp/995

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer.
Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2012/10/25

Ports

tcp/995

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

```
|-Issuer  : O=Dovecot mail server/OU=ubuntu/CN=ubuntu/E=root@dominio.com
```

65821 - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/12/11

Ports

tcp/995

```
Here is the list of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      RC4-MD5                    Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

    TLSv1
      RC4-MD5                    Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                    Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/995

```
Port 995/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/995

```
A POP3 server is running on this port through TLSv1.
```

tcp/995

```
A TLSv1 server answered on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/995

```
A POP3 server is running on this port through TLSv1.
```

tcp/995

```
A TLSv1 server answered on this port.
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

http://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/995

```
Remote POP server banner :

+OK Dovecot ready.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports

tcp/995

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports

tcp/995

```
Nessus was able to confirm that the following compression method is
supported by the target :

  NULL (0x00)
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports

tcp/995

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Issuer Name:

Organization: Dovecot mail server
Organization Unit: ubuntu
Common Name: ubuntu
Email Address: root@dominio.com

Serial Number: 00 C0 72 11 13 D3 B0 7C 71

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 18 16:21:17 2013 GMT
Not Valid After: Oct 18 16:21:17 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BC 3B 40 F0 74 E3 4C F5 5D 81 B8 3B D6 E3 E0 FE 61 85 AE
            E7 68 54 56 A0 F5 FB BE 8D 38 9D 65 A7 B4 0F 5B DF 78 00 FE
            DA 03 87 F7 0B 93 9C 7B 6A 5C FD B4 56 2D 4C F9 D5 BF 83 4A
            83 31 C4 A2 9F 9F BB AF 59 A4 D3 99 4B 75 9E 54 31 2B D2 AA
            81 0B B4 D1 83 C1 4E 6D 8C CB 5F CC ED 58 F4 B9 8E 31 ED DB
            9A 03 F5 FE 72 35 14 5B 85 38 FD 60 75 4B F0 DB 16 84 14 36
            16 AD 48 5E 96 A6 93 C2 83 B8 2D EC 94 58 F8 7D C4 F6 F4 6B
            17 C1 47 14 ED 8F DD 1C 46 E8 84 5F E2 81 43 FF 01 A7 E9 23
```

```
            D0 BA FC CA 1A B7 90 DD 10 BC 90 1E 64 47 BE E4 5A 18 E2 43
            48 5E 31 72 89 6A 14 74 54 72 5A 9F 44 AA 6C 3A F1 5C 90 4C
            CB 7F E5 F9 89 7A 08 92 51 43 F4 83 A4 1C 79 AE 0D E2 D1 D1
            62 BB 36 0C 69 90 B3 0B 35 65 53 7B D1 B7 32 03 E8 44 2C F6
            8A 92 A9 C0 00 29 A8 2C DE 33 68 DB 28 A6 85 5A 23
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 45 91 E1 C2 10 F7 3C 7D 0B DC AC BB 49 F2 6C E8 FB 90 CC
           23 D7 6A E7 59 2C 1E 95 D1 AD F7 45 E8 0C 93 E5 DF C9 2A D0
           83 FF 69 1A 16 C0 75 A5 6D B7 E7 6C A5 34 7C AB 74 C0 63 18
           64 4C 4B D9 A4 6D 7F AE 97 24 03 A6 E2 4A FF 93 4D 08 8B 82
           CC DF CC 5A 1D 1A 5C A0 5D 2C C1 D6 E9 B4 D1 34 B3 01 9D B1
           C8 AE 6E 4A 92 09 30 B4 B8 02 CD 76 F3 F9 80 E4 24 76 D2 40
           F0 94 DF A0 DA 34 4F 70 B0 1B 3B FD AB 1F 3A 1C 10 4F 34 E6
           FE DE 4A 1F E2 EA F [...]
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/995

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2013/10/18

Ports

tcp/995

```
Here is the list of SSL ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
```

```
    EDH-RSA-DES-CBC3-SHA          Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1
    DES-CBC3-SHA                  Kx=RSA         Au=RSA      Enc=3DES(168)            Mac=SHA1
    RC4-MD5                       Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                       Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

  TLSv1
    EDH-RSA-DES-CBC3-SHA          Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DHE-RSA-AES128-SHA            Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA            Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-CAMELLIA128-SHA       Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
    DHE-RSA-CAMELLIA256-SHA       Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
    DHE-RSA-SEED-SHA              Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
    DES-CBC3-SHA                  Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    AES128-SHA                    Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                    Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    CAMELLIA128-SHA               Kx=RSA         Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
    CAMELLIA256-SHA               Kx=RSA         Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
    RC4-MD5                       Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                       Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1
    SEED-SHA                      Kx=RSA         Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={mess [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/995

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA        Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA          Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA          Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA     Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA     Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA            Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      AES128-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
```

```
      AES256-SHA                  Kx=RSA       Au=RSA     Enc=AES-CBC(256)          Mac=SHA1
      CAMELLIA128-SHA             Kx=RSA       Au=RSA     Enc=Camellia-CBC(128)     Mac=SHA1
      CAMELLIA256-SHA             Kx=RSA       Au=RSA     Enc=Camellia-CBC(256)     Mac=SHA1
      SEED-SHA                    Kx=RSA       Au=RSA     Enc=SEED-CBC(128)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/995

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA        Kx=DH        Au=RSA     Enc=3DES(168)             Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA        Kx=DH        Au=RSA     Enc=3DES-CBC(168)         Mac=SHA1
      DHE-RSA-AES128-SHA          Kx=DH        Au=RSA     Enc=AES-CBC(128)          Mac=SHA1
      DHE-RSA-AES256-SHA          Kx=DH        Au=RSA     Enc=AES-CBC(256)          Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA     Kx=DH        Au=RSA     Enc=Camellia-CBC(128)     Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA     Kx=DH        Au=RSA     Enc=Camellia-CBC(256)     Mac=SHA1
      DHE-RSA-SEED-SHA            Kx=DH        Au=RSA     Enc=SEED-CBC(128)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

5353/udp

12218 - mDNS Detection (Remote Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2004/04/28, Modification date: 2013/05/31

Ports

udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : ubuntu.local.

  - Advertised services :
    o Service name      : ubuntu [00:50:56:35:9f:4f]._workstation._tcp.local.
      Port number       : 9
    o Service name      : ubuntu._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : X86_64
  - OS                  : LINUX
```

192.168.2.7

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:22:54 2014

Host Information

IP:	192.168.2.7
OS:	Linux Kernel 3.0 on Ubuntu 12.04 (precise), Linux Kernel 3.5 on Ubuntu 12.10 (quantal), Linux Kernel 3.8 on Ubuntu 13.04 (raring)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	21	25

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is -5050 seconds.
```

0/tcp

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

This script extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2013/10/31

Ports

tcp/0

```
The linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Linux Kernel 3.5 on Ubuntu 12.10 (quantal)
Linux Kernel 3.8 on Ubuntu 13.04 (raring)
Confidence Level : 85
Method : HTTP


The remote host is running one of these operating systems :
Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Linux Kernel 3.5 on Ubuntu 12.10 (quantal)
Linux Kernel 3.8 on Ubuntu 13.04 (raring)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 85
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports

tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:canonical:ubuntu_linux:12.04
  cpe:/o:canonical:ubuntu_linux:12.10 -> Canonical Ubuntu Linux 12.10
  cpe:/o:canonical:ubuntu_linux:13.04 -> Canonical Ubuntu Linux 13.04

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server 2.2.22
  cpe:/a:php:php:5.3.10 -> PHP 5.3.10
```

66334 - Patch Report

Synopsis

The remote host is missing several patches

Description

The remote host is missing one or several security patches.
This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below

Risk Factor

None

Plugin Information:

Publication date: 2013/05/07, Modification date: 2013/12/18

Ports

tcp/0

```
. You need to take the following 2 actions:

[ PHP expose_php Information Disclosure (46803) ]

+ Action to take: In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off'
 to disable this behavior.  Restart the web server daemon to put this change into effect.


[ Joomla! libraries/idna_convert/example.php lang Parameter XSS (69280) ]

+ Action to take: Unknown at this time.  It's suggested that the script be removed.
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
```

```
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 1236 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.2.7 :
192.168.1.121
?
192.168.2.7
```

80/tcp

46803 - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.
Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

http://www.0php.com/php_easter_egg.php

http://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF OSVDB:12184

Plugin Information:

Publication date: 2010/06/03, Modification date: 2012/09/05

Ports

tcp/80

```
Nessus was able to verify the issue using the following URL :

  http://192.168.2.7/index.php/component/mailto/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

69280 - Joomla! libraries/idna_convert/example.php lang Parameter XSS

Synopsis

The remote web server hosts a PHP script that is affected by a cross-site scripting vulnerability.

Description

The version of Joomla! installed on the remote host is affected by a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input to the 'lang' parameter of the 'libraries/idna_convert/example.php' script. An attacker may be able to leverage this issue to inject arbitrary HTML and script code into a user's browser to be executed within the security context of the affected site.

See Also

http://www.nessus.org/u?0af472dd

https://github.com/joomla/joomla-cms/issues/1658

Solution

Unknown at this time. It's suggested that the script be removed.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

BID	61600
XREF	OSVDB:95998

Plugin Information:

Publication date: 2013/08/09, Modification date: 2013/08/09

Ports

tcp/80

```
Nessus was able to exploit the issue using the following URL :

  http://192.168.2.7/libraries/idna_convert/example.php?
lang=";><script>alert('joomla_example_lang_xss.nasl-1388992759');</script>
```

26194 - Web Server Uses Plain Text Authentication Forms

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724

Plugin Information:

Publication date: 2007/09/28, Modification date: 2011/09/15

Ports

tcp/80

```
Page : /administrator/
Destination Page: /administrator/index.php

Page : /index.php/login
Destination Page: /index.php/login?task=user.login

Page : /index.php/log-out
Destination Page: /index.php/log-out?task=user.login

Page : /administrator/index.php
Destination Page: /administrator/index.php
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports
tcp/80

```
A web server is running on this port.
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2013/04/02

Ports
tcp/80

```
The following directories were discovered:
/administrator, /cgi-bin, /includes, /logs, /tmp, /bin, /icons, /images, /libraries, /templates

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10662 - Web mirroring

Synopsis

Nessus crawled the remote web site.

Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2013/04/11

Ports
tcp/80

```
Webmirror performed 56 queries in 41s (1.365 queries per second)

The following CGI have been discovered:


+ CGI: /index.php
  Methods: GET,POST
  Argument: Itemid
```

```
   Value: 101
  Argument: format
   Value: feed
  Argument: option
   Value: com_search
   Value: com_users
  Argument: searchword
   Value: Search...
  Argument: task
   Value: search
  Argument: type
   Value: rss
   Value: atom
  Argument: view
   Value: remind
   Value: reset


+ CGI: /index.php/component/search/
  Methods: GET,POST
  Argument: Itemid
   Value: 101
   Value: 108
   Value: 102
   Value: 107
  Argument: areas[]
   Value: categories
   Value: contacts
   Value: content
   Value: newsfeeds
   Value: weblinks
  Argument: catid
   Value: 9
  Argument: format
   Value: opensearch
  Argument: id
   Value: 3
   Value: 4
   Value: 6
   Value: 5
  Argument: option
   Value: com_search
  Argument: ordering
   Value: newest
   Value: oldest
   Value: popular
   Value: alpha
   Value: category
  Argument: searchphrase
   Value: all
   Value: any
   Value: exact
  Argument: searchword
   Value: Search...
  Argument: task
   Value: search


+ CGI: /index.php/3-welcome-to-your-blog
  Methods: GET
  Argument: layout
   Value: default
  Argument: page
  Argument: print
   Value: 1
  Argument: tmpl
   Value: component


+ CGI: /index.php/component/mailto/
  Methods: GET
  Argument: link
   Value: 4bddf76b2e160e058e70370acdb30d32b785e096
   Value: 3e44ec254174cb35555d81aadb5f0cef9c29b5b1
   Value: e2756a8d30c7adc0d52712c7035332c09aedc24a
```

```
    Value: 4ff9329b9b7e232f36040b676408efa4c544f38a
    Value: c8d4a99cde15b4c61538239e371e1b26eb349167
  Argument: template
    Value: protostar
  Argument: tmpl
    Value: component


+ CGI: /index.php/4-about-your-home-page
  Methods: GET
  Argument: layout
    Value: default
  Argument: page
  Argument: print
    Value: 1
  Argument: tmpl
    Value: component


+ CGI: /index.php/6-your-template
  Methods: GET
  Argument: layout
    Value: default
  Argument: page
  Argument: print
    Value: 1
  Argument: tmpl
    Value: co [...]
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/80

```
5 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://community.joomla.org/blogs/community.html - /
http://community.joomla.org/blogs/leadership.html - /
http://extensions.joomla.org            - /
http://fonts.googleapis.com/css?family=Open+Sans - /
http://www.joomla.org                   - /administrator/
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2011/09/28

Ports

tcp/80

```
Page : /administrator/
Destination Page: /administrator/index.php

Page : /index.php/login
Destination Page: /index.php/login?task=user.login

Page : /index.php/log-out
Destination Page: /index.php/log-out?task=user.login

Page : /administrator/index.php
Destination Page: /administrator/index.php
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2013/12/03

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports
tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /administrator/templates
    /administrator/templates/isis
    /administrator/templates/isis/css
    /bin
    /icons
    /images
    /includes
    /libraries
    /logs
    /media
    /media/jui
    /media/jui/css
    /templates
    /templates/protostar/css
    /tmp
```

48243 - PHP Version
Synopsis

It is possible to obtain the version number of the remote PHP install.

Description

This plugin attempts to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2013/10/23

Ports
tcp/80

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.10-1ubuntu3.8
  Source  : X-Powered-By: PHP/5.3.10-1ubuntu3.8
```

24260 - HyperText Transfer Protocol (HTTP) Information
Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports
tcp/80

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Fri, 24 Jan 2014 08:40:31 GMT
  Server: Apache/2.2.22 (Ubuntu)
  X-Powered-By: PHP/5.3.10-1ubuntu3.8
  P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
  Cache-Control: no-cache
  Pragma: no-cache
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=utf-8
```

21142 - Joomla! Detection

Synopsis

The remote web server contains a content management system written in PHP.

Description

The remote host is running Joomla!, an open source content management system written in PHP.

See Also

http://www.joomla.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/03/24, Modification date: 2013/06/27

Ports

tcp/80

```
The following instance of Joomla! was detected on the remote host :

  Version : 3.1.5
  URL     : http://192.168.2.7/
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/10/02

Ports

tcp/80

```
Give Nessus credentials to perform local checks.
```

5353/udp

12218 - mDNS Detection (Remote Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2004/04/28, Modification date: 2013/05/31

Ports

udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : ubuntu-2.local.

  - Advertised services :
    o Service name      : ubuntu-2 [00:50:56:33:82:84]._workstation._tcp.local.
      Port number       : 9
    o Service name      : ubuntu-2._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : X86_64
  - OS                  : LINUX
```

192.168.2.105

Scan Information

Start time:	Mon Jan 6 08:02:18 2014
End time:	Mon Jan 6 08:49:23 2014

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.2.105
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Results Summary

Critical	High	Medium	Low	Info	Total
3	3	15	7	70	98

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 5622 seconds.
```

0/tcp

33850 - Unsupported Unix Operating System

Synopsis

The remote host is running an obsolete operating system.

Description

According to its version, the remote Unix operating system is obsolete and is no longer maintained by its vendor or provider.
Lack of support implies that no new security patches will be released for it.

Solution

Upgrade to a newer version.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2008/08/08, Modification date: 2013/12/17

Ports

tcp/0

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 13.10.

For more information, see : https://wiki.ubuntu.com/Releases
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

This script extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2013/10/31

Ports

tcp/0

```
The linux distribution detected was :
 - Ubuntu 8.04 (gutsy)
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2013/09/03

Ports

tcp/0

```
Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Confidence Level : 95
Method : SSH

Not all fingerprints could give a match.  If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org.  Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SinFP:
   P1:B10113:F0x12:W5840:O0204ffff:M1460:
   P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030305:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:5202_7_p=23R
SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
 Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
 Affairs
ed093088706603bfd5dc237399b498da2d4d31c6

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1


The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/12/22

Ports

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:8.04

Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH 4.7
  cpe:/a:samba:samba:3.0.20 -> Samba 3.0.20
  cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server 2.2.8
  cpe:/a:php:php:5.2.4 -> PHP 5.2.4
  cpe:/a:isc:bind:9.4.
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

66334 - Patch Report

Synopsis

The remote host is missing several patches

Description

The remote host is missing one or several security patches.
This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below

Risk Factor

None

Plugin Information:

Publication date: 2013/05/07, Modification date: 2013/12/18

Ports

tcp/0

```
. You need to take the following 3 actions:

[ Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow (25216) ]

+ Action to take: Upgrade to Samba version 3.0.25 or later.


[ OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
 (51892) ]

+ Action to take: Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a
 patch.
```

```
+ Impact: Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Apache HTTP Server httpOnly Cookie Information Disclosure (57792) ]

+ Action to take: Upgrade to Apache version 2.2.22 or later.

+ Impact: Taking this action will resolve 2 different vulnerabilities (CVEs).
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2013/11/21

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.2.4
Plugin feed version : 201312230916
Scanner edition used : Nessus Home
Scan policy used : External Network Scan
Scanner IP : 192.168.1.121
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2014/1/6 8:02
Scan duration : 2825 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.121 to 192.168.2.105 :
192.168.1.121
?
192.168.2.105
```

21/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/21

```
Port 21/tcp was found to be open
```

22/tcp

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?5d01bdab

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	29179
CVE	CVE-2008-0166
XREF	OSVDB:45029
XREF	CWE:310

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2008/05/14, Modification date: 2011/03/21

Ports

tcp/22

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

1.9 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Publication date: 2013/10/28, Modification date: 2013/10/28

Ports

tcp/22

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

SSH is configured to allow MD5 and 96-bit MAC algorithms.

Description

The SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2013/11/22, Modification date: 2013/11/23

Ports

tcp/22

```
The following client-to-server Method Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

The following server-to-client Method Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/22

```
Port 22/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/22

```
An SSH server is running on this port.
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/10/24

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2013/12/19

Ports

tcp/22

```
Nessus negotiated the following encryption algorithm with the server : aes128-cbc

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
```

```
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/06, Modification date: 2013/10/21

Ports

tcp/22

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0


SSHv2 host key fingerprint : 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/04/03

Ports

tcp/22

```
Give Nessus credentials to perform local checks.
```

23/tcp

42263 - Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.
Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Solution

Disable this service and use SSH instead.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2009/10/27, Modification date: 2013/06/24

Ports

tcp/23

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
Ubuntu 8.04
metasploitable login:
------------------------------ snip ------------------------------
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/23

```
Port 23/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/23

```
A telnet server is running on this port.
```

10281 - Telnet Server Detection

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2012/08/30

Ports

tcp/23

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Ubuntu 8.04
metasploitable login:
------------------------------ snip ------------------------------
```

25/tcp

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This script checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information:

Publication date: 2004/12/03, Modification date: 2013/10/18

Ports

tcp/25

```
The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
```

```
Not valid after  : Apr 16 14:07:45 2010 GMT
```

52611 - SMTP Service STARTTLS Plaintext Command Injection

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.
Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

See Also

http://tools.ietf.org/html/rfc2487

http://www.securityfocus.com/archive/1/516901/30/0/threaded

Solution

Contact the vendor to see if an update is available.

Risk Factor

Medium

CVSS Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

3.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

References

BID	46767
CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165
XREF	OSVDB:71020
XREF	OSVDB:71021
XREF	OSVDB:71854
XREF	OSVDB:71946
XREF	OSVDB:73251
XREF	OSVDB:75014
XREF	OSVDB:75256
XREF	CERT:555316

Plugin Information:

Publication date: 2011/03/10, Modification date: 2012/06/14

Ports

tcp/25

```
Nessus sent the following two commands in a single packet :

  STARTTLS\r\nRSET\r\n

And the server sent the following two responses :

  220 2.0.0 Ready to start TLS
  250 2.0.0 Ok
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2012/10/25

Ports

tcp/25

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.
First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer.
Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2012/10/25

Ports

tcp/25

```
The following certificate was part of the certificate chain
sent by the remote host, but has expired :

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

20007 - SSL Version 2 (v2) Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

See Also

http://www.schneier.com/paper-ssl.pdf

http://support.microsoft.com/kb/187498

http://www.linux4beginners.info/node/disable-sslv2

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0, TLS 1.0, or higher instead.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2005-2969

Plugin Information:

Publication date: 2005/10/12, Modification date: 2013/01/25

Ports

tcp/25

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:327
XREF	CWE:326
XREF	CWE:753
XREF	CWE:803
XREF	CWE:720

Plugin Information:

Publication date: 2007/10/08, Modification date: 2013/08/30

Ports

tcp/25

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv2
      EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

    SSLv3
      EXP-ADH-DES-CBC-SHA         Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5             Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
      EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-DES-CBC-SHA             Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2(40)              Mac=MD5
export
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-DES-CBC-SHA         Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5             Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
      EXP-DES-CBC-SHA             Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2009/11/23, Modification date: 2012/04/02

Ports

tcp/25

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv2
      DES-CBC-MD5                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=MD5

    SSLv3
      ADH-DES-CBC-SHA             Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
      EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      ADH-DES-CBC-SHA             Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

51893 - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Ciphersuite Disabled Cipher Issue

Synopsis

The remote host allows the resumption of SSL sessions with a disabled cipher.

Description

The version of OpenSSL on the remote host has been shown to allow the use of disabled ciphers when resuming a session. This means that an attacker that sees (e.g. by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a disabled cipher chosen by the attacker.

Solution

Upgrade to OpenSSL 0.9.8j or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.2 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

BID	45254
CVE	CVE-2008-7270
XREF	OSVDB:69655

Plugin Information:

Publication date: 2011/02/07, Modification date: 2012/04/17

Ports

tcp/25

```
The server allowed the following session over SSLv3 to be resumed as follows :

  Session ID     : aa734424c28c0cac8716f8f2c5f79cba2fa1e4fbacd12af01eb73c44c2f86c65
  Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Resumed Cipher : SSL3_CK_EDH_DSS_DES_192_CBC3_SHA (0x0013)
```

51892 - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue

Synopsis

The remote host allows resuming SSL sessions with a weaker cipher than the one originally negotiated.

Description

The version of OpenSSL on the remote host has been shown to allow resuming session with a weaker cipher than was used when the session was initiated. This means that an attacker that sees (i.e., by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a weaker cipher chosen by the attacker.
Note that other SSL implementations may also be affected by this vulnerability.

See Also

http://openssl.org/news/secadv_20101202.txt

Solution

Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.2 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

BID	45164
CVE	CVE-2010-4180
XREF	OSVDB:69565

Plugin Information:

Publication date: 2011/02/07, Modification date: 2012/06/14

Ports
tcp/25

```
The server allowed the following session over SSLv3 to be resumed as follows :

  Session ID     : 0a244bab6b262b4cb247056e1af0db2fe8e86cb5ca109eacafe8073b88b69d64
  Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Resumed Cipher : SSL3_CK_ADH_DES_64_CBC_SHA (0x001a)

The server allowed the following session over TLSv1 to be resumed as follows :

  Session ID     : d1044044db45208db6f850e820ef4dcf79a11a5ab71a0a05f930078a2676919d
  Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Resumed Cipher : TLS1_CK_DH_anon_EXPORT_WITH_RC4_40_MD5 (0x0017)
```

45411 - SSL Certificate with Wrong Hostname

Synopsis
The SSL certificate for this service is for a different host.

Description
The commonName (CN) of the SSL certificate presented on this service is for a different machine.

Solution
Purchase or generate a proper certificate for this service.

Risk Factor
Medium

CVSS Base Score
5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information:
Publication date: 2010/04/03, Modification date: 2012/07/25

Ports
tcp/25

```
The identity known by Nessus is :

  192.168.2.105

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

42880 - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Synopsis
The remote service allows insecure renegotiation of TLS / SSL connections.

Description
The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake.
An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

See Also
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html

http://www.g-sec.lu/practicaltls.pdf

http://tools.ietf.org/html/rfc5746

Solution

Contact the vendor for specific patch information.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

References

BID	36935
CVE	CVE-2009-3555
XREF	OSVDB:59968
XREF	OSVDB:59969
XREF	OSVDB:59970
XREF	OSVDB:59971
XREF	OSVDB:59972
XREF	OSVDB:59973
XREF	OSVDB:59974
XREF	OSVDB:60366
XREF	OSVDB:60521
XREF	OSVDB:61234
XREF	OSVDB:61718
XREF	OSVDB:61784
XREF	OSVDB:61785
XREF	OSVDB:61929
XREF	OSVDB:62064
XREF	OSVDB:62135
XREF	OSVDB:62210
XREF	OSVDB:62273
XREF	OSVDB:62536
XREF	OSVDB:62877
XREF	OSVDB:64040
XREF	OSVDB:64499
XREF	OSVDB:64725
XREF	OSVDB:65202

XREF	OSVDB:66315
XREF	OSVDB:67029
XREF	OSVDB:69032
XREF	OSVDB:69561
XREF	OSVDB:70055
XREF	OSVDB:70620
XREF	OSVDB:71951
XREF	OSVDB:71961
XREF	OSVDB:74335
XREF	OSVDB:75622
XREF	OSVDB:77832
XREF	OSVDB:90597
XREF	OSVDB:99240
XREF	OSVDB:100172
XREF	CERT:120541
XREF	CWE:310

Plugin Information:

Publication date: 2009/11/24, Modification date: 2013/12/04

Ports

tcp/25

```
TLSv1 supports insecure renegotiation.

SSLv3 supports insecure renegotiation.
```

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	28482
CVE	CVE-2007-1858
XREF	OSVDB:34882

Plugin Information:

Publication date: 2008/03/28, Modification date: 2013/07/18

Ports

tcp/25

```
Here is the list of SSL anonymous ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv3
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
 export

    TLSv1
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
 export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      ADH-DES-CBC3-SHA             Kx=DH          Au=None     Enc=3DES-CBC(168)        Mac=SHA1
      ADH-RC4-MD5                  Kx=DH          Au=None     Enc=RC4(128)             Mac=MD5

    TLSv1
      ADH-DES-CBC3-SHA             Kx=DH          Au=None     Enc=3DES-CBC(168)        Mac=SHA1
      ADH-AES128-SHA               Kx=DH          Au=None     Enc=AES-CBC(128)         Mac=SHA1
      ADH-AES256-SHA               Kx=DH          Au=None     Enc=AES-CBC(256)         Mac=SHA1
      ADH-RC4-MD5                  Kx=DH          Au=None     Enc=RC4(128)             Mac=MD5

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

BID	58796
CVE	CVE-2013-2566
XREF	OSVDB:91162

Plugin Information:

Publication date: 2013/04/05, Modification date: 2013/12/11

Ports

tcp/25

```
Here is the list of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv2
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
export

    SSLv3
      EXP-ADH-RC4-MD5             Kx=DH(512)     Au=None     Enc=RC4(40)             Mac=MD5
export
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
export

    TLSv1
      EXP-ADH-RC4-MD5             Kx=DH(512)     Au=None     Enc=RC4(40)             Mac=MD5
export
      EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
export

  High Strength Ciphers (>= 112-bit key)

    SSLv2
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5

    SSLv3
      ADH-RC4-MD5                 Kx=DH          Au=None     Enc=RC4(128)            Mac=MD5
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

    TLSv1
      ADH-RC4-MD5                 Kx=DH          Au=None     Enc=RC4(128)            Mac=MD5
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
```

```
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/25

```
Port 25/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/25

```
An SMTP server is running on this port.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.
Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/25

```
Remote SMTP server banner :

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a plaintext to an encrypted communications channel.

See Also

http://en.wikipedia.org/wiki/STARTTLS

http://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/09, Modification date: 2011/12/14

Ports

tcp/25

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
```

```
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

------------------------------ snip --------- [...]
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2013/10/18

Ports

tcp/25

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

http://tools.ietf.org/html/rfc3749

http://tools.ietf.org/html/rfc3943

http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/10/18

Ports

tcp/25

```
Nessus was able to confirm that the following compression methods are
supported by the target :
```

```
NULL (0x00)
DEFLATE (0x01)
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2012/04/02

Ports

tcp/25

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75
```

45410 - SSL Certificate commonName Mismatch

Synopsis

The SSL certificate commonName does not match the host name.

Description

This service presents an SSL certificate for which the 'commonName' (CN) does not match the host name on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS host name that matches the common name in the certificate.

Risk Factor

None

Plugin Information:

Publication date: 2010/04/03, Modification date: 2012/09/30

Ports

tcp/25

```
The host name known by Nessus is :

  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2013/10/18

Ports

tcp/25

```
Here is the list of SSL ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

    SSLv2
      EXP-RC2-CBC-MD5             Kx=RSA(512)     Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
      EXP-RC4-MD5                 Kx=RSA(512)     Au=RSA      Enc=RC4(40)              Mac=MD5
export

    SSLv3
      EXP-ADH-DES-CBC-SHA         Kx=DH(512)      Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5             Kx=DH(512)      Au=None     Enc=RC4(40)              Mac=MD5
export
```

```
     EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2(40)              Mac=MD5
export
     EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

   TLSv1
     EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
     EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
     EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

 Medium Strength Ciphers (>= 56-bit and < 112-bit key)

   SSLv2
     DES-CBC-MD5                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=MD5

   SSLv3
     ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
     EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA
[...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/25

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)

   SSLv2
     EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export

   SSLv3
```

```
     EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export

   TLSv1
     EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export
     EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export

 Medium Strength Ciphers (>= 56-bit and < 112-bit key)

   SSLv2
     DES-CBC-MD5                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=MD5

   SSLv3
     ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
     EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
     DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

   TLSv1
     EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
     ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
     DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

 High Strength Ciphers (>= 112-bit key)

   SSLv2
     DES-CBC3-MD5                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=MD5
     RC2-CBC-MD5                  Kx=RSA         Au=RSA      Enc=RC2-CBC(128)         Mac=M
[...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/25

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (< 56-bit key)
```

```
    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
export

  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES(168)            Mac=SHA1

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports

tcp/25

```
  This port supports resuming TLSv1 / SSLv3 sessions.
```

58768 - SSL Resume With Different Cipher Issue

Synopsis

The remote host allows resuming SSL sessions with a different cipher than the one originally negotiated.

Description

The SSL implementation on the remote host has been shown to allow a cipher other than the one originally negotiated when resuming a session. An attacker that sees (e.g. by sniffing) the start of an SSL connection may be able to manipulate session cache to cause subsequent resumptions of that session to use a cipher chosen by the attacker.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/04/17, Modification date: 2012/04/17

Ports

tcp/25

```
The server allowed the following session over SSLv3 to be resumed as follows :

  Session ID     : 0a244bab6b262b4cb247056e1af0db2fe8e86cb5ca109eacafe8073b88b69d64
  Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Resumed Cipher : SSL3_CK_ADH_DES_64_CBC_SHA (0x001a)

The server allowed the following session over TLSv1 to be resumed as follows :

  Session ID     : d1044044db45208db6f850e820ef4dcf79a11a5ab71a0a05f930078a2676919d
  Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Resumed Cipher : TLS1_CK_DH_anon_EXPORT_WITH_RC4_40_MD5 (0x0017)
```

53/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/53

```
Port 53/tcp was found to be open
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

http://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information:

Publication date: 2003/02/13, Modification date: 2013/05/07

Ports

tcp/53

53/udp

33447 - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Synopsis

The remote name resolver (or the server it uses upstream) may be vulnerable to DNS cache poisoning.

Description

The remote DNS resolver does not use random ports when making queries to third party DNS servers.
This problem might be exploited by an attacker to poison the remote DNS server more easily, and therefore divert legitimate traffic to arbitrary sites.

Solution

Contact your DNS server vendor for a patch

Risk Factor

High

CVSS Base Score

9.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:C)

STIG Severity

I

References

BID	30131
CVE	CVE-2008-1447
XREF	OSVDB:46776
XREF	OSVDB:46777
XREF	OSVDB:46786
XREF	OSVDB:46837
XREF	OSVDB:47510
XREF	OSVDB:48186
XREF	CERT:800113
XREF	IAVA:2008-A-0045

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2008/07/09, Modification date: 2012/12/10

Ports

udp/53

```
The remote DNS server uses non-random ports for its
DNS requests. An attacker may spoof DNS responses.

List of used ports:

+ DNS Server: 79.148.101.25
|- Port: 42335
|- Port: 42335
|- Port: 42335
|- Port: 42335
```

12217 - DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.
This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.
For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.
Note: If this is an internal DNS server not accessable to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See Also

http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

Solution

Contact the vendor of the DNS software for a fix.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2004/04/27, Modification date: 2013/01/25

Ports

udp/53

```
Nessus sent a non-recursive query for example.com
and received 1 answer :

93.184.216.119
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

http://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information:

Publication date: 2003/02/13, Modification date: 2013/05/07

Ports

udp/53

10028 - DNS Server BIND version Directive Remote Version Disclosure

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf

Risk Factor

None

References

XREF OSVDB:23

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/05/24

Ports

udp/53

```
The version of the remote DNS server is :

9.4.2
```

35371 - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information:

Publication date: 2009/01/15, Modification date: 2011/09/14

Ports

udp/53

```
The remote host name is :

metasploitable
```

80/tcp

55976 - Apache HTTP Server Byte Range DoS

Synopsis

The web server running on the remote host is affected by a denial of service vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive. Exploit code is publicly available and attacks have reportedly been observed in the wild.

See Also

http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html

http://www.gossamer-threads.com/lists/apache/dev/401638

http://www.nessus.org/u?404627ec

http://httpd.apache.org/security/CVE-2011-3192.txt

http://www.nessus.org/u?1538124a

http://www-01.ibm.com/support/docview.wss?uid=swg24030863

Solution

Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192.
Version 2.2.20 fixed the issue, but also introduced a regression.
If the host is running a web server based on Apache httpd, contact the vendor for a fix.

Risk Factor

High

CVSS Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

References

BID	49303
CVE	CVE-2011-3192
XREF	OSVDB:74721
XREF	CERT:405811
XREF	EDB-ID:17696
XREF	EDB-ID:18221

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2011/08/25, Modification date: 2013/11/27

Ports

tcp/80

```
Nessus determined the server is unpatched and is not using any
of the suggested workarounds by making the following requests :

-------------------- Testing for workarounds --------------------
HEAD /twiki/TWikiHistory.html HTTP/1.1
Host: 192.168.2.105
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

HTTP/1.1 206 Partial Content
Date: Thu, 16 Jan 2014 06:07:11 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Last-Modified: Sun, 02 Feb 2003 02:45:15 GMT
ETag: "12ae7-ccc1-3b5a70731c4c0"
Accept-Ranges: bytes
Content-Length: 857
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=4f0103c7fbec7771a
-------------------- Testing for workarounds --------------------

-------------------- Testing for patch --------------------
```

```
HEAD /twiki/TWikiHistory.html HTTP/1.1
Host: 192.168.2.105
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=0-,1-
Range: bytes=0-,1-
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

HTTP/1.1 206 Partial Content
Date: Thu, 16 Jan 2014 06:07:17 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Last-Modified: Sun, 02 Feb 2003 02:45:15 GMT
ETag: "12ae7-ccc1-3b5a70731c4c0"
Accept-Ranges: bytes
Content-Length: 105027
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=4f0103ccc4d6b43b
-------------------- Testing for patch --------------------
```

11229 - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :
- The username of the user who installed PHP and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2003/02/12, Modification date: 2013/10/23

Ports

tcp/80

```
Nessus discovered the following URL that calls phpinfo() :

  - http://192.168.2.105/phpinfo.php
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.9 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2003/01/23, Modification date: 2013/03/29

Ports

tcp/80

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
```

```
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus124203146.html HTTP/1.1
Connection: Close
Host: 192.168.2.105
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Thu, 16 Jan 2014 05:58:02 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus124203146.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.2.105
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis

The web server running on the remote host has an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host has an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://httpd.apache.org/security/vulnerabilities_22.html

http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution

Upgrade to Apache version 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	51706

CVE	CVE-2012-0053
XREF	OSVDB:78556
XREF	EDB-ID:18442

Plugin Information:

Publication date: 2012/02/02, Modification date: 2013/10/01

Ports

tcp/80

```
Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: 192.168.2.105
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Size of a request header field exceeds server limit.<br />
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

26194 - Web Server Uses Plain Text Authentication Forms

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724

Plugin Information:

Publication date: 2007/09/28, Modification date: 2011/09/15

Ports

tcp/80

```
Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination Page: /twiki/bin/passwd/TWiki/WebHome

Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination Page: /twiki/bin/passwd/Main/WebHome

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination Page: /twiki/bin/passwd/TWiki/WebHome

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination Page: /twiki/bin/passwd/Main/WebHome
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/12/13

Ports

tcp/80

```
A web server is running on this port.
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2013/04/02

Ports

tcp/80

```
The following directories were discovered:
/cgi-bin, /icons, /twiki/bin

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10662 - Web mirroring

Synopsis

Nessus crawled the remote web site.

Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2013/04/11

Ports

tcp/80

```
Webmirror performed 212 queries in 1204s (0.176 queries per second)

The following CGI have been discovered:


+ CGI: /twiki/bin/view/Main/WebHome
  Methods: GET
  Argument: rev
   Value: 1.20
   Value: 1.19
   Value: 1.18
   Value: r1.20
   Value: r1.19
   Value: r1.18
   Value: r1.17
   Value: r1.16
   Value: r1.15
   Value: r1.14
   Value: r1.13
   Value: r1.12
   Value: r1.11
   Value: r1.10
   Value: r1.9
   Value: r1.8
   Value: r1.7
```

```
    Value: r1.6
    Value: r1.5
    Value: r1.4
    Value: r1.3
    Value: r1.2
    Value: r1.1
  Argument: skin
    Value: print
  Argument: topic
  Argument: unlock
    Value: on


+ CGI: /twiki/bin/search/Main/SearchResult
  Methods: GET
  Argument: nosearch
    Value: on
  Argument: order
    Value: modified
  Argument: regex
    Value: on
  Argument: reverse
    Value: on
  Argument: scope
    Value: text
    Value: topic
  Argument: search
    Value: Web%20*Home%5B%5EA-Za-z%5D
    Value: TWiki%20*Groups%5B%5EA-Za-z%5D
    Value: Office%20*Locations%5B%5EA-Za-z%5D
    Value: TWiki%20*Users%5B%5EA-Za-z%5D
    Value: %5C.*
    Value: Web%20*Changes%5B%5EA-Za-z%5D
    Value: Web%20*Index%5B%5EA-Za-z%5D
    Value: Web%20*Search%5B%5EA-Za-z%5D
    Value: Web%20*Preferences%5B%5EA-Za-z%5D
    Value: Web%20*Topic%20*List%5B%5EA-Za-z%5D
    Value: Web%20*Notify%5B%5EA-Za-z%5D
    Value: Web%20*Statistics%5B%5EA-Za-z%5D
    Value: Peter%20*Thoeny%5B%5EA-Za-z%5D
    Value: TWiki%20*Variables%5B%5EA-Za-z%5D
    Value: Charleythe%20*Horse%5B%5EA-Za-z%5D
    Value: TWiki%20*Admin%20*Group%5B%5EA-Za-z%5D
    Value: John%20*Talintyre%5B%5EA-Za-z%5D
    Value: San%20*Jose%20*Office%5B%5EA-Za-z%5D
    Value: London%20*Office%5B%5EA-Za-z%5D
    Value: Tokyo%20*Office%5B%5EA-Za-z%5D
    Value: Nicholas%20*Lee%5B%5EA-Za-z%5D
    Value: TWiki%20*Guest%5B%5EA-Za-z%5D
    Value: Web%20*Rss%5B%5EA-Za-z%5D
    Value: Nobody%20*Group%5B%5EA-Za-z%5D
    Value: Kevin%20*Kinnell%5B%5EA-Za-z%5D
    Value: Mike%20*Mannix%5B%5EA-Za-z%5D
    Value: Andrea%20*Sterbini%5B%5EA-Za-z%5D
    Value: Richard%20*Donkin%5B%5EA-Za-z%5D
    Value: Grant%20*Bo [...]
```

49705 - Web Server Harvested Email Addresses

Synopsis

email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2012/08/14

Ports

tcp/80

```
The following email addresses have been gathered :


- 'webmaster@your.company', referenced from :
   /twiki/bin/attach/Sandbox
   /twiki/bin/search/TWiki/SearchResult
   /twiki/bin/view/TWiki/TWikiShorthand
   /twiki/bin/view/TWiki/InstalledPlugins
   /twiki/bin/rdiff/TWiki/WebHome
   /twiki/bin/attach/Sandbox/WebHome
   /twiki/bin/rdiff/Main/WebRss
   /twiki/bin/view/TWiki/TWikiSystemRequirements
   /twiki/bin/view/Sandbox/WebHome
   /twiki/bin/rdiff/Main/CharleytheHorse
   /twiki/bin/view/Sandbox/WebChanges
   /twiki/bin/view/Main/WebNotify
   /twiki/bin/view/Main/TokyoOffice
   /twiki/bin/view/Main/TWikiAdminGroup
   /twiki/bin/view/Main/KevinKinnell
   /twiki/bin/view/Sandbox/WebIndex
   /twiki/bin/view/TWiki/WebNotify
   /twiki/bin/edit/Know/WebHome
   /twiki/bin/view/TWiki/FileAttachment
   /twiki/bin/view/TWiki/ManagingTopics
   /twiki/bin/edit/TWiki
   /twiki/bin/rdiff/Main/WebPreferences
   /twiki/bin/search/Sandbox/SearchResult
   /twiki/bin/attach/Main/OfficeLocations
   /twiki/bin/view/TWiki/TWikiFuncModule
   /twiki/bin/view/TWiki/TWikiMetaData
   /twiki/bin/view/TWiki/TWikiTopics
   /twiki/bin/view/TWiki/WikiCulture
   /twiki/bin/view/TWiki/InstantEnhancements
   /twiki/bin/view/TWiki/TWikiUpgradeGuide
   /twiki/bin/attach
   /twiki/bin/view/TWiki/TWikiSiteTools
   /twiki/bin/attach/TWiki/WebHome
   /twiki/bin/rdiff/Main/GrantBow
   /twiki/bin/view/TWiki/TWikiHistory
   /twiki/bin/view/Main/
   /twiki/bin/view/Main/WebHome
   /twiki/bin/rdiff/Main/JohnTalintyre
   /twiki/bin/view/Main
   /twiki/bin/view/Sandbox/WebPreferences
   /twiki/bin/view/TWiki/WebPreferences
   /twiki/bin/attach/Know
   /twiki/bin/rdiff/Main
   /twiki/bin/view/TWiki/TWikiDocumentation
   /twiki/bin/view/Know/WebHome
   /twiki/bin/edit/Sandbox/TestTopic7
   /twiki/bin/view/TWiki/TextFormattingRules
   /twiki/bin/rdiff/Main/WebStatistics
   /twiki/bin/view/TWiki/StartingPoints
   /twiki/bin/view/TWiki/TWikiTutorial
   /twiki/bin/view/TWiki/AppendixFileSystem
   /twiki/bin/view/TWiki/TWikiAdminCookBook
   /twiki/bin/view/Main/ [...]
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/80

```
381 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://TWiki.SourceForge.net/           - /twiki/bin/rdiff/Main/WebHome
http://TWiki.org/                       - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/attach/TWiki/FileAttachment?filename=Sample.txt&revInfo=1 - /twiki/
TWikiDocumentation.html
http://TWiki.org/cgi-bin/attach/TWiki/FileAttachment?filename=Smile.gif&revInfo=1 - /twiki/
TWikiDocumentation.html
http://TWiki.org/cgi-bin/edit/Main/MartinRaabe?topicparent=TWiki.TWikiDocumentation - /twiki/
TWikiDocumentation.html
http://TWiki.org/cgi-bin/edit/TWiki/NewTopic?topicparent=TWiki.TWikiDocumentation - /twiki/
TWikiDocumentation.html
http://TWiki.org/cgi-bin/edit/TWiki/NotExistingYet?topicparent=TWiki.TWikiDocumentation - /twiki/
TWikiDocumentation.html
http://TWiki.org/cgi-bin/rename/TWiki/FileAttachment?attachment=Sample.txt - /twiki/
TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/IncorrectDllVersionW32PTH10DLL - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/NoDisclosure - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/OperatingSystem - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/OsHPUX - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/OsLinux - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/OsSolaris - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/OsVersion - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/OsWin - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/PublicFAQ - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/PublicSupported - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/ReadmeFirst - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/TopicClassification - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Know/WinDoze95Crash - /twiki/TWikiDocumentation.html
http://TWiki.org/cgi-bin/view/Main/GrantBow  [...]
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2011/09/28

Ports

tcp/80

```
Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination Page: /twiki/bin/passwd/TWiki/WebHome

Page : /twiki/bin/view/TWiki/TWikiDocumentation
Destination Page: /twiki/bin/passwd/Main/WebHome

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
```

```
Destination Page: /twiki/bin/passwd/TWiki/WebHome

Page : /twiki/bin/view/TWiki/TWikiUserAuthentication
Destination Page: /twiki/bin/passwd/Main/WebHome
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2013/12/03

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /changes
    /icons
    /oops
    /oops/TWiki
    /rdiff
    /rdiff/TWiki
    /search
    /search/Main
    /twiki
```

```
/twiki/changes
/twiki/pub
/twiki/pub/TWiki
/twiki/pub/TWiki/FileAttachment
/twiki/pub/TWiki/TWikiPreferences
/twiki/search
/twiki/search/Know
/twiki/search/Main
/twiki/view
/twiki/view/Main
/view
/view/Main
/view/TWiki
```

48243 - PHP Version

Synopsis

It is possible to obtain the version number of the remote PHP install.

Description

This plugin attempts to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2013/10/23

Ports

tcp/80

```
Nessus was able to identify the following PHP version information :

  Version : 5.2.4-2ubuntu5.10
  Source  : Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
  Source  : http://192.168.2.105/phpinfo.php
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/80

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 16 Jan 2014 05:59:57 GMT
  Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
```

```
Last-Modified: Wed, 17 Mar 2010 14:08:25 GMT
ETag: "107f7-2d-481ffa5ca8840"
Accept-Ranges: bytes
Content-Length: 45
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

See Also

http://projects.webappsec.org/Directory-Indexing

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. And use access restrictions or disable directory indexing for any that do.

Risk Factor

None

Plugin Information:

Publication date: 2009/09/15, Modification date: 2013/03/21

Ports

tcp/80

```
The following directories are browsable :

http://192.168.2.105/twiki/bin/view/TWiki/TWikiInstallationGuide
http://192.168.2.105/twiki/bin/view/TWiki/TWikiDocumentation
http://192.168.2.105/twiki/TWikiDocumentation.html
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

http://www.nessus.org/u?d636c8c7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/10/02

Ports

tcp/80

```
Give Nessus credentials to perform local checks.
```

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2013/01/16

Ports

udp/137

```
The following 7 NetBIOS names have been gathered :

 METASPLOITABLE   = Computer name
 METASPLOITABLE   = Messenger Service
 METASPLOITABLE   = File Server Service
 __MSBROWSE__     = Master Browser
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Master Browser
 WORKGROUP        = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

139/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2012/01/31

Ports

tcp/139

```
An SMB server is running on this port.
```

445/tcp

25216 - Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

Synopsis

It is possible to execute code on the remote host through Samba.

Description

The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

See Also

http://www.samba.org/samba/security/CVE-2007-2446.html

Solution

Upgrade to Samba version 3.0.25 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

BID	23973
BID	24195
BID	24196
BID	24197
BID	24198
CVE	CVE-2007-2446
XREF	OSVDB:34699
XREF	OSVDB:34731
XREF	OSVDB:34732
XREF	OSVDB:34733

Exploitable with

CANVAS (true)Metasploit (true)

Plugin Information:

Publication date: 2007/05/15, Modification date: 2013/02/01

Ports

tcp/445

42411 - Microsoft Windows SMB Shares Unprivileged Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	8026
CVE	CVE-1999-0519

CVE	CVE-1999-0520
XREF	OSVDB:299

Plugin Information:

Publication date: 2009/11/06, Modification date: 2011/03/27

Ports

tcp/445

```
The following shares can be accessed using a NULL session  :

- tmp  - (readable,writable)
  + Content of this share :
..
8610.jsvc_up
5443.jsvc_up
.ICE-unix
.X11-unix
```

57608 - SMB Signing Disabled

Synopsis

Signing is disabled on the remote SMB server.

Description

Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

See Also

http://support.microsoft.com/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information:

Publication date: 2012/01/19, Modification date: 2013/10/24

Ports

tcp/445

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2012/01/31

Ports

tcp/445

```
A CIFS server is running on this port.
```

25240 - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

http://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2013/01/07

Ports

tcp/445

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It is possible to obtain information about the remote operating system.

Description

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2013/06/25

Ports

tcp/445

```
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It is possible to log into the remote host.

Description

The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :
- NULL session
- Guest account
- Given Credentials

See Also

http://support.microsoft.com/kb/143474

http://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2000/05/09, Modification date: 2013/04/23

Ports

tcp/445

```
- NULL sessions are enabled on the remote host
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).
The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information:

Publication date: 2002/02/13, Modification date: 2012/08/10

Ports

tcp/445

```
The remote host SID value is :

1-5-21-1042354039-2475377354-766472396

The value of 'RestrictAnonymous' setting is : unknown
```

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

It is possible to enumerate local users.

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/02/13, Modification date: 2012/08/10

Ports

tcp/445

```
  - Administrator (id 500, Administrator account)
  - nobody (id 501, Guest account)
  - root (id 1000)
  - root (id 1001)
  - daemon (id 1002)
  - daemon (id 1003)
  - bin (id 1004)
  - bin (id 1005)
  - sys (id 1006)
  - sys (id 1007)
  - sync (id 1008)
  - adm (id 1009)
  - games (id 1010)
  - tty (id 1011)
  - man (id 1012)
  - disk (id 1013)
  - lp (id 1014)
  - lp (id 1015)
  - mail (id 1016)
  - mail (id 1017)
  - news (id 1018)
  - news (id 1019)
  - uucp (id 1020)
  - uucp (id 1021)
  - man (id 1025)
  - proxy (id 1026)
  - proxy (id 1027)
  - kmem (id 1031)
  - dialout (id 1041)
  - fax (id 1043)
  - voice (id 1045)
  - cdrom (id 1049)
  - floppy (id 1051)
  - tape (id 1053)
  - sudo (id 1055)
  - audio (id 1059)
  - dip (id 1061)
  - www-data (id 1066)
  - www-data (id 1067)
  - backup (id 1068)
  - backup (id 1069)
  - operator (id 1075)
  - list (id 1076)
  - list (id 1077)
  - irc (id 1078)
  - irc (id 1079)
  - src (id 1081)
  - gnats (id 1082)
  - gnats (id 1083)
  - shadow (id 1085)
  - utmp (id 1087)
  - video (id 1089)
  - sasl (id 1091)
  - plugdev (id 1093)
  - staff (id 1101)
  - games (id 1121)
  - libuuid (id 1200)

Note that, in addition to the Administrator and Guest accounts, Nessus
has enumerated only those local users with IDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2012/11/29

Ports

tcp/445

```
Here are the SMB shares available on the remote host when logged as a NULL session:

  - print$
  - tmp
  - opt
  - IPC$
  - ADMIN$
```

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It is possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

http://technet.microsoft.com/en-us/library/bb456988.aspx

http://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/07/25, Modification date: 2012/07/25

Ports

tcp/445

```
Share path : \\METASPLOITABLE\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers

Share path : \\METASPLOITABLE\tmp
Local path : C:\tmp
Comment : oh noes!

Share path : \\METASPLOITABLE\opt
Local path : C:\tmp

Share path : \\METASPLOITABLE\IPC$
Local path : C:\tmp
Comment : IPC Service (metasploitable server (Samba 3.0.20-Debian))

Share path : \\METASPLOITABLE\ADMIN$
Local path : C:\tmp
Comment : IPC Service (metasploitable server (Samba 3.0.20-Debian))
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2011/03/04

Ports

tcp/445

```
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF OSVDB:300

Plugin Information:

Publication date: 2000/05/09, Modification date: 2011/09/14

Ports

tcp/445

```
Here is the browse list of the remote host :

METASPLOITABLE ( os : 0.0 )
```

3306/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/3306

```
Port 3306/tcp was found to be open
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'
request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/18, Modification date: 2013/09/18

Ports

tcp/3306

```
A MySQL server is running on this port.
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/13, Modification date: 2013/01/07

Ports

tcp/3306

```
Version  : 5.0.51a-3ubuntu5
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

3632/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/3632

```
Port 3632/tcp was found to be open
```

5432/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/5432

```
Port 5432/tcp was found to be open
```

26024 - PostgreSQL Server Detection

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

http://www.postgresql.org/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Publication date: 2007/09/14, Modification date: 2013/02/14

Ports

tcp/5432

8009/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/8009

```
Port 8009/tcp was found to be open
```

8180/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2013/10/15

Ports

tcp/8180

```
Port 8180/tcp was found to be open
```

E

Pliego de condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de una *Informática Forense: auditoría de seguridad*. En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales.

1.– La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el proyecto a concurso se reserva el derecho a declararlo desierto.

2.– El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3.– En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4.– La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5.– Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6.– El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7.– Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8.– Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9.– Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento

a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10.– Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11.– Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12.– Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13.– El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14.– Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15.– La garantía definitiva será del 4 % del presupuesto y la provisional del 2 %.

16.– La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17.– La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18.– Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19.– El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20.– Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma, por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21.– El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22.– Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la

Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23.– Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad "Presupuesto de Ejecución de Contratаz anteriormente llamado "Presupuesto de Ejecución Material"que hoy designa otro concepto.

Condiciones particulares.

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1.– La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2.– La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3.– Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4.– En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones así como su cantidad.

5.– En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6.– Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7.– Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8.– Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9.– Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10.– La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11.– La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12.– El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.

F

Presupuesto

En el presente documento se expone el presupuesto para la realización del proyecto completo. Este documento corresponde con el presupuesto que se debe entregar al cliente.

F.1. Descripción del servicio

EL servicio presupuestado corresponde al diseño e implementación de una red empresarial y auditoría de seguridad de dicha red con el fin de cumplir la normativa del estado.

Tareas a realizar:

Diseño e implementación de la red: el proceso del diseño e implementación de la red se ha separado en tres tareas diferentes:

- **Diseño de la red:** diseño de los diferentes servicios y configuraciones de la red. Tarea realizada por un *Senior* para asegurar que no se producen errores en el diseño.
- **Instalación de los servicios:** instalación de los diferentes servidores. Tarea realizada por un *Técnico* debido a que es una persona cualificada para las instalaciones físicas.
- **Configuración de los servicios:** configuración de todos los servidores tanto en los servicios como en el funcionamiento final. Tarea realizada por un *Técnico* debido a que es una persona cualificada para las instalaciones físicas.

Auditoría de seguridad: la auditoría de seguridad, se ha separado en cuatro procesos diferentes:

- **Revisión de la normativa:** revisión del cumplimiento de la normativa aplicable a los organismos oficiales del estado. Tarea realizada por un *Junior* debido a que es necesario tener conocimientos de seguridad pero no es una tarea crítica.
- **Seguridad física:** revisión de la seguridad física de la empresa. Tarea realizada por un *Senior* debido a que es necesario tener un acceso total a la empresa donde puede encontrar información confidencial.
- **Seguridad de usuario:** revisión de la seguridad relativa a los diferentes usuarios de la red. Tarea realizada por un *Senior* debido a que es necesario tener un acceso total a la empresa donde puede encontrar información confidencial y debe de tratar con el departamento de RRHH (Recursos Humanos).
- **Test de penetración:** realización de un test de penetración a toda la red empresarial. Tarea realizada por un *Senior* debido a que es necesario contar con amplios conocimientos de seguridad.

La dirección del proyecto será realizada por un *Senior nivel 3* con amplia experiencia de al menos 5 años en proyectos similares, con una dedicación de un 30 % de la duración del proyecto, que suponen un total de 57,6 horas ,con un coste de 75 €/hora.

Para la realización de todo el proyecto se utilizara software libre, sin coste alguno en licencias.

F.2. Valoración económica

Diseño e implantación de la red				
Concepto	**Empleado**	**Precio/hora**	**Horas**	**Coste**
Diseño de la red	Senior	70,83 €	24	1.700 €
Instalación de los servicios	Técnico	37,50 €	40	1.500 €
Configuración de los servidores	Técnico	37,50 €	40	1.500 €
			Total implantación	4.700 €

Tabla F.1: Tabla de presupuesto de diseño e implantación de la red.

Auditoría de seguridad				
Concepto	**Empleado**	**Precio/hora**	**Horas**	**Coste**
Revisión de normativa	Junior	41,67 €	24	1.000 €
Seguridad física	Senior	70,83 €	8	567 €
Seguridad de usuario	Senior	70,83 €	16	1.133 €
Test de penetración	Senior	70,83 €	24	3.000 €
			Total auditoría de seuridad	5.700 €

Tabla F.2: Tabla de presupuesto de auditoría de seguridad.

Presupuesto total	
Concepto	**Coste**
Total implantación	4.700 €
Total auditoría	5.700 €
Dirección proyecto	4.320 €
Total	**14.720 €**

Tabla F.3: Tabla de presupuesto total.

- Los precios no incluyen *IVA* o impuestos equivalentes.

Lugar de trabajo: En las instalaciones del cliente.

Duración del servicio: 2 meses.

Forma de pago: 60 días.

Madrid, Febrero de 2014

El Ingeniero Jefe de Proyecto

Fdo: Jose Manuel Agrelo de la Torre

Ingeniero Superior de Telecomunicaciones