UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

“EVALUACIÓN DE SEGURIDAD INFORMÁTICA EN PYME’S”

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

OCTAVIO DOMÍNGUEZ SALGADO

DIRECTORA DE TESIS: M.C. MA. JAQUELINA LÓPEZ BARRIENTOS

Ciudad Universitaria, México 2014

AGRADECIMIENTOS

A mis padres Héctor y Sofía

Que siempre estuvieron ahí para apoyarme y darme sus ánimos, para darme la oportunidad de prepararme para ser mejor persona y que pueda enfrentar los retos que vienen

A mis amigos

Que siempre estuvieron en los momentos difíciles y no dejaron que me rindiera, siempre dándome la mano

A mi novia

Que siempre me ayudó cuando más lo necesitaba, que me daba fuerzas para seguir y no quedarme atrás, me daba el cariño para continuar un poco más.

A la Universidad Nacional Autónoma de México

Por ser quien me dio todo el conocimiento y ser mi segunda casa

A la Dirección General de Cómputo y de tecnologías de información y comunicación

Por darme la oportunidad de especializarme en el área de la computación a la que me quiero dedicar toda la vida

A la M.C. Ma. Jaquelina López Barrientos

Por ser mi directora de tesis y mi mentora, que me dio muchos consejos para la realización de este trabajo.

Al Ing. Gabriel Peral

Por ser mi asesor de tesis y mi maestro, sin el cual no hubiera tenido el ánimo de hacer este trabajo

Octavio Domínguez Salgado

ÍNDICES

Índice de contenido

Índice de figuras

Índice de tablas

Introducción

Las fallas de seguridad en un sistema informático pueden resultar en un acceso no autorizado de recursos, infección por malware, robo de datos o daños de la infraestructura de tecnología, así como de los activos más importantes en una organización. Una de las principales preocupaciones en materia de seguridad es la explotación de vulnerabilidades según lo indica el reporte de seguridad de ESET (compañía que desarrolla antivirus) para Latinoamérica 2013. Las violaciones de seguridad son el resultado de agentes externos o internos a las organizaciones, que tienen acceso a información importante y confidencial para la empresa, lo que puede provocar problemas legales o económicos a la organización, esto demuestra la importancia que tiene el proteger los recursos y sistemas de las empresas.

En años anteriores sólo las grandes organizaciones y compañías se preocupaban por los riesgos de seguridad en sus sistemas informáticos, sin embargo ahora se vienen dando con más frecuencia los ataques a las pequeñas y medianas empresas, lo que causa serios daños a la continuidad de negocio, afectación en las relaciones comerciales, pérdida de clientes, de credibilidad, y oportunidades de negocio, principalmente.

Es necesario que las PyME's refuercen su seguridad informática por medio de auditorías a sus sistemas informáticos, pruebas de penetración, herramientas de software y buenas prácticas, sin embargo un problema que puede presentarse al recurrir a estas soluciones son los altos costos que presentan.

La importancia de realizar una auditoría, pruebas de penetración o ambas en los sistemas informáticos de una organización, es que permite obtener un diagnóstico y recomendaciones para mitigar las vulnerabilidades que estén presentes y que puedan afectar a los activos de información más relevantes de la empresa. Dado que los costos son elevados, se puede recurrir a una alternativa más económica, la cual es que la empresa evalúe con herramientas de software gratuitas algunos puntos estratégicos donde comúnmente existen vulnerabilidades. Según el estado de los puntos evaluados, del diagnóstico previo y del resultado, se puede optar por una auditoría o por pruebas de penetración en tanto la empresa pueda disponer de los recursos para contratar algún servicio de esta naturaleza y lo requiera.

La evaluación de seguridad que auto-realice la organización debe estar sustentada por guías técnicas de acceso público como la del National Institute Standards and Technology 800-115 (NIST 800-115) o Penetration Testing Execution Standard (PTES), las cuales son una buena base para saber lo que conlleva el procedimiento de pruebas de penetración, además de que dan a conocer ciertas herramientas para cada fase.

Así, el **objetivo del presente trabajo de tesis** es proporcionar las herramientas y las pruebas que permitan identificar algunas vulnerabilidades comunes, malas configuraciones en dispositivos de red y análisis tráfico en la red de la organización, además de proponer una capa extra de seguridad, por medio de la gestión de la información o a través de un dispositivo que

englobe diversas soluciones de seguridad informática. Reflejando así un ahorro de costos para las PyME's.

Para alcanzar el objetivo planteado se decide construir un entorno virtualizado y controlado con el fin de simular una infraestructura de red de una pequeña o mediana empresa y realizar pruebas con la tranquilidad de saber que no se verá afectado ningún servicio como los que tienen los entornos reales.

El presente trabajo de tesis se desarrolla en el capítulo 1 los conceptos básicos para entender qué es la seguridad informática; en el capítulo 2 se dan a conocer algunas estadísticas de las preocupaciones en cuestión de seguridad que tienen las PyME's, además de presentar algunas causas que producen vulnerabilidades, en el capítulo 3 se define el concepto de una auditoría en sistemas informáticos y sus fases; mientras que en el capítulo 4 se describe la aplicación de las pruebas que permiten encontrar huecos de seguridad existentes en la infraestructura computacional de una organización, identificarlos y eliminarlos antes de que sean descubiertos; así, en el capítulo 5 se presentan buenas prácticas de seguridad informática, las etapas de un sistema de gestión de información, así como la implementación de una herramienta que engloba varias soluciones de seguridad en una sola, finalmente en las conclusiones se mencionan los logros obtenidos, los resultados y las buenas prácticas aprendidas.

Capítulo I
Conceptos básicos de Seguridad informática

1.1 Introducción

Hoy en día la tecnología se ha convertido en una necesidad que está presente en casi todos los aspectos de la vida cotidiana. Las computadoras son el centro de todos los negocios, que van desde los sistemas financieros de acciones hasta páginas web de pequeñas empresas para ofertar sus servicios. Las computadoras son responsables por mantener cosas tales como: cuentas de bancos, registros médicos, reportes bancarios e historiales de crédito. Claramente, todo individuo que posea una tarjeta de crédito y/o débito y usa un cajero electrónico debe estar preocupado por la integridad y privacidad de su información personal. Toda persona que use equipos de cómputo o similar debe conocer los conceptos básicos que engloba la seguridad entorno a dichos dispositivos.

1.2 Seguridad Informática y sus objetivos

La seguridad informática es un área de la informática que se enfoca en proteger a los activos concernientes a las tecnologías de la información, garantizando la triada de la seguridad como se menciona a continuación (véase figura 1.1):

a) Confidencialidad: Garantiza que sólo aquellas personas o procesos autorizados puedan acceder a la información.

b) Integridad: Se encarga de conservar la exactitud y totalidad de la información, esto es, que la información no sea modificada de alguna forma por usuarios o procesos no autorizados.

c) Disponibilidad: Garantiza que usuarios y procesos autorizados tengan acceso a la información cuando lo necesiten y cuantas veces se requiera.

Figura 1.1 Triada de la seguridad

1.3 Conceptos básicos

Para empezar a entender la seguridad informática hay que conocer primero los conceptos básicos que ayudarán a comprender esta gran área del cómputo, algunos conceptos se definen enseguida.

a) Activo: Cualquier objeto tangible, intangible o información que tenga valor para alguien o un grupo de personas.

b) Amenaza: Es todo aquello que pretende causar algún daño a algún activo, en forma de destrucción, modificación, robo o divulgación del activo.

c) Vulnerabilidad: Es un fallo o defecto de seguridad que puede causar daño a un activo.

d) Ataque: Es la culminación de una amenaza al explotar una o varias vulnerabilidades. Los ataques se pueden clasificar en:

- Por la forma en la que afecta a la información (Activos o Pasivos)
- Por su lugar de concurrencia (Internos o Externos)
- Por el servicio contra el cual atenta (Suplantación, Modificación, Interrupción e Intercepción)

e) **Impacto**: Es la medición de las consecuencias de la materialización de algún riesgo o de una amenaza.

f) Riesgo: La probabilidad o posibilidad de la pérdida o daño de algún activo.

1.4 Los bienes informáticos y su seguridad

Los bienes informáticos están presentes casi en cualquier parte de la vida de los seres humanos, por ejemplo: la computadora, el smartphone, las usb´s, los dvd´s o cd´s, el ipad, principalmente. Por lo tanto es necesario conocer diferentes conceptos que permitan identificar qué o quién puede causar daños a los bienes mencionados, esto aplica para una sola persona o para una organización.

1.4.1 Entorno a proteger

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware se entiende el conjunto formado por todos los elementos físicos de un sistema informático, tales como: CPU’s, terminales, cableado, medios de almacenamiento secundario (SSD, DVD, discos duros externos, memorias USB´s principalmente.), tarjetas de red, entre otros. Por software el conjunto de programas lógicos que hacen funcional al hardware, tales como: sistemas operativos, aplicaciones, programas, etc. Por

información entiéndase el conjunto de datos manejados por el software y el hardware, como por ejemplo: paquetes que circulan por un cable de red, una base de datos, archivos en general, etc.

Habitualmente la información constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar, sin embargo, al ser intangible la información, lo que se amenaza es a los recursos que la resguardan, procesan o transmiten (véase figura 1.2).

(Microsoft, 2014)

Figura 1.2 Tipos de bienes informáticos

1.4.2 Tipos de amenazas

A continuación se presentan los principales tipos de amenazas que podrían atentar contra los bienes informáticos de una organización o de algún usuario.

1.4.2.1 Humanas

La mayoría de los ataques a un sistema informático van a provenir en última instancia de personas que intencionada o descuidadamente, pueden causar pérdidas (véase figura 1.3).

(www.smedio.com, 2014)

Figura 1.3 Ataque de tipo humano

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para los sistemas informáticos, generalmente se dividen en dos grandes grupos: **(1) los atacantes pasivos**, aquellos que fisgonean por el sistema pero no lo modifican o destruyen datos, y **(2) los atacantes activos**, quienes dañan el objetivo atacado o lo modifican a su favor.

a) Personal: Las amenazas a la seguridad de un sistema proveniente del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados, lo que regularmente ocurre es que más que de ataques, se trate de accidentes causados por error o por desconocimiento de las normas básicas de seguridad. Un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los registros de un sistema.

b) Ex empleados: Generalmente, se trata de personas descontentas con la organización que pueden aprovechar las fallas de un sistema informático, ya que conocen perfectamente como dañarlo o tomar venganza por algún hecho que no consideran justo.

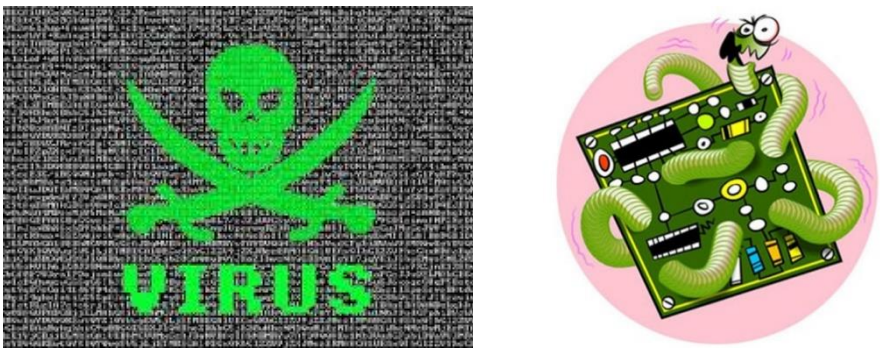
c) Hacker: es un intruso que se dedica a la tarea de entrar a los sistemas informáticos para demostrar que puede y sabe hacerlo, en forma de pasatiempo o reto técnico, también puede no pretender hacer algún daño, pero al introducirse a un sistema ajeno ya está violando la confidencialidad del sistema, por tanto se le considera delito en muchos países, ya que se podría revelar información sin autorización.

d) Intrusos remunerados*:* son expertos en cómputo contratados por terceros para la obtención de información confidencial o hacer ataques, por ejemplo: para causar daño o sabotajes a alguna organización.

e) Ociosos: son aquellas personas que no forman parte del personal de una organización, ni tampoco tienen intenciones de causar daño, simplemente descargan software de la red y lo ejecutan para ver qué pasa.

1.4.2.2 Lógicas

Las amenazas lógicas son un tipo de código malicioso es decir, se trata de cualquier tipo de programa que fue desarrollado para causar algún daño o poder introducirse sin autorización a algún sistema informático (véase figura 1.4).



(malwaridades.blogspot.mx, 2012)

Figura 1.4 Amenaza lógica

a) Virus: es una secuencia de código que se inserta en un programa y/o archivo ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

b) Troyanos: son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecuta funciones ocultas sin el conocimiento del usuario.

c) Gusanos: programas capaces de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando fallos de los sistemas a los que se conecta para dañarlos.

d) Spyware: son programas que se instalan en la computadora del usuario desde una página web los cuales pueden capturar o sustraer información almacenada en el equipo, así como contraseñas, nombres de usuario, y más.

e) Sniffer: es un programa (o una persona) que puede capturar los paquetes que viajan a través de la red, pero sin modificarlos, en otras palabras sólo “fisgonea” qué pasa a través de la red.

f) **Botnet:** hace referencia al termino bot que significa “robot”, se puede decir que es robot informático que se ejecutan de manera autónoma, tratándose de apoderar de las computadoras de forma remota, las cuales quedan en un estado zombi después que se introdujo el bot en la computadora, para que después el atacante la pueda usar como le plazca, por ejemplo: para realizar ataques de negación de servicio.

1.4.2.3 Físicas

Las amenazas físicas son más relacionadas al medio, donde se encuentran los activos informáticos, aquí algunas amenazas que podrían causar daño a los activos:

a) Desastres naturales

Son las amenazas menos probables en los entornos habituales, simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a sus sistemas informáticos en una gran ciudad, pero es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un hacker o una infección por malware.

b) Ocasionadas por el hombre

Este tipo de amenazas son más probables que ocurran y puedan causar daño a algún bien informático, pueden ser disturbios, sabotajes internos o externos en alguna organización, robo de un activo informático, principalmente.

1.5 Tipos de seguridad

Ahora ya se sabe qué males pueden aquejar a los bienes informáticos, entonces es tiempo de saber cómo se pueden proteger, esto puede aplicar tanto para una sola persona o para una organización, depende el caso.

1.5.1 Seguridad Física

Es la implementación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas que puedan afectar a los recursos y a la información (véase figura 1.5).

(telavip.com.ve, 2012)

Figura 1.5 Control de acceso

Se recomienda que se tenga un plan de seguridad física complementando las políticas de seguridad de una empresa u organización.

Los puntos importantes que debe abordar este tipo de plan se anuncian enseguida:

- Descripción de los activos físico a los cuales se les brinda la protección.

- Una descripción de la ubicación y zona de donde se encuentran los activos que se están protegiendo.

- Análisis de las posibles amenazas de las que hay que proteger a los activos.

- Descripción de las defensas de seguridad que se utilizan y como pueden mejorarse

- Calcular un costo estimado de las mejoras posibles, también calcular el costo del activo que se protege y la probabilidad de un ataque, accidente o desastre que pueda afectar al activo.

1.5.1.1 Acceso Físico

Para obtener una buena seguridad en el acceso físico se pueden seguir las siguientes recomendaciones:

- Todos los equipos deben estar posicionados en un lugar donde la seguridad sea equivalente al nivel crítico de estos.

- El acceso físico al hardware debe ser autorizado de acuerdo al nivel del personal de la empresa u organización.

- Es importante colocar mecanismos de prevención y detección.

- Algunos mecanismos de prevención pueden ser: el monitoreo, registro de entrada/salida, acciones realizadas en los equipos, etc.

- Algunos mecanismos de detección son: software para detección de intrusos, monitoreos con cámaras de vigilancia, personas en puestos de vigilancia, etc.

Se debe tomar muy en cuenta a las personas que contrata una organización principalmente cuando se trata de trabajos de alto impacto o riesgo. Por eso el **estándar ISO 27001** (véase figura 1.6) marca que:

(www.gopixpic.com, 2014)

Figura 1.6 ISO 27001

- Los candidatos deberán ser seleccionados adecuadamente, más si se trata de un puesto de sensitivo y de alta importancia

- Los empleados, contratistas u otra persona que maneje información de la empresa, deberá firmar un acuerdo de confidencialidad.

1.5.2 Seguridad Lógica

La seguridad lógica es un conjunto de aplicaciones que forma una barrera, además de procedimientos que protegen el acceso al activo, que son los datos y la información.

(www.thewindowsclub.com, 2014)

Figura 1.6 Seguridad lógica

A continuación se describen los elementos que conforman a la seguridad lógica.

a) Identificación y autenticación

Identificación: es un proceso por el cual una persona, usuario, o programa muestra quien es, en otras palabras muestra su identidad.

Autenticación: es un proceso para comprobar y verificar la identidad de una persona, usuario o programa por medio de información adicional.

Se basa en 3 factores:
- Algo que se sabe: regularmente contraseñas
- Algo que se tiene: en la mayoría de casos tarjetas magnéticas
- Algo que se es: típicamente la huella dactilar

b) Modalidad de acceso

Es un marco conceptual que dicta cómo los usuarios acceden a los datos, objetos o información. Existen 3 modelos de control de acceso, enseguida se describen brevemente cada uno de ellos.

- **Discrecional:** el usuario es dueño de la información o datos y él decide qué usuarios pueden tener acceso al recurso.

- **Mandatorio:** se basa en un sistema donde los recursos tienen una etiqueta de seguridad (Secreto, Ultra secreto, Confidencial, etc.)

- **No mandatorio (basada en roles):** se emplea una administración centralizada por el cual se determina cómo los usuarios y objetos interactúan entre sí. Los accesos se basan en el rol que tiene el sujeto en la empresa u organización.

c) Control de acceso interno:

Se utilizan generalmente para la autenticación de los usuarios y sirven para proteger la información y las aplicaciones dentro de una organización, los siguientes son ejemplos de controles de acceso internos:

- **Contraseñas:** se utilizan para realizar autenticación y sirven para proteger los datos y aplicación a las cuales se quiera tener acceso.

- **Lista de control de acceso:** es un registro donde se encuentra los nombres de los usuarios que obtuvieron permiso para acceder a algún recurso del sistema.

- **Cifrado:** es un procedimiento que utiliza un algoritmo para transformar un mensaje, de tal forma que sea incomprensible, y que solamente podrá ser comprensible por quienes posean la clave o llave apropiada para el proceso de descifrado.

d) Control de acceso externo:

Algunos elementos que sirven para el uso del control de acceso lógico son:

- **Firewall**

Es un dispositivo (software o hardware) que tiene un conjunto de reglas específicas, con las cuales determina que tráfico de red puede entrar o salir.

Existen 3 tipos de tecnologías de Firewall

-Filtrado de paquetes: el filtrado se realiza a cada paquete basándose solamente en la información contenida en el paquete.
-Filtrado por estado: permite abrir “puertas” a cierto tráfico basado en una conexión y volver a cerrarla cuando termina la conexión.
-Filtrado por aplicación: actúa sobre las 7 capas del modelo OSI y puede validar el contenido de la trama, además de soportar autenticación de usuario, lo malo es que este tipo de filtrado es muy lento y se necesita un hardware muy robusto.

- **Servidor Proxy**

Es un programa o dispositivo intermediario entre los equipos de cómputo o la red interna y la red externa (internet).

Los tipos de servidores Proxies son:

-**Proxy Cache:** permite acceder a una página web que está almacenada en cache, de esta manera el usuario visualiza en menor tiempo la página.

-**Proxy Transparente:** combina un servidor proxy con una NAT (traducción de direcciones de red) de manera que las conexiones son enrutadas dentro del proxy sin configuraciones por parte del cliente y sin que se percate de la existencia del proxy.

-**Proxy Inverso:** Es un servidor proxy instalado cerca de uno o más servidores web, donde todo el tráfico que entra de internet pasa primero por el proxy y después llega al servidor web.

-**Proxy Abierto:** Es un proxy que acepta peticiones desde cualquier computadora, generalmente es usado para hacer anónimo el tráfico, por lo cual muchos de estos proxies se usan para fines indebidos.

- **Integridad en el sistema**

Para ello se utilizan mecanismos que almacenan los *hashes* de los archivos de los sistemas que son monitoreados, con el fin de garantizar y verificar la integridad de dicho sistema, ante un presunto ataque por malware.

- **VPN (Virtual Private Networks)**

Es una estructura de red corporativa implantada sobre una red de carácter público, con la ventaja de que es como si el usuario trabajara en su misma red local, guardando la confidencial e integridad de los datos que viajan a través de este tipo de red.

- **Zona desmilitarizada (DMZ)**

DMZ o red perimetral, es una red local ubicada entre la red interna de una organización y la red externa, con el objetivo que la conexión de la DMZ se permita sólo hacia el exterior y las conexiones de red interna y red externa estén permitidas, de esta manera los equipos de la DMZ no puedan conectarse a las red interna.

Capítulo II
Vulnerabilidades y pruebas de penetración en Sistemas Informáticos

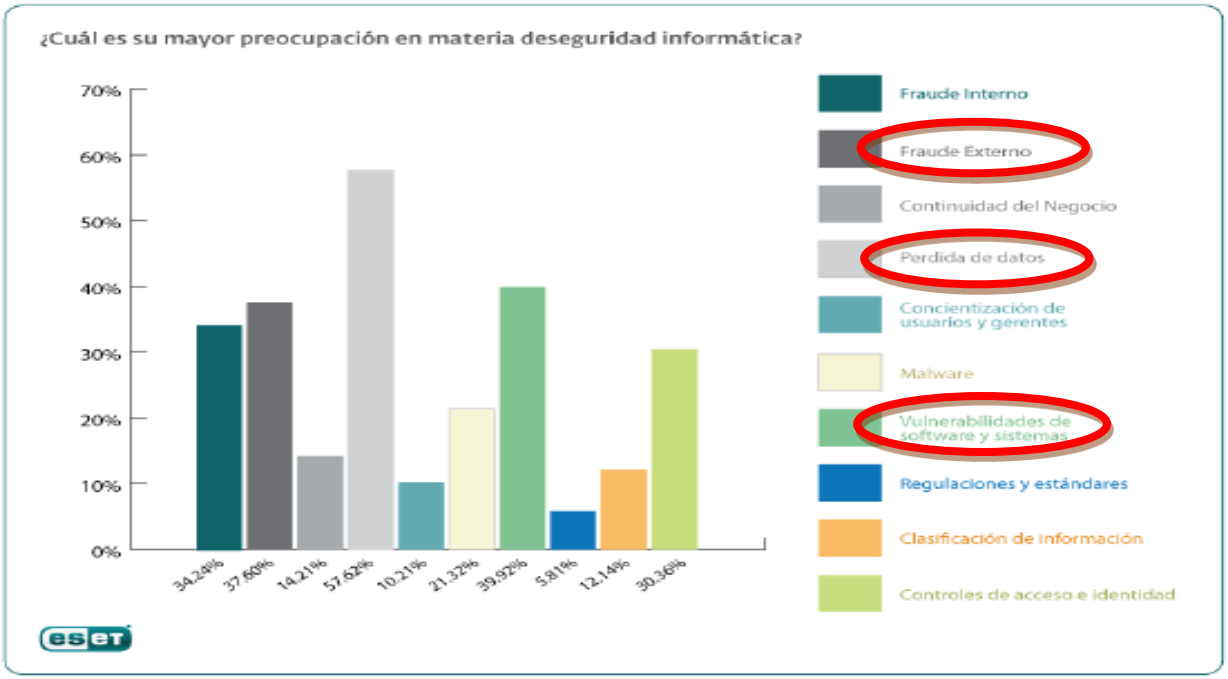
2.1 Introducción

Los sistemas informáticos y la infraestructura de las empresas por lo regular tienden a tener vulnerabilidades, y estas pueden ser explotadas por entes malintencionados, como lo indica el Security Report de ESET de Latinoamérica en el 2013, del cual solo se mencionan las estadísticas que competen a México. Como se puede observar el 17.30% de las empresas encuestadas en México, han sufrido la explotación de alguna vulnerabilidad, este número puede aumentar si se considera que hay empresas que aún no saben si personas malintencionadas están aprovechando alguna vulnerabilidad para entrar a sus sistemas, véase figura 2.1

(ESET_security_report_Latinoamérica, 2013)

Figura 2.1 Explotación de vulnerabilidades en empresas en México

En otra encuesta realizada por ESET pero del año 2010 en materia de seguridad informática se presentó la siguiente información (véase la figura 2.2):



(ESET_security_report, 2010)

Figura 2.2 Preocupaciones en materia de seguridad informática

Se puede observar que la pérdida de datos fue un importante problema que enfrentaron los consultados con un 57,62%, en segundo lugar, se encontraron las vulnerabilidades de software y sistemas con un 40%, y en tercer lugar quedó el fraude externo.

Otra estadística importante son las principales preocupaciones de las empresas en cuestión a la seguridad informática, solo se van a comentar las preocupaciones de las pequeñas y medianas empresas, que son las que interesan para el desarrollo de los temas posteriores, como se puede observar, las 3 principales preocupaciones en seguridad son: el malware, la explotación de las vulnerabilidades y el fraude, véase figura 2.3, donde empatan como preocupaciones de una empresa con las anteriores gráficas. La explotación de vulnerabilidades es una de las principales preocupaciones, no solo para las empresas en México sino para las empresas Latinoamericanas, esta comparativa se hace para observar la tendencia que existe en cuestión de las vulnerabilidades en los sistemas de las empresas, por lo cual se dedica un capítulo entero, para entenderlas mejor.

(ESET_security_report_Latinoamérica, 2013)

Figura 2.3 Principales preocupaciones en materia de seguridad de una empresa en Latinoamérica

2.2 Las vulnerabilidades y sus causas

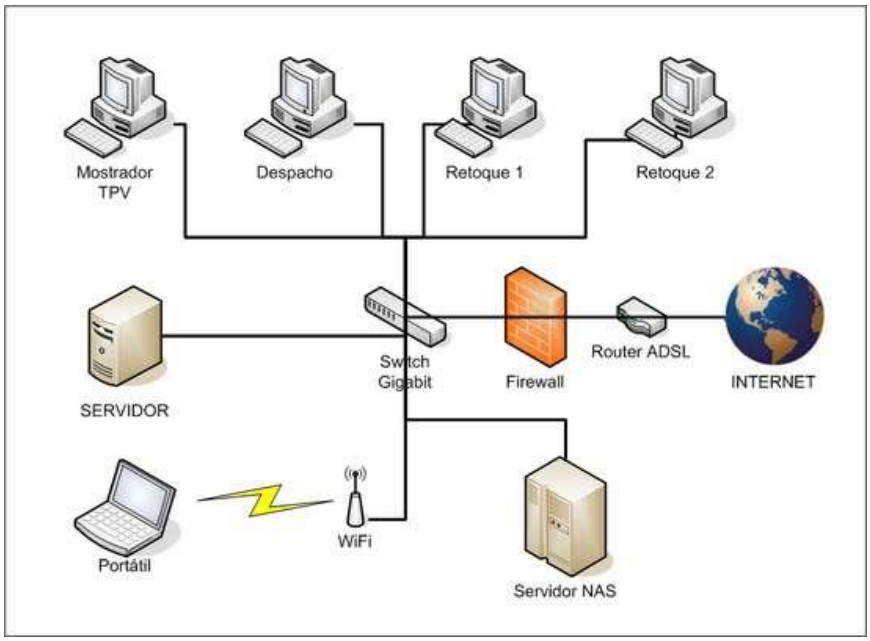
Una vulnerabilidad es un fallo de seguridad, en este capítulo se habla de las causas que pueden provocar huecos (vulnerabilidades) en los sistemas informáticos, véase figura 2.4, basándose en lo que mencionan el libro "Enciclopedia de la seguridad informática" del autor Álvaro Gómez Vieites, además de proporcionar una introducción a las herramientas y métodos que pueden ayudar a encontrar vulnerabilidades y darles una solución.

(www.utp.ac.pa,2014)

Figura 2.4 Vulnerabilidades en los sistemas informáticos

a) Diseño de la red de datos

El mal diseño de la red de datos, trae diversas vulnerabilidades, algunas situaciones que provocan estas son: un mal cableado estructurado, una mala ubicación del rack de comunicaciones, una mala implementación en los protocolos para la comunicación de la red, véase figura 2.5. La lista es grande cuando se habla de las posibles causas que provocan vulnerabilidades en una red. Un ejemplo más específico de error de diseño, consiste en intercambiar información importante en texto claro, sin cifrar, como en los servicios básicos de conexión remota a otros equipos (telnet), de transferencia de archivos (FTP) o de correo electrónico en su versión más básica (SMTP).
Otro ejemplo es la versión 1 y 2 SNMP (Simple Network Managment Protocol) que es un protocolo que sirve para la gestión de red, que usa unas bases de datos llamadas *MIBS* que pueden ser consultadas a través de SNMP, en las primeras versiones del protocolo se basaba en el uso de claves compartidas, por tanto el protocolo tenía una seguridad muy débil, hasta la versión 3, que ya contempla el cifrado de información a través de la red y la autenticación de dispositivos.



(hstech-electronica.blogspot.mx, 2011)

Figura 2.5 Diseño de la red de datos

b) Programación

El mayor número de vulnerabilidades es provocado a la hora de programar aplicaciones o sistemas, véase figura 2.6.

Las actualizaciones para parchar estos errores de programación puede tardar bastante tiempo, este lapso de tiempo es bastante importante, ya que el software o el sistema está vulnerable a un ataque que podría afectar el funcionamiento del mismo, podría provocar desde

un daño leve como tener que abrir de nuevo el programa o hasta dejar inservible al sistema, también las mismas actualizaciones pueden traer al sistema nuevas vulnerabilidades.

(www.genbetadev.com, 2014)

Figura 2.6 Errores de programación

Por tanto es necesario evaluar la rapidez de respuesta de cada fabricante de software, por ejemplo Oracle tardó alrededor de 3 meses para emitir una actualización para java, que usa el sistema móvil Android, pero mientras tanto, la vulnerabilidad pudo ser explotada, por los atacantes interesados. A este tipo de vulnerabilidad se llama “vulnerabilidad de día cero”, quiere decir que ningún usuario o fabricante se ha percatado de la existencia de esta, mientras tanto las personas que se dedican a hacer malware están aprovechando y explotando la vulnerabilidad, es peligrosa por el hecho de que el fabricante no sabe de su existencia, sumando el tiempo en el que tardan en parcharla, con una actualización, por lo mientras muchos equipos o sistemas se encuentran propensos a ataques.

Otra causa frecuente de vulnerabilidades en las aplicaciones o sistemas informáticos se debe a un comportamiento incorrecto frente a entradas no validadas, que pueden provocar situaciones indeseadas como el desbordamiento de una área de memoria utilizada por una aplicación o sistema, *Buffer overflow*, se produce cuando un programa intenta escribir en la memoria de la computadora por encima de los límites de una cadena, o zona de memoria reservada.

c) Configuración de equipos de cómputo y sistemas

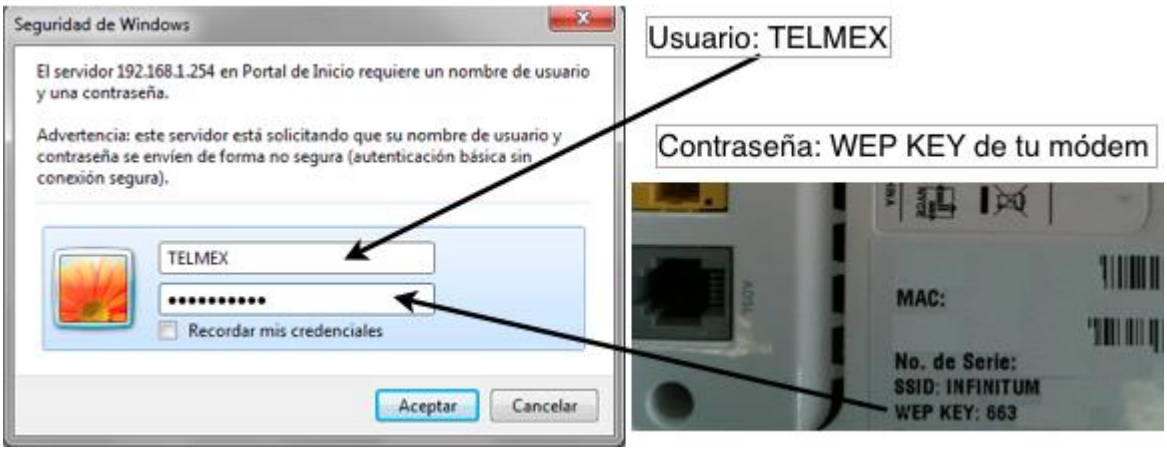
La inadecuada configuración de los sistemas informáticos permite explotar determinadas vulnerabilidades, algunos ejemplos de estas configuraciones deficientes son:

-Dejar las configuraciones de fábrica, en las computadoras, equipos de red y en el software, las cuales son poco seguras y fácilmente deducibles, véase figura 2.7.

-Un mantenimiento inadecuado a(los) sistema(s) informático(s), como no instalar las actualizaciones propuestas por el fabricante para parchar las vulnerabilidades descubiertas.

-Dejar los servicios activos que no son necesarios en los equipos de cómputo, como dejar los puertos abiertos, servicio de red en escucha, hilos de ejecución de programas extraños, principalmente.

-El configurar sin apegarse a las políticas de seguridad informática con las que debiera contar cada organización.



(parentesis.com, 2011)

Figura 2.7 Configuraciones de computadoras

d) Políticas de seguridad informática deficientes

Las organizaciones en ocasiones no tienen la cultura de implementar políticas de seguridad o si las implementan es de una manera deficiente, estas pueden acarrear vulnerabilidades, porque no existen las reglas que dicten que se puede hacer o no en la organización y que cuidados hay que tener al manejar algún equipo, sistema o información dentro de la organización. No solamente es necesario contar con políticas, sino éstas deben estar acordes a la problemática que viva la organización, el nivel de seguridad debe ser el adecuado después de todo un análisis a la problemática y a las políticas, así como las herramientas instaladas y los procedimientos correspondientes, deben revisarse y actualizarse periódicamente, para que de esta manera se tenga una renovación de los puntos anteriores y por lo tanto no se descuide o se tengan fallos, véase figura 2.8.
A continuación se citan distintas situaciones que provocan vulnerabilidades en los sistemas informáticos que podrían ser usadas por los atacantes, por deficientes políticas de seguridad:

-Políticas de contraseñas poco robustas.
-Deficiente control de los intentos de acceso al sistema.
-Escaso rigor en el control de acceso a los recursos.
-Deficiente o inexistente limitación del acceso físico a los equipos más sensibles dispositivos de red y cableado.
-Información sensible que se guarda sin cifrar en el sistema.
-Inadecuado almacenamiento de las copias de seguridad.

(www.idg.es ,2014)

Figura 2.8 Políticas de seguridad

e) Capacitación

La capacitación (véase figura 2.9) a los empleados en una organización es esencial para la adecuada integración al equipo de trabajo, también para que el empleado o nuevo usuario conozca el funcionamiento del sistema, y no por la ignorancia, modifique o configure inadecuadamente un sistema, lo cual podría causar que el sistema informático sea vulnerable a algún ataque, de cualquiera de las personas mencionadas en el capítulo uno.

(www.supersuk.com.mx, 2014)

Figura de 2.9 Capacitación

Las organizaciones pueden y deben dar capacitación a los empleados nuevos, para mitigar que estos hagan mal uso de las instalaciones, equipos de cómputo y activos de la empresa.

Los tipos de capacitación que pueden dar son:

-Capacitación para el trabajo: Dirigida al empleado que va a desempeñar una nueva actividad, ya sea por ser de reciente ingreso o por haber sido promovido o reubicado dentro de la misma empresa.
-Capacitación promocional: A través de ella se da la oportunidad de alcanzar puestos de mayor nivel jerárquico. Esta puede ser la mejor manera de detectar el talento y encontrar a la persona adecuada para ser promovida.
-Capacitación en el trabajo: Encaminada a desarrollar actividades y mejorar actitudes en los trabajadores de la organización.

f) Puertas traseras en los sistemas informáticos

Es importante eliminar y evitar las puertas traseras en los sistemas informáticos, véase figura 2.10, ya que por medio de estas se puede tomar el control del sistema o robar información, modificarla o borrarla, principalmente. Teniendo el control del sistema, el atacante puede hacer prácticamente lo que sus conocimientos e intereses le permitan, todo esto por no cuidar y eliminar las backdoors (puertas traseras) que pudiera contener un sistema, ya sea por error humano o por algún ataque informático, sin embargo es necesario contemplar que hay ocasiones en las que se necesitan y pueden no ser un error si se han diseñado con conocimiento y debido cuidado, por ejemplo para poder controlar un sistema informático remotamente, el cual es muy útil si no se tiene acceso físico al sistema, en caso de que se requiera, para dar una solución a algún problema que se su cite, principalmente.

(profesoradeinformatica.com, 2014)

Figura 2.10 Puertas traseras

g) Equipos informáticos

Los equipos de cómputo, *smartphones*, tablet (véase figura 2.11), pueden ser una gran vulnerabilidad principalmente por la fuga de información privada o confidencial que puede ocasionar estos equipos de uso cotidiano.
Es recomendable que los dispositivos cuenten con una clave de acceso, y que estén vinculados a algún servicio de localización por medio de GPS, ya que permite a la persona que pueda monitorear donde está su dispositivo, desde el sitio web del servicio, incluso si es robado, se puede mandar una señal que reinicie y borre la información del dispositivo.

(tecnomagazine.net, 2011)

Figura 2.11 Dispositivos

2.3 Análisis de vulnerabilidades y metodologías para pruebas de penetración en sistemas informáticos.

Existen en internet diversas herramientas para el análisis de vulnerabilidades, estas son herramientas que sirven para evaluar los posibles fallos que se encuentran en los sistemas informáticos, pueden ser herramientas de paga o de software libre, el análisis de estas herramientas son en su mayoría correctos, pero también puede haber falsos positivos o negativos en la vulnerabilidad evaluada.

Algunas herramientas son:

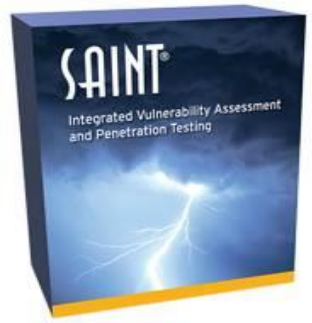
Nombre de la herramienta	Empresa	Con versión de evaluación	Principales características	Logo
Nessus	Tenable	Si	-Escaneo de red, sistemas, datos y aplicaciones -Análisis de vulnerabilidades -Análisis de configuración en servidores, dispositivos de red, base de datos, principalmente	
Saint	SAINT	Si	-Identifica las vulnerabilidades en los dispositivos de red, sistemas operativos, aplicaciones de escritorio, aplicaciones web y base de datos. -Detecta y corrige posibles deficiencias en la seguridad de la red. -Posee estándares y regulaciones que demanda la industria.	
Renita	Beyondtrust	No	-Identifica vulnerabilidades, actualizaciones faltantes, debilidades de configuración. -Posee mejores prácticas para la industria para proteger activos informáticos -Proporciona evaluación de riesgos de seguridad	

Tabla 2.1 Software de escaneo de vulnerabilidades

2.3.1 Pruebas de penetración en sistemas informáticos

Según el NIST (National Institute of Standars and Technology) las pruebas de penetración son evaluaciones de seguridad técnicas, donde se simulan ataques reales con la finalidad de identificar métodos para eludir las características de seguridad en un aplicación, sistema o red.

Para el SANS Institute (SysAdmin Audit, Networking and Security Institute) las pruebas de penetración, es un proceso enfocado a la penetración de las defensas de una organización, comprometer los sistemas informáticos y obtener acceso a información no autorizada.

EC-Council menciona que las pruebas de penetración son el proceso de simular métodos que los intrusos utilizan para obtener acceso no autorizado en los sistemas de una organización y comprometerlos.

2.3.1.1 Metodologías de pruebas de penetración

Las principales metodologías de pruebas de penetración son:

- Penetration Testing Execution Standard (PTES).
- National Institute Standards and technology 800-115 (NIST 800-115)
- PTF (Penetration Test Framework)

a) Penetration Testing Execution Standard (PTES)

Es un proyecto diseñado por especialistas de diferentes áreas de la industria para proporcionar a las empresas y proveedores de servicios de seguridad un enfoque común para las pruebas de penetración. El proyecto inicio en noviembre del 2010, su contenido es abierto y recibe propuestas para mejorar el procedimiento, por esto se encuentra en versión BETA.

b) NIST 800-115

Es una guía técnica para pruebas y evaluación de seguridad de información, que proporciona metodologías, técnicas y herramientas para realizar la evaluación de procesos, servicios, pruebas de penetración y revisión de políticas de seguridad. La metodología plantea 3 fases principales para la evaluación de seguridad: planeación, ejecución y post-ejecución.

c) PTF (Penetration Test Framework)

Es un marco para la realización de pruebas de penetración, propone una metodología con técnicas y herramientas. Fue diseñado por Kevin Orrey y se encuentra en la versión 0.59.

2.3.1.2 Etapas de una prueba de penetración

Estas pruebas de penetración constan de las siguientes etapas (véase figura 2.12):

Planeación: Es una la fases más importantes, porque contempla todos los aspectos que se realizan antes de las pruebas de penetración, tales como contratos, acuerdos de confidencialidad, permisos y activos que se van a evaluar.

Reconocimiento: Es el proceso en el cual se recaba la mayor cantidad de información sobre la organización que se va a evaluar, tales como; los servicios de registro de dominio y sitios web, principalmente.

Escaneo: El fin es encontrar a los activos objetivo que puedan poseer vulnerabilidades.

Explotación: Para garantizar que existe algún fallo se deben lograr explotar las vulnerabilidades encontradas, esto permite eliminar falsos positivos o prevenir falsos negativos.

Documentación: El objetivo de esta fase es plasmar los resultados obtenidos desde la fase de reconocimiento hasta la de explotación. Esta evidencia sirve para elaborar un informa de hallazgos y las vulnerabilidades encontradas durante el proceso.

(unam-cert, 2014)

Figura 2.12 Fases de una prueba de penetración

2.3.1.3 Clasificación de pruebas de penetración

La siguiente clasificación de pruebas de penetración es por el lugar donde se ejecutan:

a) Pruebas de penetración internas

Estas pruebas son llevadas a cabo en la red interna de la organización, por medio del análisis de protocolos de red y servicios, la autenticación de usuarios, permisos, acceso a recursos compartidos, también incluyen la explotación de vulnerabilidades más conocidas en los principales servicios y aplicaciones que tienen los sistemas operativos, base de datos o servidores, además del análisis de seguridad en estaciones de trabajo, la evaluación del comportamiento de los antivirus, principalmente.

b) Pruebas de penetración externas

Estas pruebas se realizan en el exterior de la red de la organización, para encontrar huecos de seguridad que puedan ser explotados por personas malintencionadas, también se revisan los puertos y protocolos para saber las entradas y servicios que están proporcionando los servidores de la organización al exterior, se analiza el tráfico que pasa de la red externa a la red interna, el rango de direcciones utilizado, los intentos de conexión vía internet, las líneas telefónicas, redes inalámbricas, también se realizan intentos de denegación de servicio, ataques para explotar vulnerabilidades en los sistemas y a la infraestructura de red, que solicite el servicio.

La siguiente clasificación de pruebas de penetración de acuerdo al conocimiento previo:

a) Caja negra

En este tipo de pruebas de penetración no se tiene conocimiento previo del objetivo o sistema que se va a evaluar, se considera un escenario real.

b) Caja Blanca

En este tipo de pruebas se tiene acceso a gran parte de la información del objetivo o sistema que se va a evaluar

c) Caja Gris

En este tipo de prueba se tiene acceso a alguna información del objetivo o sistema que se va a evaluar, puede decirse que es una mezclar entre pruebas de caja negra y caja blanca.

Capítulo III
Auditorías de sistemas informáticos

3.1 Introducción

Otra forma de encontrar huecos de seguridad son las auditorías en sistemas informáticos, por lo cual adquieren cada vez mayor importancia, debido a la necesidad de garantizar la seguridad, continuidad y disponibilidad de las infraestructuras informáticas sobre las que se sustentan los procesos de negocio de toda empresa u organización.

3.2 Auditoría de sistemas de información

Se menciona cuál es la definición de una Auditoría en sistemas de Información, sus objetivos y sus fases, además que fases le permitirían a una PyME encontrar sus fallos y realizar las mejoras adecuadas (véase figura 3.1).

(portalmx101.trabajando.com,2014)

Figura 3.1 Auditoría en Sistemas de información

3.2.1 Concepto de Auditoría en sistemas informáticos

A continuación se mencionan distintas definiciones de una Auditoría en Sistemas informáticos:

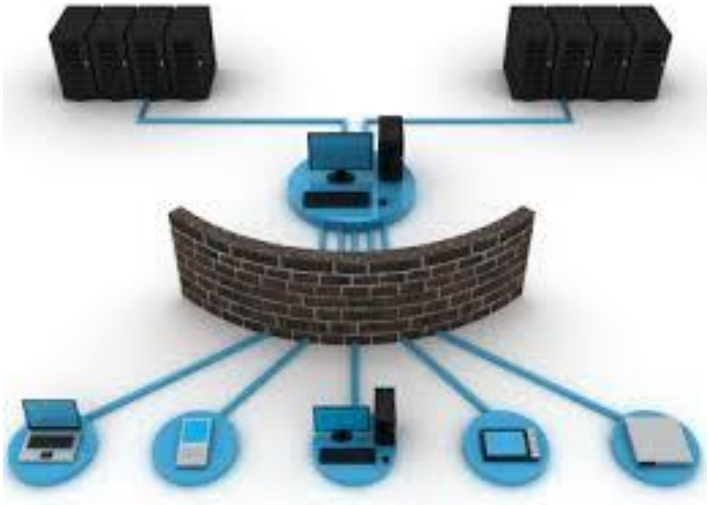
La Auditoría de sistemas informáticos es el proceso de recolección y evaluación de evidencias utilizadas para determinar cuándo un sistema informático salvaguarda sus activos, mantiene la integridad de sus datos, si ejecuta eficazmente los objetivos marcados por la organización con políticas de seguridad y consume los recursos eficientemente.

Una Auditoría en sistemas informáticos pretende evaluar y analizar los posibles fallos o huecos de seguridad que posee una infraestructura informática de una organización para garantizar que los activos informáticos estén resguardados de entes mal intencionados.

Una Auditoría de sistemas informáticos debe tener presente la cantidad de información almacenada en el sistema, la cual en muchos casos puede ser confidencial, ya sea para los usuarios, las empresas o las instituciones, lo que significa que se debe cuidar del mal uso de esta información, de los robos, fraudes, sabotajes y sobre todo de la destrucción parcial o total.

3.2.2 Objetivos de la Auditoría en Sistemas Informáticos

Los objetivos a establecer en una Auditoría de Sistemas Informáticos deben abarcar todo el entorno informático de una organización, que comprende desde el centro de proceso de datos hasta cualquier tipo de comunicación o redes que existan en el entorno físico del sistema.



(www.tecnimedios.com, 2014)

Figura 3.2 Objetivos de la Auditoría en Sistemas Informáticos

3.3 Clasificación de Tipos de Auditorías informáticas

A continuación se menciona los diferentes tipos de auditoría informáticas más importantes.

3.3.1 Auditoría Informática de Aplicaciones, Bases de Datos y Programas

Es una evaluación del llamado análisis de programación y sistemas, por ejemplo una aplicación podría tener las siguientes fases de auditoría:

•Prerrequisitos del usuario y del entorno
•Análisis funcional
•Diseño
•Análisis orgánico (preprogramación y programación)
•Pruebas
•Explotación

Todas estas fases deben estar sometidas a un exigente control interno, de lo contrario, puede producir insatisfacción del cliente, insatisfacción del usuario o altos costos. Por lo tanto, la auditoría deberá comprobar la seguridad de los programas, bases de datos, aplicaciones, en el sentido de garantizar que el servicio ejecutado proporcione, los resultados exactamente previstos y no otros.

3.3.2 Auditoría Informática de Sistemas de Información

Una Auditoría Informática de Sistemas de Información se ocupa de analizar la actividad que se conoce como técnica de sistemas, en todos sus factores, es decir; determina si un sistema de información salvaguarda sus activos, mantiene la integridad de sus datos, cumple con las normas de seguridad fijadas por la organización y la utilización de sus recursos es la adecuada. La importancia creciente de las telecomunicaciones ha propiciado que las redes LAN, WAN y MAN, se auditen por separado, aunque formen parte del entorno general del sistema de información.

3.3.3 Auditoría Informática de Infraestructura de Red

Una Auditoría Informática de Infraestructura de Red deberá actuar sobre los equipos de comunicaciones tipo hubs, switches, routers, firewalls, con el fin de determinar si están operando adecuadamente y cumplen con las políticas de seguridad establecidas por la organización, por lo que es importante verificar las configuraciones de los equipos a detalle por ejemplo: a nivel puerto. Así mismo es la responsable de verificar si los enlaces de comunicación salvaguardan la seguridad de salida y acceso a la organización, para ello la auditoría debe verificar diagramas de conexión de los enlaces (incluyendo los enlaces de respaldo), cuántos son, de que tipo, de que ancho de banda, donde están instalados, que configuración tienen, a donde se conectan, que tipo de información viaje por ellos, principalmente. Otro punto importante a considerar es el cableado, la auditoría debe incluir la revisión de la topología de la red, longitudes, que tipo de cable es el que se está utilizando y si cumple con las políticas de seguridad definidas por la organización, se deben verificar las conexiones entre pisos, áreas, departamentos, centros de cómputo, áreas de comunicaciones, servidores, entre otros, con el fin de identificar puntos de conexión no permitidos o vulnerabilidades de accesos no autorizados.

3.4 Fases de una Auditoría en Sistemas informáticos

En seguida se mencionan las fases de una Auditoría en Sistemas informáticos que se describen en las normas elaboradas por *ISACA.*

3.4.1 Relación con la Organización

Comprende un análisis inicial que tiene que ver con la organización global de la empresa y también comprende el estudio sobre la estructura organizativa a nivel jerárquico y formal del

departamento de sistemas informáticos. Posteriormente se procede a conocer con más profundidad o detalle la estructura organizativa de la empresa a través de los denominados papeles de trabajo que comprenden las entrevistas y cuestionarios que se formulan para la comprensión de la organización.

En esta fase se aplican las siguientes normas de auditoría de sistemas informáticos, la norma 010: Título de Auditoría, la norma 020: Independencia y la norma 030: Ética y Normas Profesionales. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas informáticos es resaltar la independencia y ética profesional del auditor con respecto a la organización.

3.4.2 Planificación de la Operación

Comprende el detalle de los aspectos relevantes que van a ser considerados en la realización de la auditoría, por ejemplo: áreas que cubrirá el estudio (alcance de la auditoría), objetivos esperados de la auditoría, forma en que se llevará a cabo la auditoría (logística), personas que colaborarán en el desarrollo de la auditoría, documentación a reunir o solicitar (estadísticas, manuales de procedimientos, reportes, evidencias, principalmente.) y en que no intervendrán la auditoría véase figura 3.4.

En esta fase se aplican las siguientes normas de auditoría de sistemas informáticos, la norma 040: Idoneidad, la norma 050: Planificación. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas informáticos es resaltar la habilidad y capacidad (técnica y administrativa) del auditor para planear y conducir la auditoría.

(negocios.uncomo.com, 2014)

Figura 3.4 Planificación de la operación

3.4.3 Desarrollo de la Auditoría

Comprende la ejecución y evaluación de los puntos contemplados en el paso anterior y los temas específicamente analizados de esta fase serán:

El entorno informático (interno y externo) del sistema.

Los aspectos referidos al grado de utilización y satisfacción de los diferentes usuarios que manejan las aplicaciones.

En esta fase se aplica la siguiente norma de auditoría de sistemas informáticos, la norma 060: Ejecución del Trabajo de Auditoría. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas informáticos es garantizar el cumplimiento de los objetivos de la auditoría con base a la planeación realizada y a través de evidencias confiables y suficientes.

(www.impulsotecnologico.com, 2014)

Figura 3.5 Desarrollo de la Auditoría en Sistemas de Información

3.4.4 Síntesis y Diagnóstico

Como su nombre indica se procede a analizar e interpretar la información obtenida en las fases anteriores. En esta etapa se pretende poner en evidencia los puntos débiles y fuertes de la infraestructura informática, los riesgos eventuales, las mejoras y las soluciones posibles a alcanzar (análisis costo-beneficio).

En esta fase se aplica la siguiente norma de auditoría de sistemas informáticos, la norma 070: Informes. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas de información es resaltar el alcance y el objetivo de la auditoría contra los hallazgos encontrados.

3.4.5 Presentación de Conclusiones

Debe efectuarse mediante hechos constatados, esto es: las conclusiones deben estar argumentadas, probadas y documentadas evitando su posible refutación. Proposiciones realistas y constructivas. Análisis costo-beneficio.
Esta fase también aplica, la norma 070: Informes.

(redctic.blogspot.com, 2011)

Figura 3.7 Conclusiones de la Auditoría en Seguridad Informática

3.4.6 Redacción de Informe y Formaciones de Plan de Mejoras

En este sentido el informe final de auditoría constituye el documento que expresa el juicio emitido por el auditor y la única referencia oficial. El informe de auditoría (véase figura 3.8) debe estar estructurado de la siguiente forma:

Carta de Presentación: Se debe presentar un resumen-conclusión del trabajo de auditoría.

Introducción al Informe: Se deben exponer los objetivos evaluados, las condiciones en que se desarrolló la auditoría y un resumen de las observaciones y recomendaciones.

Principales Observaciones y Recomendaciones: Se debe reflejar el detalle de las observaciones realizadas y las deficiencias constatadas de acuerdo con los siguientes criterios: descripción exacta, convincente y no repetitiva de las deficiencias. Consecuencias y repercusiones predecibles y breve recomendación del auditor.

Plan de Acción-Mejoras: El plan de mejoras normalmente se puede contemplar en 3 plazos: A corto plazo con mejoras que supongan pequeña inversión en tiempo y dinero; a medio plazo con implantación de aplicaciones que exigen una mayor inversión en tiempo y dinero; a largo plazo con consideraciones que afectan a políticas o reorganizaciones estructurales de la empresa.

(sites.google.com, 2014)

Figura 3.8 Informe de la Auditoría en Sistemas informáticos

En esta fase se aplican las siguientes normas de auditoría de sistemas informáticos, la norma 070: Informes, la norma 080: Actividades de Seguimiento. El propósito de aplicar estas normas en esta fase del desarrollo de una auditoría de sistemas informáticos es resaltar el informe final completo del resultado de la auditoría y los planes de acción a seguir para corregir las desviaciones detectadas, así como el seguimiento a los planes de acción para asegurar el cierre de las desviaciones.

3.5 Introducción al laboratorio para realizar evaluaciones de seguridad

El realizar una Auditoria en Sistemas informáticos o pruebas de penetración, es mucho trabajo y el servicio es muy costoso, por tanto las PyME's difícilmente aceptarían un servicio de este tipo aunque, sus activos informáticos tenga bajos niveles de seguridad, entonces lo que se propone a esta situación es aplicar una evaluación de seguridad, en la cual se puede seguir al menos 3 de la fases de una Auditoría en Sistemas de Información, (la planificación de la operación, el desarrollo de la auditoría, y la síntesis y el diagnostico) o basarse en una metodología de pruebas de penetración en las cuales se utilizan herramientas para la búsqueda de vulnerabilidades, ya que estas pueden provocar riesgos altos para los activos informáticos de la PyME y para la misma empresa.

Lo que se busca es utilizar herramientas de software libre o licencia gratuita que permitan a la PyME realizar una evaluación de seguridad informática a bajo costo y con el resultado de aumentar el nivel de seguridad de la empresa.

Los siguientes subtemas son introductorios a la parte técnica, que proporcionan una visión general de las herramientas más conocidas y genéricas de software libre que pueden dar el análisis y evaluación de las vulnerabilidades en infraestructura de red de la empresa.

Para simular la infraestructura de red de una PyME y hacer la evaluación más realista, se escogieron los componentes más comunes que se encuentran en la infraestructura informática de las empresas, estos componentes son: computadoras con sistemas operativos Windows XP, Windows 7 o Windows 8, un servidor Windows server 2012 R2, un router cisco para una red inalámbrica, en este caso el modelo E1200, y un servidor de seguridad perimetral (Untangle) como solución extra posterior a la evaluación.

(Microsoft, Untangle, kali linux, 2013)

Figura 3.9 Infraestructura de prueba

a) Análisis de vulnerabilidades de una infraestructura de red

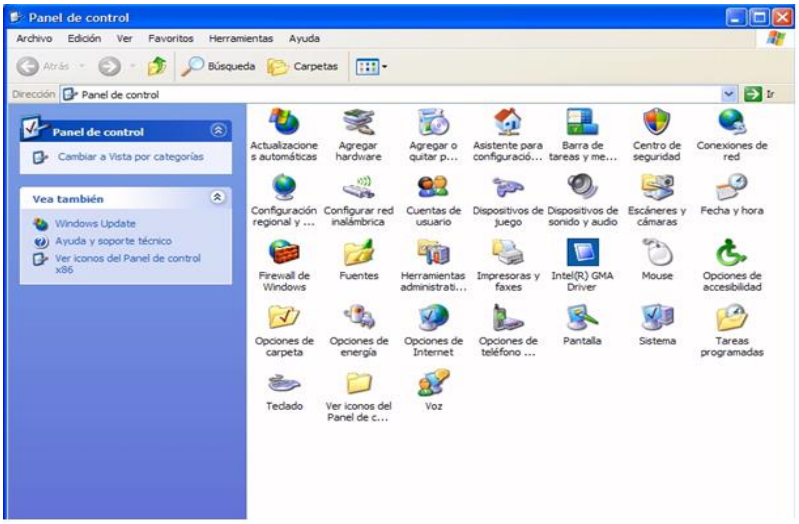
El análisis de vulnerabilidades se realiza por lo regular con herramientas (véase el punto 2.2 del capítulo 2) que permiten evaluar las posibles fallas o huecos de seguridad que tienen los componentes de una red, como los equipos de cómputo, servidores, router, principalmente. Estas herramientas facilitan el trabajo del auditor o pentester y permiten que sea más rápido dar el diagnóstico de la infraestructura de red (véase figura 3.10).

(www.dosbit.com, 2010)

Figura 3.10 Vulnerabilidades de Windows

b) Configuración de equipos de cómputo

No dejar configuraciones por default de los equipos, actualizar los dispositivos y equipos de cómputo o colocar una contraseña más robusta en los dispositivos como los routers, puede dificultar la intrusión de alguna persona mal intencionada (véase figura 3.11).

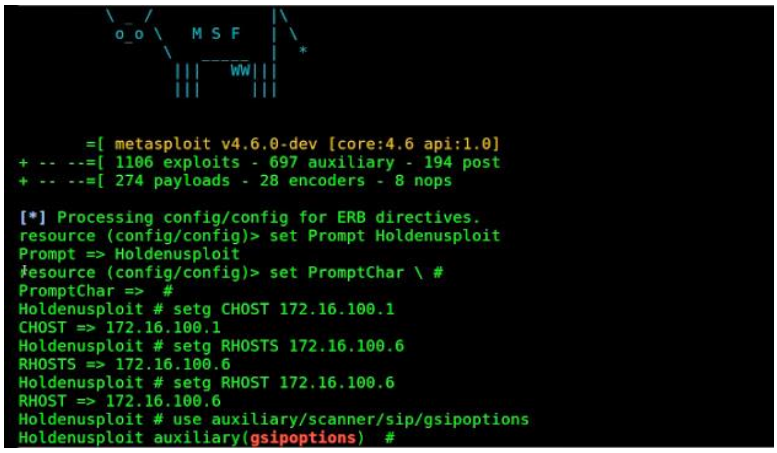


(daixp.wikispace.com, 2014)

Figura 3.11 Configuraciones de equipos

c) Pruebas de penetración

Estas pruebas se utilizan para realizar ataques controlados a los equipos de una red, tratando de explotar alguna vulnerabilidad de forma controlada, esto para que la falla sea parchada antes de que una persona mal intencionada pueda explotarla. Se pueden realizar estas pruebas también para eliminar falsos positivos que poseen los resultados del escaneo de vulnerabilidades, para cerciorarse si en verdad tiene una vulnerabilidad el equipo de cómputo, servidor o router.

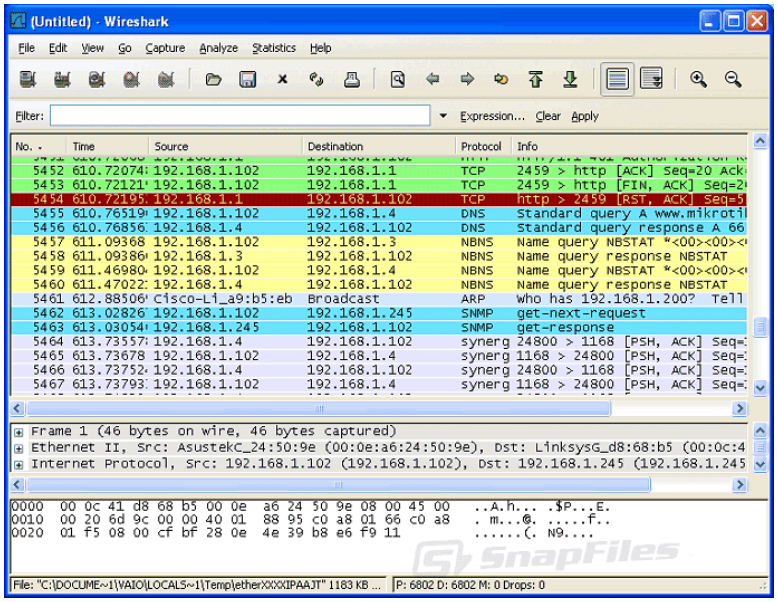


(hack-tools.blackploit.com, 2014)

Figura 3.12 Pruebas de penetración

d) Análisis de tráfico en red

Este tipo de pruebas son utilizadas para detectar, analizar y relacionar tráfico, identificando las posibles amenazas a la red (véase figura 3.14), hay diversas herramientas de software libre que ayudan a realizar este análisis de una manera más sencilla, posteriormente se hablará más de este tema.



(www.dosbit.com,2014)

Figura 3.14 Análisis de tráfico de red

Capítulo IV
Casos de estudio de una evaluación de seguridad

4.1 Introducción

Es importante realizar evaluaciones de seguridad que permitan encontrar fallos en los sistemas informáticos, por medio de herramientas como escáneres de vulnerabilidad, analizadores de tráfico, *sniffers* o metodologías de *pentest*, para saber dónde está el fallo y remediarlo lo más antes posible.

4.2 Análisis de vulnerabilidades en una infraestructura de red

A continuación se propone una herramienta sencilla de usar, para realizar un análisis de vulnerabilidades en los equipos y servidores de la red interna de una organización.

4.2.1 Análisis de vulnerabilidades con Nessus

Nessus es un scanner de vulnerabilidades robusto, existen 2 versiones, la versión “home” que tiene todos los *plug-in* necesarios para realizar una evaluación estándar y la versión profesional que posee acceso a otras soluciones de seguridad que desarrolla Tenable, que es la empresa que le da soporte a esta herramienta.

Nessus trabaja bajo una arquitectura cliente servidor, la cual al descargar el software e instalarlo, también se descargan los plug-ins que servirán a la hora de auditar las fallas de seguridad de los equipos de cómputo o servidores, ya que contienen la información y módulos de prueba sobre las diferentes vulnerabilidades conocidas para cada campo específico. Al instalar la herramienta e iniciarla, se ingresa el usuario y contraseñas de Nessus, se despliega el menú principal donde se puede observar los reportes obtenidos, los escaneos, las políticas para lanzar el escaneo y los usuarios de la red.

4.2.1.1 Caso práctico No. 1

Se realiza un escaneo de vulnerabilidades a los equipos y servidores de la red del laboratorio, la herramienta escanea los puertos, prueba los fallos de los equipos por medio de políticas que se configuran antes de lanzar el escaneo y con la ayuda de los plug-ins se van obteniendo los huecos de seguridad en los equipos.
Para configurar una política en Nessus, solo se le da en la opción de nueva política, para este caso se va a lanzar un escaneo general a todos los equipos de la red (incluyendo servidores), por tanto se elige la opción *Basic Network scan*, véase figura 4.1

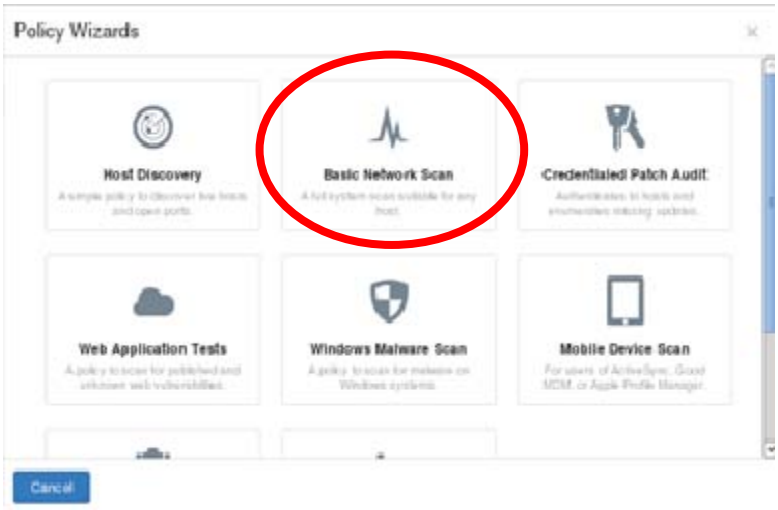


Figura 4.1 Opciones de política en Nessus

Ya que se creó la política, como se puede observar (véase figura 4.2), se procede a lanzar el escaneo.

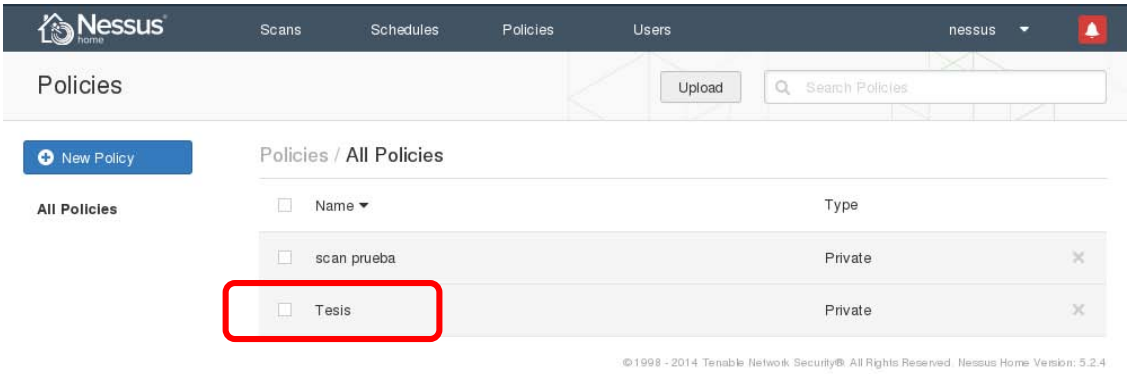


Figura 4.2 Creación de la política

Solo hay que ponerle un nombre al escaneo, decirle que tome como política la que se creó y darle el rango de ip´s que se quiere escanear, véase figura 4.3.

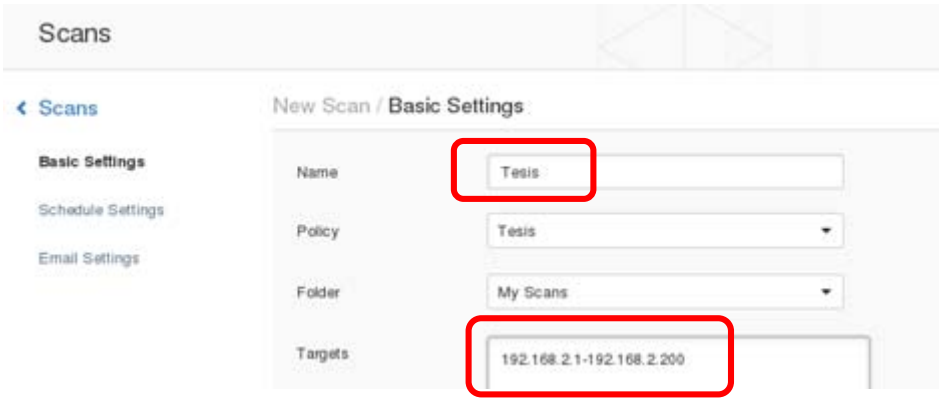


Figura 4.3 Configuración del escaneo en Nessus

Al lanzar el escaneo y esperar el debido tiempo para que la herramienta realice su trabajo, se obtuvieron los siguientes resultados, en la ip 192.168.2.104 que es la de un Windows server 2012 se encontraron 13 vulnerabilidades, una de alto riesgo, 8 de medio riesgo y otras 4 de bajo riesgo, en la ip 192.168.2.155 que es el sistema operativo Windows 7 se detectó solo una vulnerabilidad de medio riesgo, esto debido a que se le instalaron las actualizaciones al sistema operativo antes del escaneo, la ip 192.168.2.1 que es el servidor Untange, se le detectaron 13 vulnerabilidades, una de alto riesgo, 8 de medio riesgo y otras 4 de bajo riesgo, la ip 192.168.2.177 que es el sistema operativo Kali, solo se le detectó una vulnerabilidad de medio riesgo, véase figura 4.4.

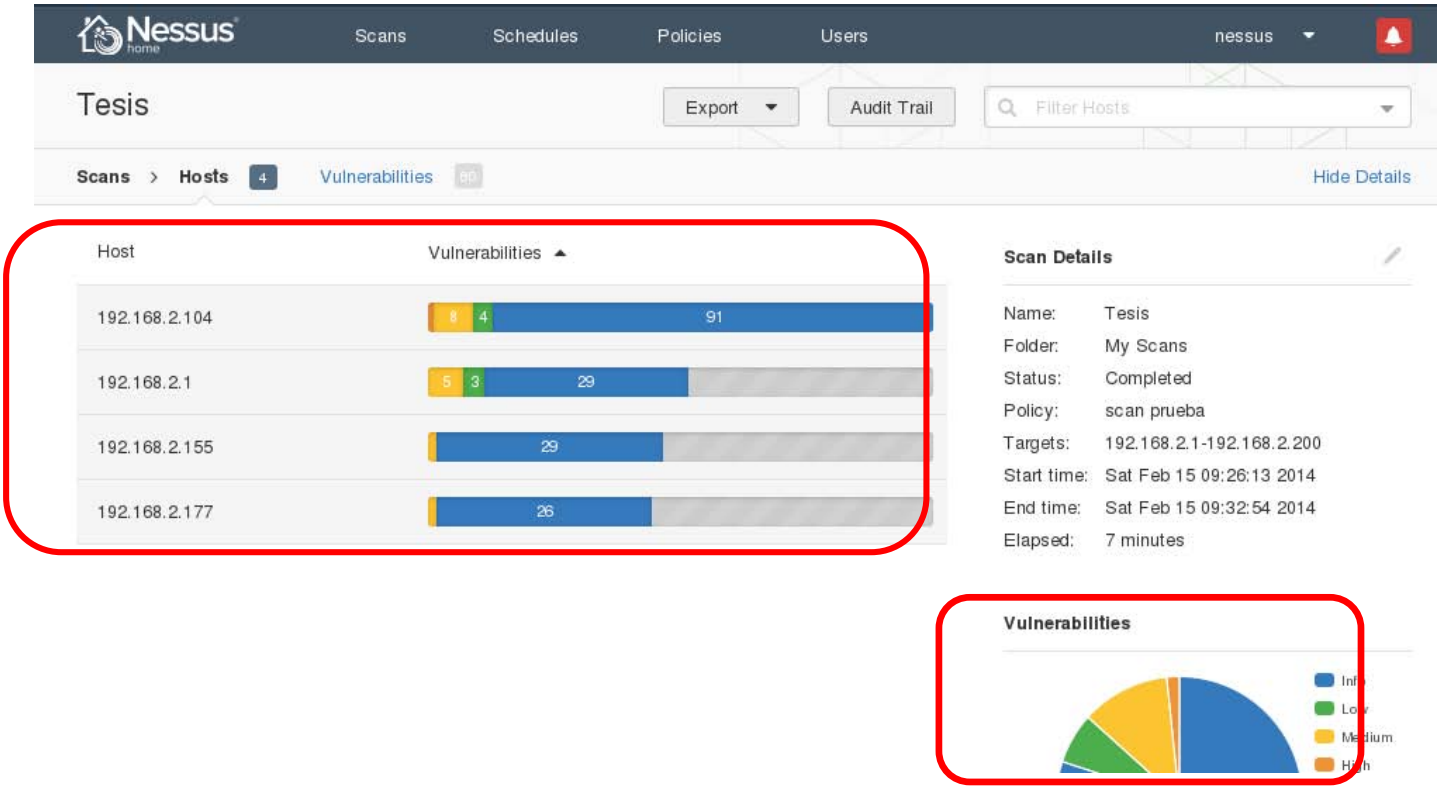


Figura 4.4 Resultado del análisis de vulnerabilidades con Nessus

4.2.1.1 Resultado

Como se puede observar en los resultados, las vulnerabilidades se pueden corregir, por medio de las actualizaciones, el sistemas operativo Windows 7 al cual se le aplicaron las actualizaciones automáticas, se muestra con menos fallos que el servidor con el sistema operativo Windows Server 2012, al cual no se le aplicó ninguna actualización, también se observa que el mismo *firewall* (Untangle), que se utiliza para filtrar lo que viene de Internet hacia la red interna y viceversa, necesita actualizarse, cabe mencionar que las vulnerabilidades que son de mayor importancia en resolver para la organización debe ser las de medio y alto riesgo. Otra situación que hay que considerar es que las herramientas de análisis de vulnerabilidades puede dar como resultados falsos positivos o peor aún falsos negativos, por lo que es importante cerciorarse de que se trata de una vulnerabilidad, esto se logra explotando el fallo encontrado como se puede observar en el Anexo A.

4.3 Configuración de equipos informáticos

Es indispensable modificar la configuración de fábrica de los diferentes equipos de la red de una organización para evitar que sean vulnerados.

4.3.1 Configuraciones por default

La configuración de los elementos de la red es muy importante, ya que de ahí se puede derivar varias vulnerabilidades dependiendo el dispositivo. Algunos fallos son causados por dejar configuraciones por default o de fábrica, el no tener la cultura de seguridad y no darse un poco de tiempo para cambiar este tipo de configuraciones, puede ser muy costoso, ya que atacantes malintencionados podrían aprovechar las fallas, para obtener información de la organización de donde vulneraron el dispositivo, realizar una negación de servicio al dispositivo o espiar lo que pasa a través de la red, principalmente.

4.3.1.1 Caso práctico No. 2

La prueba se realizó en una instalación de la facultad de Medicina donde se encontró un router inalámbrico, bastante vulnerable, ya que traía todas las configuraciones de fábrica, como el usuario y password que por *default* en los dos casos era “admin”, véase figura 4.5.

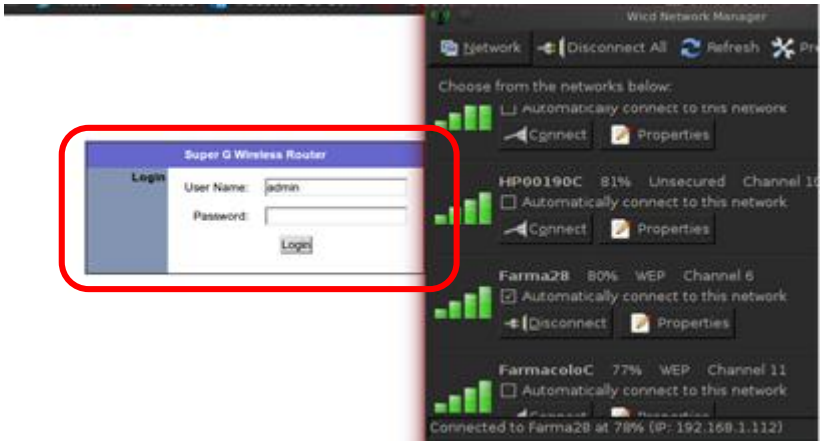


Figura 4.5 Configuraciones por default de router inalámbrico encontrado

Como se puede observar ya entrando al router inalámbrico, se tiene acceso a todas las configuraciones del dispositivo, como el segmento de red que proporciona, permite saber cuáles son las direcciones de los servidores DNS, qué usuarios están conectados, cuál es su dirección mac, por mencionar aspectos relevantes, véase figura 4.6.

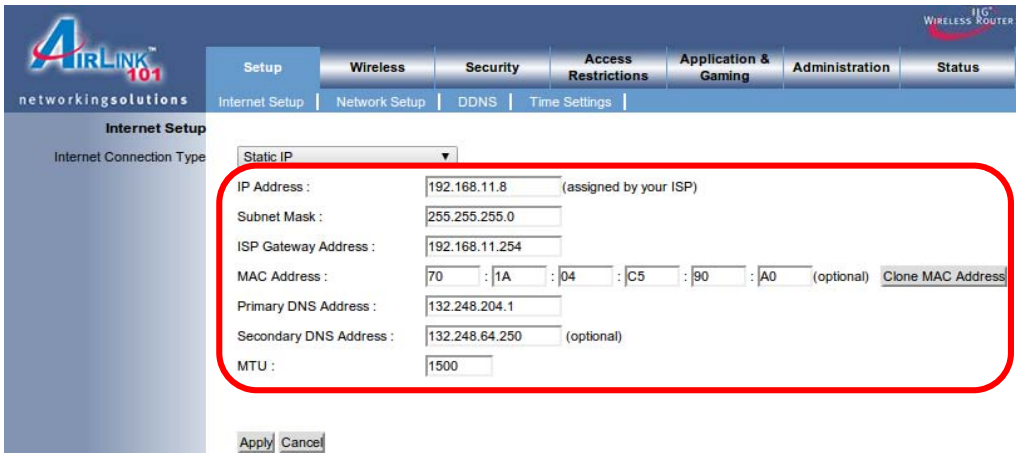


Figura 4.6 Dentro del router

En la siguiente imagen se puede observar también la escasa seguridad que posee este router, ya que la contraseña de acceso a la red es muy sencilla (12345) y se está usando un protocolo de conexión que proporciona una seguridad prácticamente nula en estos días, por lo que no es recomendado que se utilice el protocolo (WEP) para redes inalámbricas, véase figura 4.7.

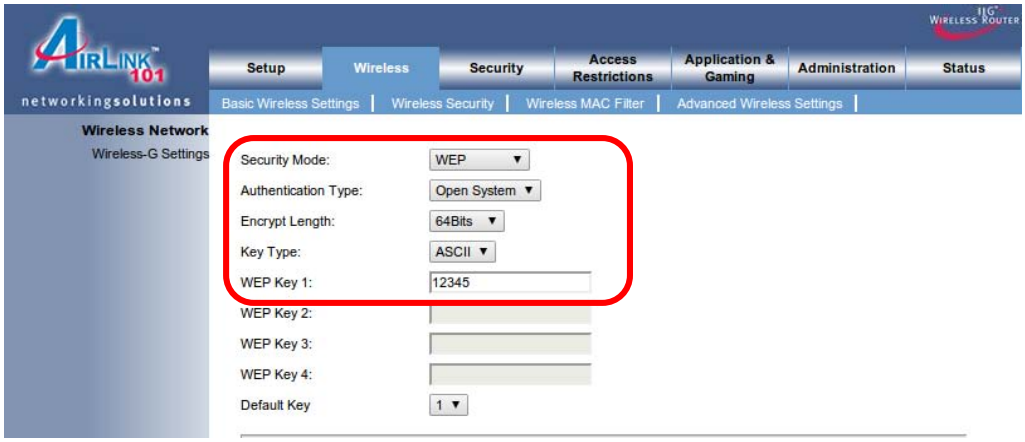


Figura 4.7 Escasa seguridad en el router

En esta otra imagen se observa que también se tiene acceso al password del router, el cual debería de ser más robusto para evitar que sea fácilmente deducible, véase figura 4.8.

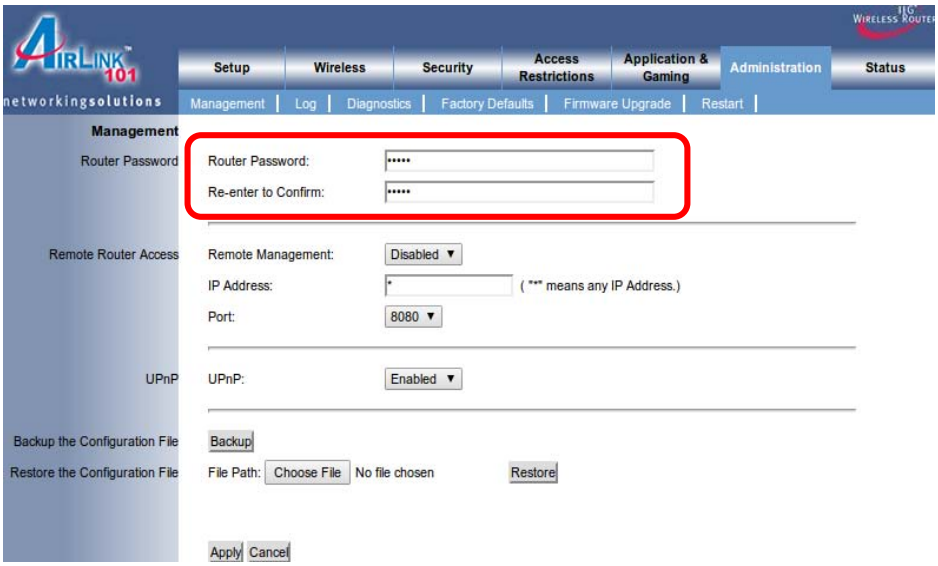


Figura 4.8 Password de acceso al router

Cabe mencionar que se puede sacar bastante información, que a un usuario mal intencionado podría servirle, se pueden ver las direcciones MAC, el tiempo de conexión, el tipo de comunicación inalámbrica y cuál es la velocidad de la comunicación, véase figura 4.9.

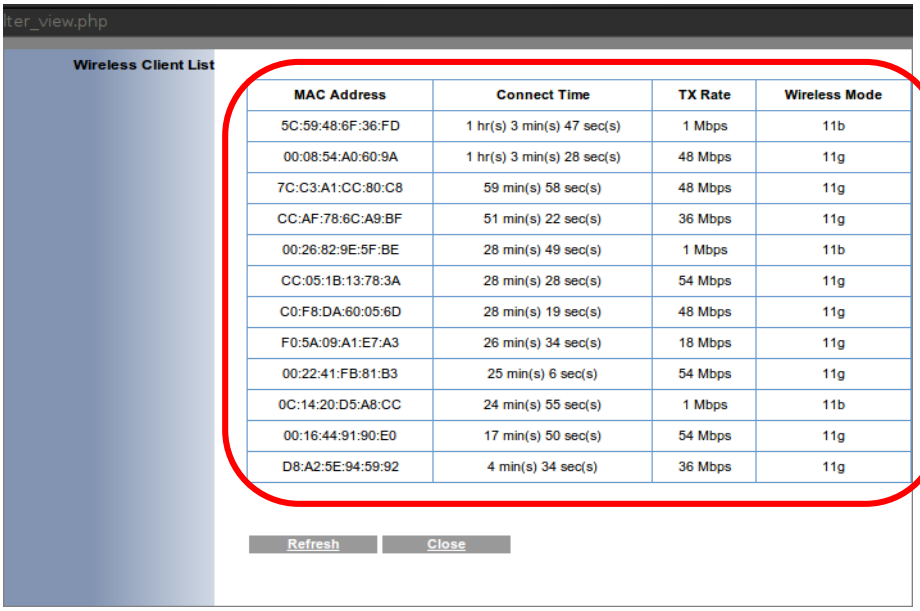


Figura 4.9 Direcciones MAC encontradas

4.3.1.2 Resultado

Los router inalámbricos con configuraciones por *default* son bastante vulnerables, sin ningún esfuerzo computacional (ataque de fuerza bruta) se obtuvo la contraseña del router. Aquí la solución inmediata es cambiar el usuario y contraseña por *default*, por otros que contengan caracteres alfanuméricos, y de mayor longitud (arriba de 8 caracteres), cambiar el protocolo de conexión por uno que brinde mayor seguridad como lo son WPA o WPA2, además de realizar un filtrado por dirección MAC.

4.4 Evaluación de seguridad de red inalámbrica.

Muchas PyME's poseen dispositivos de red inalámbricos, que no siempre usan protocolos de comunicación seguros o sus contraseñas son fáciles de predecir, por tanto auditar la parte de infraestructura inalámbrica es indispensable para encontrar si las vulnerabilidades se encuentran en los puntos anteriormente mencionados.

4.4.1 Obtención de usuarios y contraseñas

En estas pruebas se pretende auditar la parte de la infraestructura inalámbrica de la red simulada de una organización.

Principalmente se realizan 2 pruebas, una con la herramienta hydra que realiza un ataque de fuerza bruta para encontrar datos de usuario y contraseña de un router inalámbrico, para poder determinar si la contraseña es lo suficientemente robusta, por tanto pueda aguantar este tipo de ataques, y la otra prueba es con la suite de software de seguridad Aircrack, para tratar de obtener

la contraseña ahora de la red inalámbrica y probar si es lo suficientemente robusta, además de verificar si el router realiza conexiones seguras a través de protocolos como WPA y WPA2 (protocolos para la conexión de redes inalámbricas).

Hydra es un software que intenta *crakear* por fuerza bruta la contraseña de una cantidad grande de protocolos, como: TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC, RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, AFP, LDAP2, Cisco AAA.
Aircrack-ng es una suite de software de seguridad inalámbrica que consiste en un analizador de paquetes de redes, un crackeador de redes con seguridad WEP y WPA/WPA2-PSK, y otro conjunto de herramientas de auditoría inalámbrica.

Las herramientas más utilizadas para la auditoría inalámbrica son:

- Aircrack-ng: descifra la clave de los vectores de inicio.
- Airodump-ng: escanea las redes y captura vectores de inicio.
- Aireplay-ng: inyecta tráfico de red para elevar la captura de vectores de inicio o permite la captura de *handshakes*.
- Airmon-ng: establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores y paquetes de red.

4.4.1.1 Caso práctico No. 3.1

Las contraseñas débiles siguen siendo en la mayoría de los casos la mayor vulnerabilidad de cualquier sistema de red. Es común que los usuarios no tenga conciencia de lo necesario que es tener una contraseña robusta, precisamente hydra explota esta vulnerabilidad que se da en las personas o usuarios de algún sistemas de la red, por tanto realizar una auditoria donde se evalué la fortaleza de la contraseñas en un organización debería ser necesaria, por tanto el siguiente es un caso simulado donde se trata de vulnerar un router inalámbrico cisco, que podría estar en una casa o en una organización, demostrando así lo fácil que puede ser entrar a un router que carece de un contraseña bien elaborada.

Por medio de hydra se obtendrá la contraseña y el usuario del router, en seguida se observa como con una simple línea de comando proporciona el resultado, véase figura 4.10.

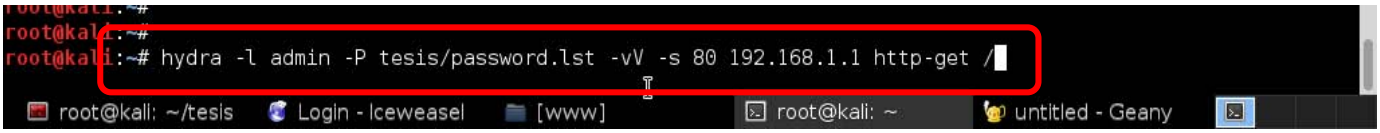


Figura 4.10 Línea de comando para la obtención de usuario y contraseña

En seguida se puede ver el crackeo de manera acertada de la contraseña y el usuario del router cisco, que es en este caso es “admin” y “admin”, véase figura 4.11.

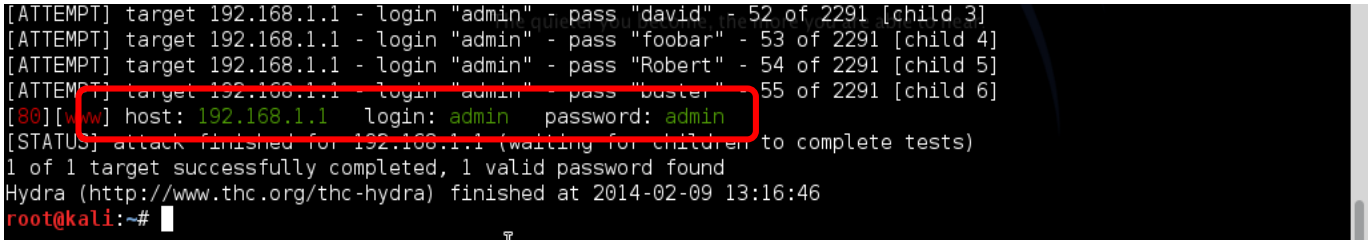


Figura 4.11 Obtención del usuario y contraseña

En esta otra imagen se observa otro resultado pero con una contraseña más robusta, véase figura 4.12, esto quiere decir que por medio de un ataque de diccionario de datos o fuerza bruta es posible obtener la contraseña o el usuario, de lo que va depender es que el atacante tenga un buen diccionario de palabras y el poder de procesamiento de la computadora que se está usando para generar el ataque.

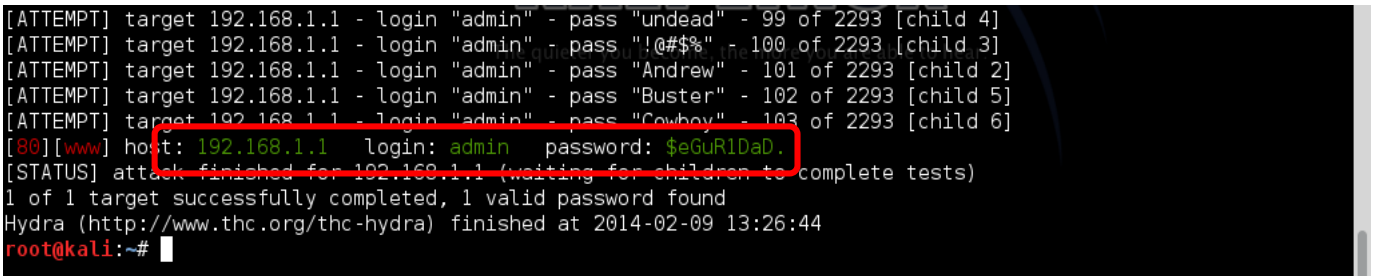


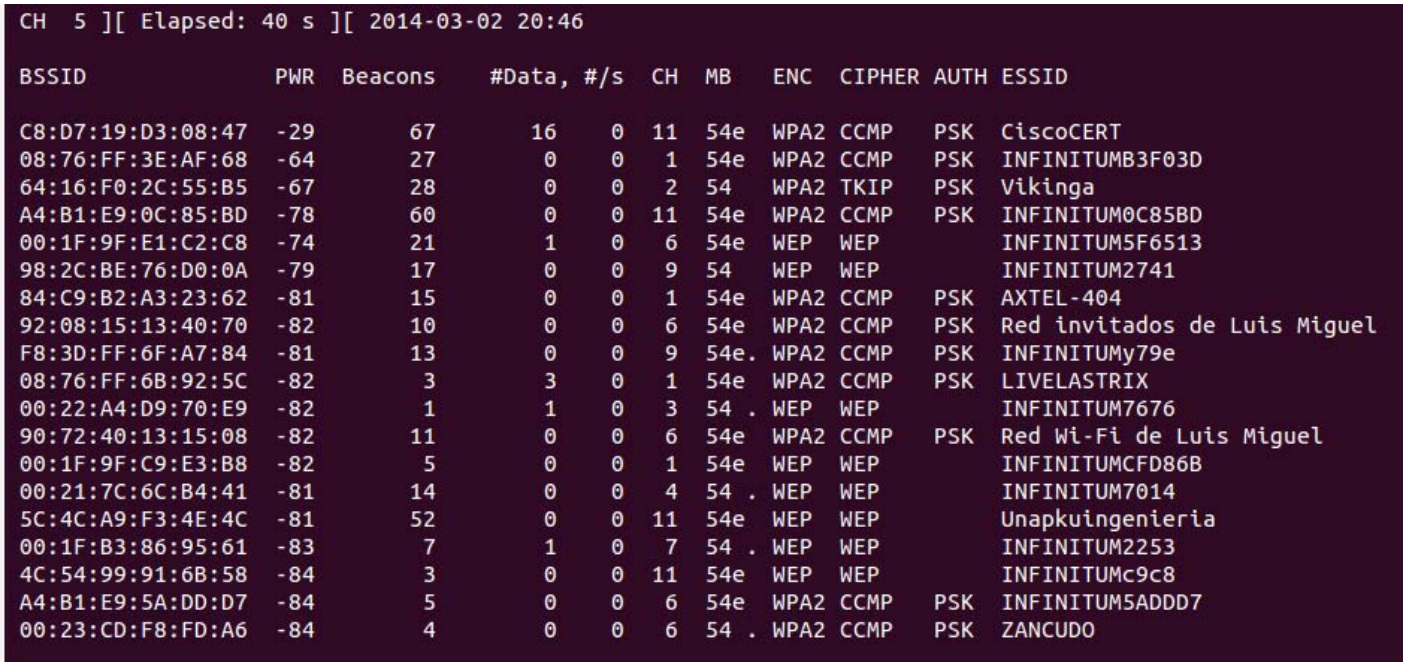
Figura 4.12 Obtención de una contraseña más robusta

4.4.1.2 Resultado

Los resultados con hydra fueron satisfactorios obteniendo la contraseña y el usuario, esto reafirma que el tener una buena contraseña con caracteres alfanuméricos y cambiar las configuraciones por *default* de los dispositivos de red es una buena práctica de seguridad para una organización, con este tipo de pruebas se puede descartar si las vulnerabilidades se encuentran en los password de los dispositivos de red.

4.5.1.1 Caso práctico No. 3.2

Por medio de aircrak y airodump, se pueden realizar pruebas para comprobar la efectividad de la seguridad en la red inalámbrica de una organización, a continuación se realiza el monitoreo de las redes disponibles y se elige el objetivo, en este caso es la red CiscoCERT donde se utiliza el protocolo WPA2 que es acrónimo de WiFI Protected Access 2 (Acceso Protegido Wi-FI 2) que se utiliza para realizar la conexión segura entre el dispositivo o equipo al router inalámbrico, véase figura 4.13.



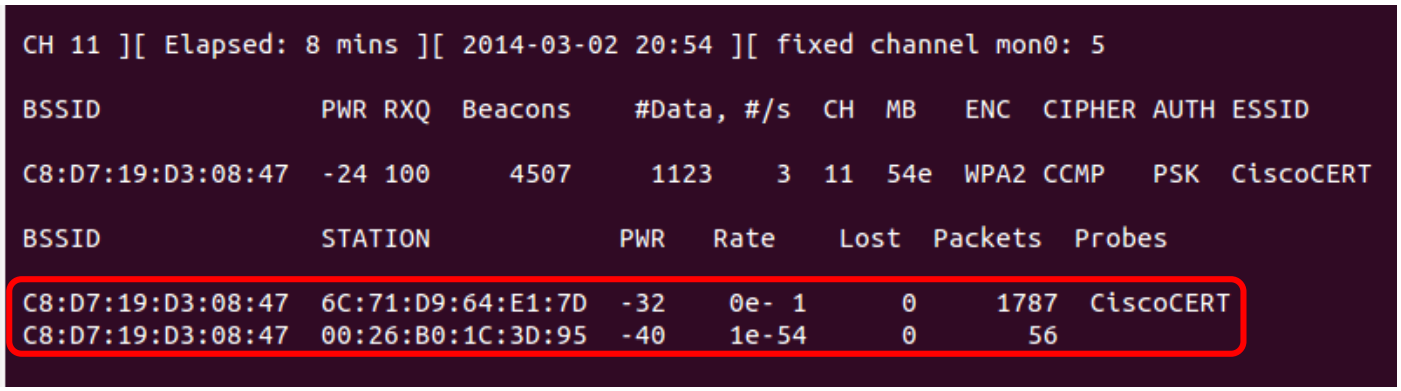
```
CH  5 ][ Elapsed: 40 s ][ 2014-03-02 20:46

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:D7:19:D3:08:47  -29       67       16    0  11  54e  WPA2 CCMP   PSK  CiscoCERT
08:76:FF:3E:AF:68  -64       27        0    0   1  54e  WPA2 CCMP   PSK  INFINITUMB3F03D
64:16:F0:2C:55:B5  -67       28        0    0   2  54   WPA2 TKIP   PSK  Vikinga
A4:B1:E9:0C:85:BD  -78       60        0    0  11  54e  WPA2 CCMP   PSK  INFINITUM0C85BD
00:1F:9F:E1:C2:C8  -74       21        1    0   6  54e  WEP  WEP         INFINITUM5F6513
98:2C:BE:76:D0:0A  -79       17        0    0   9  54   WEP  WEP         INFINITUM2741
84:C9:B2:A3:23:62  -81       15        0    0   1  54e  WPA2 CCMP   PSK  AXTEL-404
92:08:15:13:40:70  -82       10        0    0   6  54e  WPA2 CCMP   PSK  Red invitados de Luis Miguel
F8:3D:FF:6F:A7:84  -81       13        0    0   9  54e. WPA2 CCMP   PSK  INFINITUMy79e
08:76:FF:6B:92:5C  -82        3        3    0   1  54e  WPA2 CCMP   PSK  LIVELASTRIX
00:22:A4:D9:70:E9  -82        1        1    0   3  54 . WEP  WEP         INFINITUM7676
90:72:40:13:15:08  -82       11        0    0   6  54e  WPA2 CCMP   PSK  Red Wi-Fi de Luis Miguel
00:1F:9F:C9:E3:B8  -82        5        0    0   1  54e  WEP  WEP         INFINITUMCFD86B
00:21:7C:6C:B4:41  -81       14        0    0   4  54 . WEP  WEP         INFINITUM7014
5C:4C:A9:F3:4E:4C  -81       52        0    0  11  54e  WEP  WEP         Unapkuingenieria
00:1F:B3:86:95:61  -83        7        1    0   7  54 . WEP  WEP         INFINITUM2253
4C:54:99:91:6B:58  -84        3        0    0  11  54e  WEP  WEP         INFINITUMc9c8
A4:B1:E9:5A:DD:D7  -84        5        0    0   6  54e  WPA2 CCMP   PSK  INFINITUM5ADDD7
00:23:CD:F8:FD:A6  -84        4        0    0   6  54 . WPA2 CCMP   PSK  ZANCUDO
```

Figura 4.13 Monitoreo de las redes disponibles

Ya que se tiene el objetivo, se empiezan a capturar paquetes del router, se puede observar qué 2 clientes están conectados, véase figura 4.14.



```
CH 11 ][ Elapsed: 8 mins ][ 2014-03-02 20:54 ][ fixed channel mon0: 5

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:D7:19:D3:08:47  -24 100     4507     1123    3  11  54e  WPA2 CCMP   PSK  CiscoCERT

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

C8:D7:19:D3:08:47  6C:71:D9:64:E1:7D  -32    0e- 1      0     1787  CiscoCERT
C8:D7:19:D3:08:47  00:26:B0:1C:3D:95  -40    1e-54      0       56
```

Figura 4.14 Captura de paquetes del access point objetivo

Posteriormente se desautentica a uno de los usuarios por medio de aireplay y se trata de capturar su Three Way Handshake (procedimiento de negociación para conexión de 3 pasos), obteniendo esto se puede proseguir a realizar un ataque de diccionario de datos para encontrar el password, véase figura 4.15

Figura 4.15 Obtención de Three Way Handshake

Como puede verse se encontró la contraseña, la cual es muy común y cualquier diccionario de datos la tiene por default, véase figura 4.16.

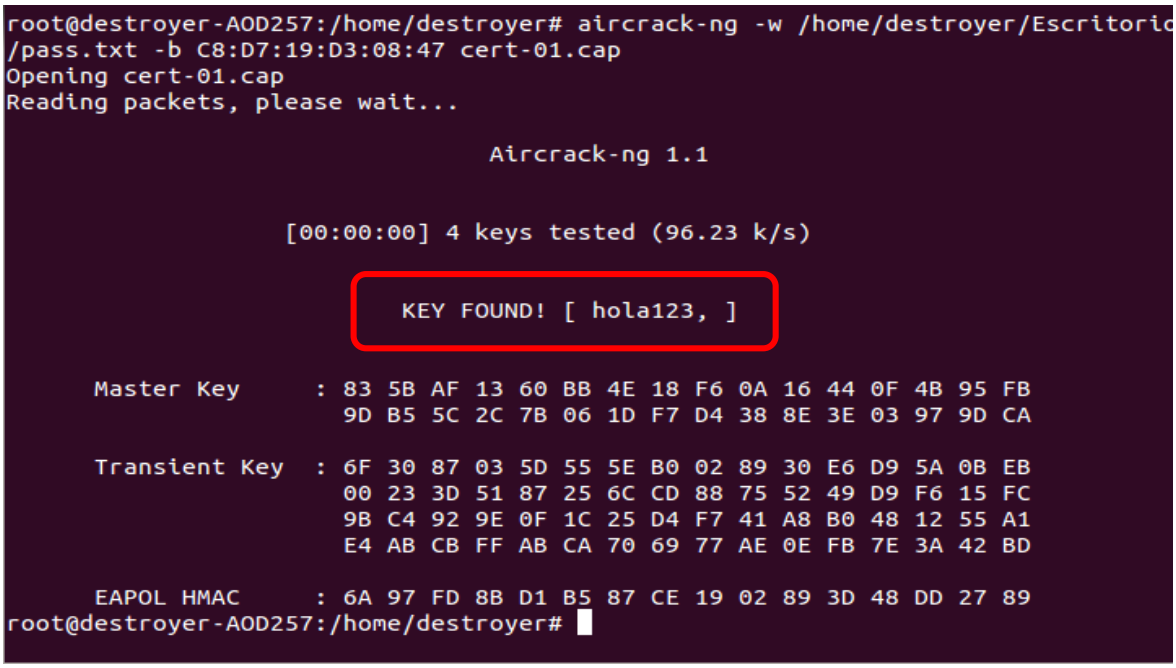


Figura 4.16 Obtención de la contraseña

4.5.1.2 Resultado

El auditar las propias redes inalámbricas en una organización es indispensable, ya que le permite al administrador de la red identificar si se posee alguna vulnerabilidad, por ejemplo: al usar un protocolo de conexión poco seguro como WEP (Wired Equivalet Privacy) o tener una contraseña corta que no combine caracteres alfanuméricos.

En protocolos más seguros como WPA o WPA2, cabe mencionar que se tiene que deshabilitar la opción de WPS (Wi-FI Protected Setup), el cual es la definición de diversos mecanismos para facilitar la configuración de una red WLAN segura con WPA2, pero que contiene una debilidad

que permite romper su seguridad en pocas horas, por lo cual es recomendable que las organizaciones no activen este tipo configuración rápida.

4.6 Análisis de tráfico de red

El monitorear el tráfico que pasa por la red de una organización es importante, porque a partir de ahí es posible detectar alguna infección por malware o un uso inadecuado del ancho de banda de la red de la PyME.

4.6.1 Herramienta Wireshare y Ntop

Ntop es una herramienta que permite controlar en tiempo real a los usuarios y aplicaciones que están consumiendo recursos de red, además de que ayuda a detectar malas configuraciones en algún equipo.

Si un equipo tiene algún error leve o grave dependiendo del nivel del error, la herramienta despliega una bandera amarilla o roja.

Posee un microservidor web desde el que cualquier usuario con acceso puede ver las estadísticas del monitoreo.

Wireshare es una herramienta de análisis de protocolos y ayuda a solucionar problemas en las redes de datos, proporciona una interfaz gráfica y filtrado de paquetes, también permite ver todo el tráfico que pasa por una red estableciendo la configuración en modo promiscuo.

4.6.1.1 Caso Práctico No. 4.1

Ntop permite de una manera rápida y fácil obtener un panorama general del tráfico que pasa por una red, esto en la opción de *All Protocols*. Se puede observar la cantidad de datos intercambiados por TCP o UDP, qué sistema operativo está enviando peticiones a qué servidores y de qué país son esos servidores. Esta opción de la herramienta es una de las más útiles para analizar qué está ocurriendo en tiempo real en la red de la empresa, se recomienda utilizarla con un puerto espejo.

En la siguiente imagen (véase figura 4.17) se presenta cómo Ntop proporciona un “panorama general” de lo que se está transmitiendo en la red, los datos enviados y recibidos, así como los protocolos más comunes, también se puede observar si se trata de un sistema Linux o Windows que recibe o envía datos.

Network Traffic [All Protocols]: All L3 Hosts - Data Sent+Received

Hosts: All Data: All

Host	Location	Data		TCP	UDP	ICMP	ICMPv6	IPsec	(R)ARP	NetBios	GRE	IPv6	STP	IPsec	OSPF
destroyer-PC.example.com		3.0 MBytes	33.8 %	2.7 MBytes	8.0 KBytes	0	0	0	46	0	0	0	0	0	0
fpdownload.adobe.com		1.4 MBytes	16.0 %	1.3 MBytes	0	0	0	0	0	0	0	0	0	0	0
WIN-...1A1EISPA.example.com		1.4 MBytes	15.7 %	1.0 MBytes	63.0 KBytes	429	0	0	2.4 KBytes	0	0	0	0	0	0
blu.stc.s-msn.com		703.9 KBytes	7.8 %	552.2 KBytes	0	0	0	0	0	0	0	0	0	0	0
img....gets.video.s-msn.com		600.9 KBytes	6.7 %	558.1 KBytes	0	0	0	0	0	0	0	0	0	0	0
www.google.com.mx		399.1 KBytes	4.4 %	271.1 KBytes	0	0	0	0	0	0	0	0	0	0	0
s.ytimg.com		323.2 KBytes	3.6 %	254.1 KBytes	0	0	0	0	0	0	0	0	0	0	0
i1.ytimg.com		198.0 KBytes	2.2 %	155.6 KBytes	0	0	0	0	0	0	0	0	0	0	0
192.168.2.1		160.4 KBytes	1.8 %	1.6 KBytes	144.0 KBytes	207	0	0	14.6 KBytes	0	0	0	0	0	0
dsl-...rod-infinitum.com.mx		113.3 KBytes	1.3 %	88.4 KBytes	0	0	0	0	0	0	0	0	0	0	0
www.gstatic.com		110.3 KBytes	1.2 %	84.0 KBytes	0	0	0	0	0	0	0	0	0	0	0
apis.google.com		96.3 KBytes	1.1 %	90.4 KBytes	0	0	0	0	0	0	0	0	0	0	0

Figura 4.17 Tráfico de red de los protocolos más comunes

Otra opción interesante de Ntop, es que se pueden obtener estadísticas de a qué dominios se están enviando paquetes o de dónde se están recibiendo los paquetes, esta es una utilidad muy buena, ya que se puede saber si un equipo de la organización ha sido infectado por algún *malware* y está generando tráfico en la red, tratando de enlazarse con un servidor malicioso, lo cual mostraría una anormal cantidad de datos enviados al dominio que quiere conectarse véase figura 4.18.

Statistics for all Domains

Name	Location	TCP/IP				ICMP				Graphs
		Total				TCP		UDP		IPv4		IPv6		
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	
google.com		13.0 KBytes	0.1%	2.8 KBytes	0.0%	13.0 KBytes	2.8 KBytes	0	0	0	0	0	0	
iqnection.com		2.6 KBytes	0.0%	22.4 KBytes	0.0%	0	0	2.6 KBytes	22.4 KBytes	0	0	0	0	
		6.9 MBytes	59.1%	10[illegible]3 MBytes	71.4%	0	0	0	0	0	0	0	0	
1e100.net		1.1 KBytes	0.0%	[illegible]5 KBytes	0.0%	1.1 KBytes	1.5 KBytes	0	0	0	0	0	0	
clients.google.com		3.9 MBytes	32.9%	90.1 KBytes	0.1%	3.5 MBytes	90.1 KBytes	0	0	0	0	0	0	
googleapis.com		8.6 KBytes	0.1%	[illegible]3 KBytes	0.0%	8.6 KBytes	8.3 KBytes	0	0	0	0	0	0	
example.com		813.7 KBytes	6.8%	4[illegible]3 MBytes	28.5%	760.3 KBytes	31.8 KBytes	51.6 KBytes	37.2 KBytes	634	74	0	0	
[illegible]static.com		120.8 KBytes	1.0%	8.9 KBytes	0.0%	94.6 KBytes	8.9 KBytes	0	0	0	0	0	0	

Figura 4.18 Estadística de los dominios con los que se tiene conexión.

También se pueden obtener gráficas por hora para identificar los hosts que están provocando más tráfico en la red, esto puede ayudar a la organización a detectar algún equipo que ha sido comprometido, o algún usuario malintencionado o sin intención que esté ocupando mucho ancho de banda, véase figura 4.19.

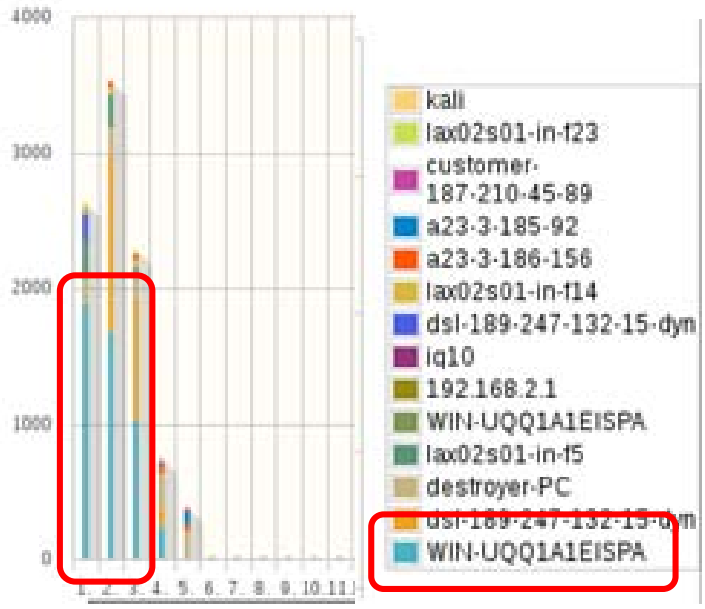


Figura 4.19 Gráfica de la red

4.6.1.2 Resultado

Ntop es una herramienta gratuita y fácil de usar que permite identificar rápidamente alguna anomalía, es muy útil para auditar la red, ya que se puede saber rápidamente que equipo o servidor dentro de la organización tiene un comportamiento raro y que podría presentar un riesgo para los intereses de la empresa, por lo tanto poder tomar acciones para solucionar el problema.

4.7.1.1 Caso práctico No. 4.2

Wireshark es una herramienta de propósito variado, en este caso se utilizó para detectar un posible *malware* que se aloja en un equipo de la red virtualizada, esta situación se podría presentar en cualquier organización y lo importante es darle solución.

Para realizar este análisis se procedió a colocar el *malware* en un entorno controlado, en este caso una máquina virtual con Windows XP o 7 sin internet y con un sistema kali Linux que posee una herramienta llamada *honeypot* que permite engañar al malware, permitiendo que se conecte a la *honey* en vez del servidor real al que se quiere conectar.

Se procedió a seleccionar la interfaz por la que wireshark debía capturar los paquetes, de tal manera que al iniciar la captura, se pueden filtrar los paquetes de acuerdo a la necesidad de quien analice la actividad del *malware*, véase figura 4.20.

Figura 4.20 Selección de interfaz para la captura de paquetes de red

Por medio de wireshark se puede reconocer a qué servidores se quiere conecta el malware a través de peticiones DNS, para observar con más comodidad se puede aplicar un filtro para el protocolo de "DNS", véase figura 4.21.

Figura 4.21 Filtro DNS

Otro aspecto que se debe tomar en cuenta al analizar y determinar si se trata de un malware, es ver las peticiones realizadas a algún servidor desconocido, por medio de los métodos Post y Get del protocolo HTTP. (véase la figura 4.22)

Figura 4.22 Método GET

4.7.1.2 Resultado

El emular el entorno donde se puede ejecutar el *malware* es la parte laboriosa, la parte interesante del caso es observar por medio de wireshark el comportamiento del proceso que se está ejecutando para determinar si se trata de un *malware* o es algún otro proceso benigno que genera tráfico en la red, lo cual puede darse el caso real en una organización, lo anterior permite obtener un diagnóstico más certero de lo que ocurre en el equipo posiblemente comprometido de la red de una PyME, como solución alternativa contra infecciones por malware se recomienda la instalación de software antivirus en su versión gratuita, los mejores antivirus gratuitos son de los de la compañía Avast y AVG.

Capítulo V
Gestión e implementación de seguridad

5.1 Introducción

Existen mecanismos que además de ayudar a detectar los fallos ayudan a colocar una capa más en la seguridad de la infraestructura de una organización, una herramienta muy útil es un UTM que proveen de varias soluciones y provienen de ataques que llegue de afuera de la infraestructura hacia adentro o viceversa, además hay sistemas de gestión de seguridad, que proporcionan controles y políticas de seguridad para la adecuada administración de información y reducción de riesgos.

5.2 Mecanismos para mejorar seguridad informática

Existen diferentes técnicas y servicios que ayudan a mejorar los niveles de seguridad en una organización, estos son: identificación de usuarios, políticas de contraseñas, control de accesos, copias de seguridad, centros de respaldos, cifrado en las comunicación, protocolos seguros, análisis y filtrado de tráfico en la red, servidores proxy, sistemas de detecciones de intrusos, antivirus, principalmente.

5.2.1 Políticas de seguridad y procedimientos de seguridad

Política de seguridad: [2] "*Es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y eliminar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran*".
Procedimiento de seguridad: es la definición detallada de los pasos a ejecutar para llevar a cabo tareas determinadas. Los procedimientos de seguridad permiten aplicar e implantar las políticas de seguridad que han sido aprobadas por una organización, describiendo cuáles son las actividades que se tiene que realizar en el sistema, en qué momento o lugar, quiénes deben ser los responsables y cuáles son los controles aplicables para supervisar su correcta ejecución.

Políticas	Procedimiento	Tarea a realizar
Protección de un servidor Web de la organización contra accesos no autorizados.	Actualización del software del servidor web.	-Revisión diaria de las actualizaciones publicadas por el fabricante. -Seguimiento de las noticias sobre los posibles fallos de seguridad.
	Revisión de los registros de actividad en el servidor.	-Revisión semanal de los "logs" del servidor para detectar situaciones anormales.

		-Configuración de alertas de seguridad que permiten reaccionar de forma urgente ante determinados tipos de ataques e intentos de intrusión.

Tabla 5.1 Políticas de seguridad

5.2.2 Respuesta a incidentes de seguridad

La organización debe definir un procedimiento que permita actuar al momento que ocurra un incidente de seguridad, de modo que pueda realizar una serie de actividades previamente establecidas para controlar y limitar el impacto del incidente. Las políticas de seguridad pueden definir que herramientas se van a utilizar para facilitar la detección y la respuesta rápida ante los incidentes.

5.2.3 Herramientas de seguridad Física

Son [2] "*Aplicaciones de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial." En otras palabras son los controles y mecanismos que están dentro o alrededor de la infraestructura de la organización así como los medios de acceso remoto, implementados para proteger el hardware y los medios de almacenamiento.*

5.3 UTM

La seguridad en capas básicamente se refiere a las distintas protecciones en cada nivel, entre más niveles haya se puede decir que está más protegido el sistemas informático aunque debe haber un equilibrio, por lo tanto una capa extra de seguridad en una infraestructura de TI de una organización puede ser por medio de un UTM, es una herramienta que unifica varias herramienta de seguridad, en otra palabras es un solución todo en uno, posee herramientas como antivirus, antispam, detector de intrusos, antiphising, filtrado web, VPN, firewall, entre las principales herramientas. Estos servidores o firewall de seguridad perimetral funciona en modo proxy (procesa y redirige el tráfico interno) o en modo transparente (procesa el tráfico y analiza los paquetes en tiempo real) para el usuario.

5.3.1 Untangle

Es una solución de seguridad perimetral multifuncional que engloba en un único servidor varias soluciones de seguridad, es una distribución de código abierto basada en Debian. Es un UTM óptimo para las pequeñas y medianas empresa, ya que centralizan toda la gestión de seguridad de red en una única consola de administración vía web.

5.3.1.1 Requerimientos, ventajas y desventajas

Los requerimientos para poder hacer que el servidor funcione adecuadamente (tabla 5.1), de acuerdo a la necesidad de la organización es el siguiente:

Usuarios	Procesador	Memoria	Disco duro	NICs	Arquitectura
1-50	Atom/P4 equivalente o mayor	1 GB	80 GB	2 o más	32 bits
51-150	Dual Core	2 GB	80 GB	2 o más	32 bits
151-500	2 o más Cores	2 o más GB	80 GB	2 o más	32 bits
501-1500	4 Cores	4 GB	80 GB	2 o más	64 bits
1501-5000	4 o más Cores	4 o más GB	80 GB	2 o más	64 bits

Tabla 5.1 Requerimientos para Untagle

Ventajas:

-Sustituye a varias herramientas de seguridad por una sola, facilitando la gestión de seguridad.
-Solo se realiza un gasto para la organización.

Desventajas:

-Si falla la herramienta queda desprotegida la organización.
Módulos de Untangle de la versión libre, tabla 5.2.

Protección	
Virus Blocker Lite	1
Firewall	1
Intrusion Prevention	1

Phish Blocker	1
Spyware Blocker	1
Attack Blocker	1
Filtro	
Web Filter Lite	1
Spam Blocker Lite	1
Application Control Lite	1
Ad Blocker	1
Conexión	
OpenVPN	1
Captive Portal	1
Reports	1

Tabla 5.2 Módulos de untagle

5.4 Módulos de untangle

Las herramientas de untangle son muy sencillas de utilizar, y proporcionan una interfaz web que centraliza y facilita la gestión del firewall perimetral.

a) Web filter

Este módulo se encarga de filtrar el tráfico web que llega a red interna de la organización, bloquea contenidos inapropiados y monitorea el contenido que acceden los usuarios, el módulo utiliza varias técnicas de filtrado basándose en diferentes patrones, de este modo, se puede determinar que contenido es inadecuado, véase figura 5.1. Los diferentes patrones que se usan para determinar que un contenido es inadecuado son:

-Categorías de páginas web según su contenido.
-Lista de sitios bloqueados.
-Lista de sitios permitidos.
-Lista de direcciones IP con acceso permitido.
-Filtrado de ficheros por cabecera MIME.
-Filtrado de ficheros por tipos de archivo.

Figura 5.1 Listas de bloqueo

Configuración

Para editar las categorías solo se tiene que seleccionar la categoría que se quiere bloquear, el *flag* es para que se guarde el registro del acceso o intento de entrar a los sitios web no permitidos, véase figura 5.2.

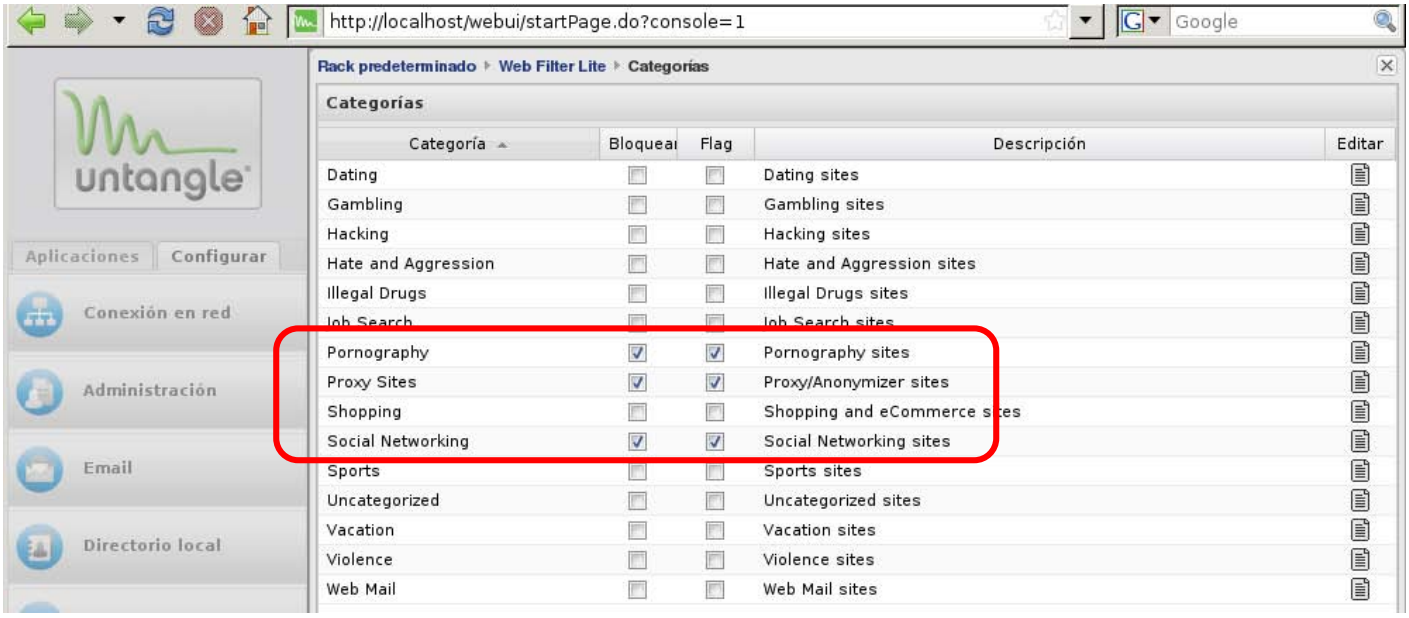


Figura 5.2 Categorías

Para editar el sitio web explícitamente se agrega la dirección URL que se quiere bloquear o simplemente que se guarde el registro, en todo caso ambas opciones y una descripción, véase figura 5.3.

Figura 5.3 Adicionar un sitio para ser bloqueado

Para evitar las descarga de archivos por medio de su extensión, se tienen que seleccionar las extensiones de los archivos que se van a bloquear y el *flag* si se desea que se guarde un registro, figura 5.4.

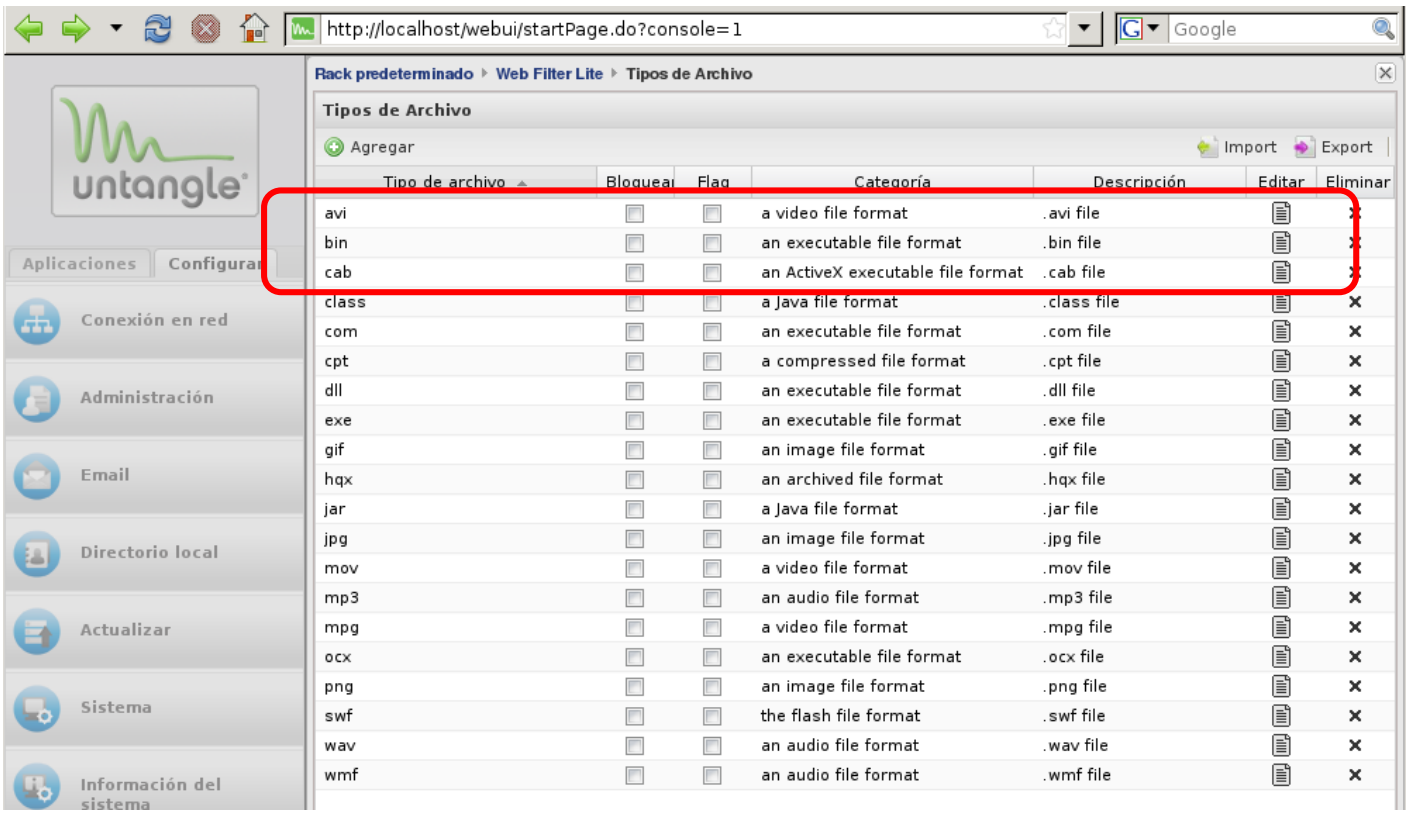


Figura 5.4 Tipos de archivos que se pueden bloquear

Para la siguiente opción se elige el MIME del archivo a bloquear, esta opción permite anticipar la descarga de ciertos archivos que no llevan extensión y quieran engañar al filtro, figura 5.5.

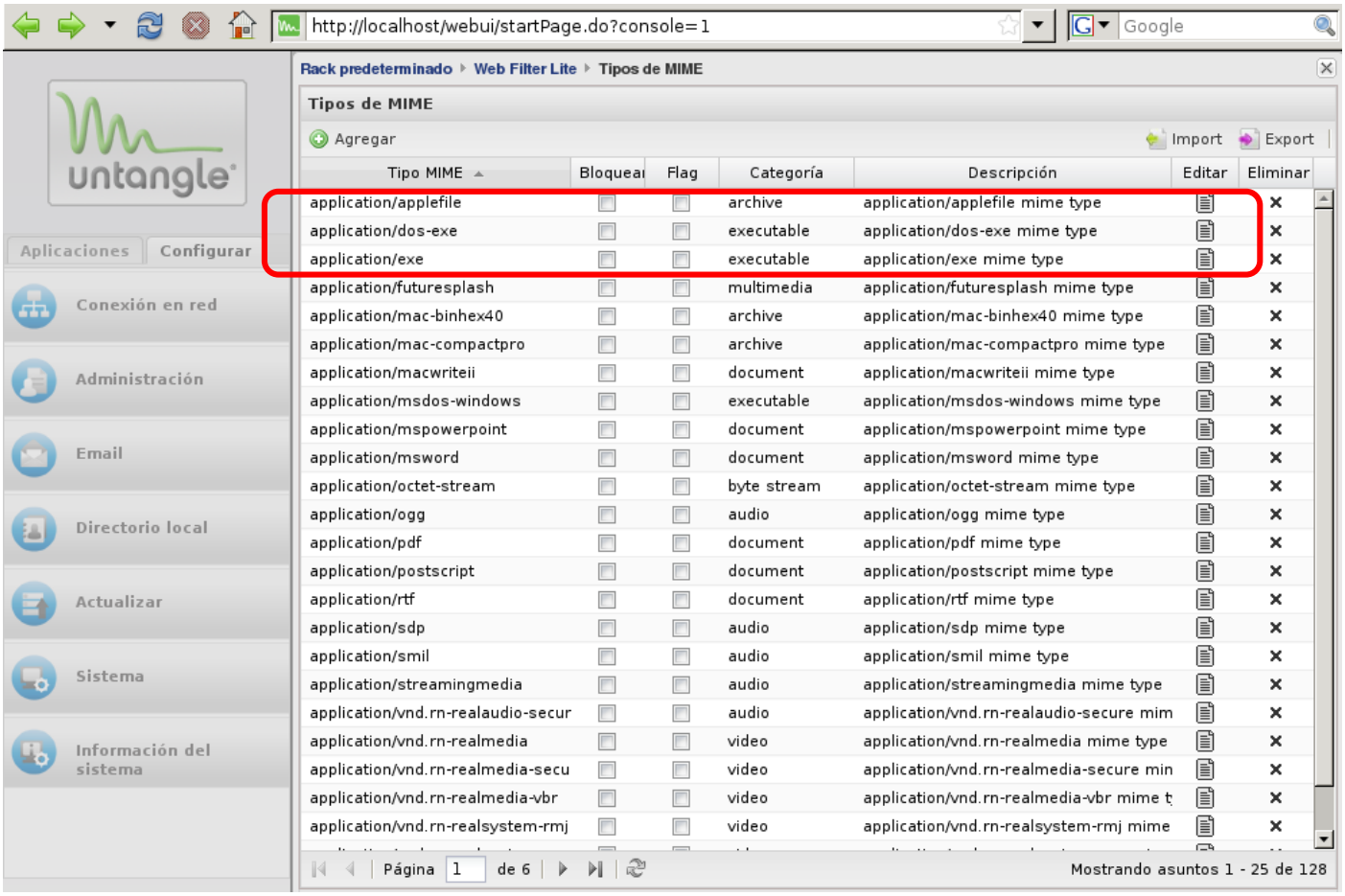


Figura 5.5 Tipos de MIME

Listas permitidas es donde se configura todo aquello que se permita, en *edit passed sites* se coloca la IP que se desea permitir y un breve descripción, y el *edit passed client IPs* es la IP del cliente que va estar permitido para acceder a los recursos de la red, figura 5.6.

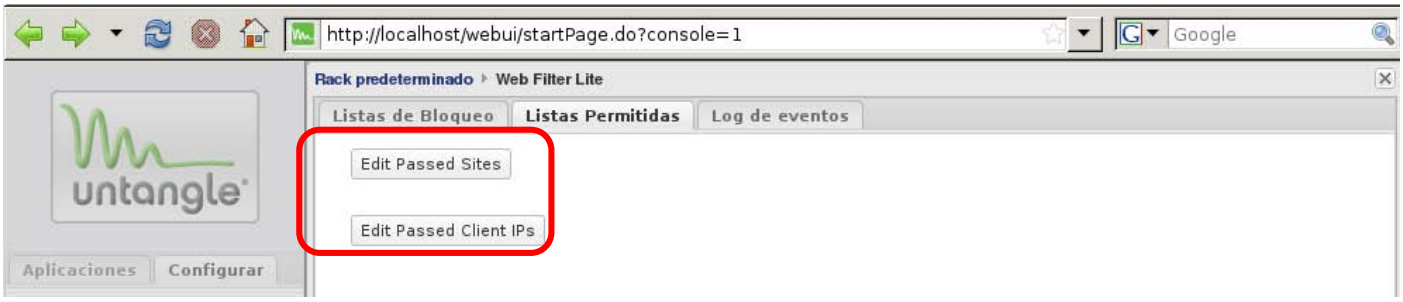


Figura 5.6 Opción de listas permitidas

Si un usuario trata de acceder a alguna página bloqueada por el módulo de *web filter*, le aparecerá una página similar con una pequeña explicación de lo que ocurrió, como se muestra en la figura 5.7.

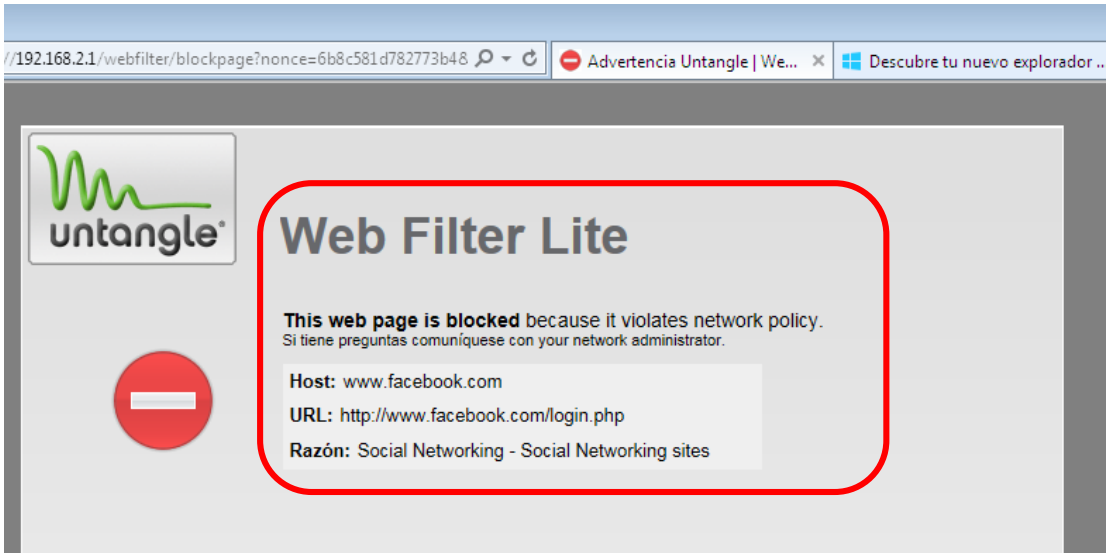


Figura 5.7 Bloqueo de página

Como se observa en la imagen, en el tiempo en que se realizó la prueba se tuvieron 239 violaciones a algunas reglas configuradas en el módulo, pero solo 50 violaciones de las reglas se bloquearon figura 5.8.

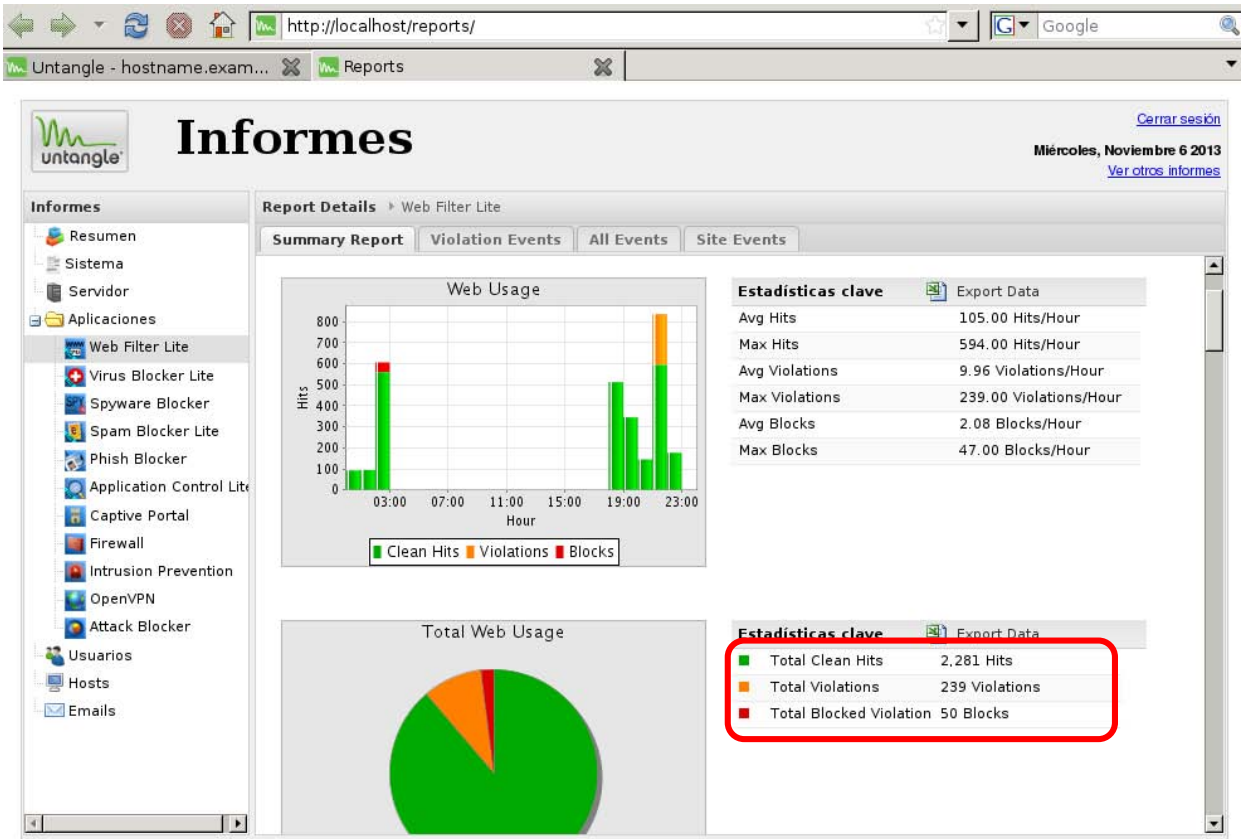


Figura 5.8 Reporte del módulos web filter

b) Virus Blocker

Este módulo de Untangle permite detener los ataques de virus antes de que lleguen a los usuarios de escritorio, posee una interfaz gráfica de usuario intuitiva, con la capacidad de escanear múltiples protocolos y actualizaciones regulares, por lo que siempre se tiene la protección más actualizada.

Protege a los usuarios de amenazas como: virus, gusanos, troyanos o malware en la web, correo electrónico y en protocolos de transferencia de archivos comunes, además de analizar archivos y archivos comprimidos como ZIP, RAR, Tar, principalmente.

Configuración

Este módulo posee la opción de análisis de tráfico, de modo que el antivirus analizará todas las páginas web que los usuarios de la red de la organización visiten, en busca de malware, figura 5.9

Figura 5.9 Opción de red

También se puede habilitar el análisis de tráfico de SMTP, POP3 e IMAP de modo de que el antivirus analiza todos los correo electrónicos enviados y recibidos a través de estos protocolos, figura 5.10.

Figura 5.10 Opción de Email

Para el análisis de FTP se puede habilitar la opción dedicada, de modo de que el antivirus analiza todos los archivos cargados desde la red de la organización o descargados, a través de este protocolo, figura 5.11.

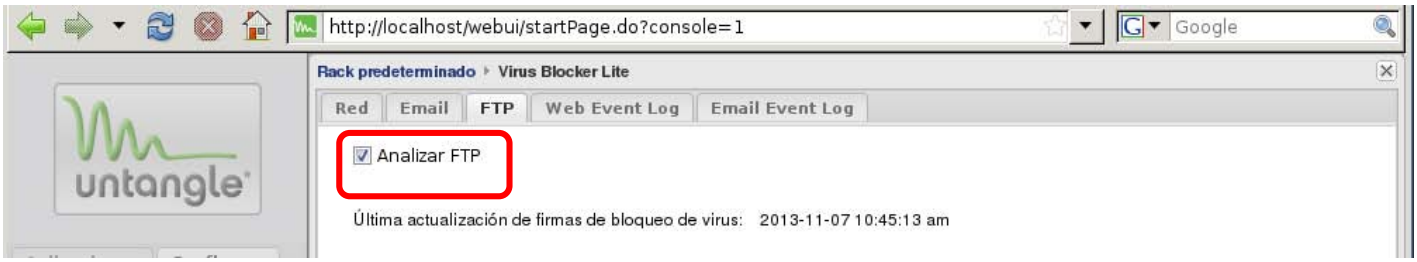


Figura 5.11 Opción FTP

En la siguiente imagen se puede ver el resultado del módulo *Virus blocker* el cual ha escaneado 2547 documentos y no se detectó ni bloqueo de algún virus, figura 5.12

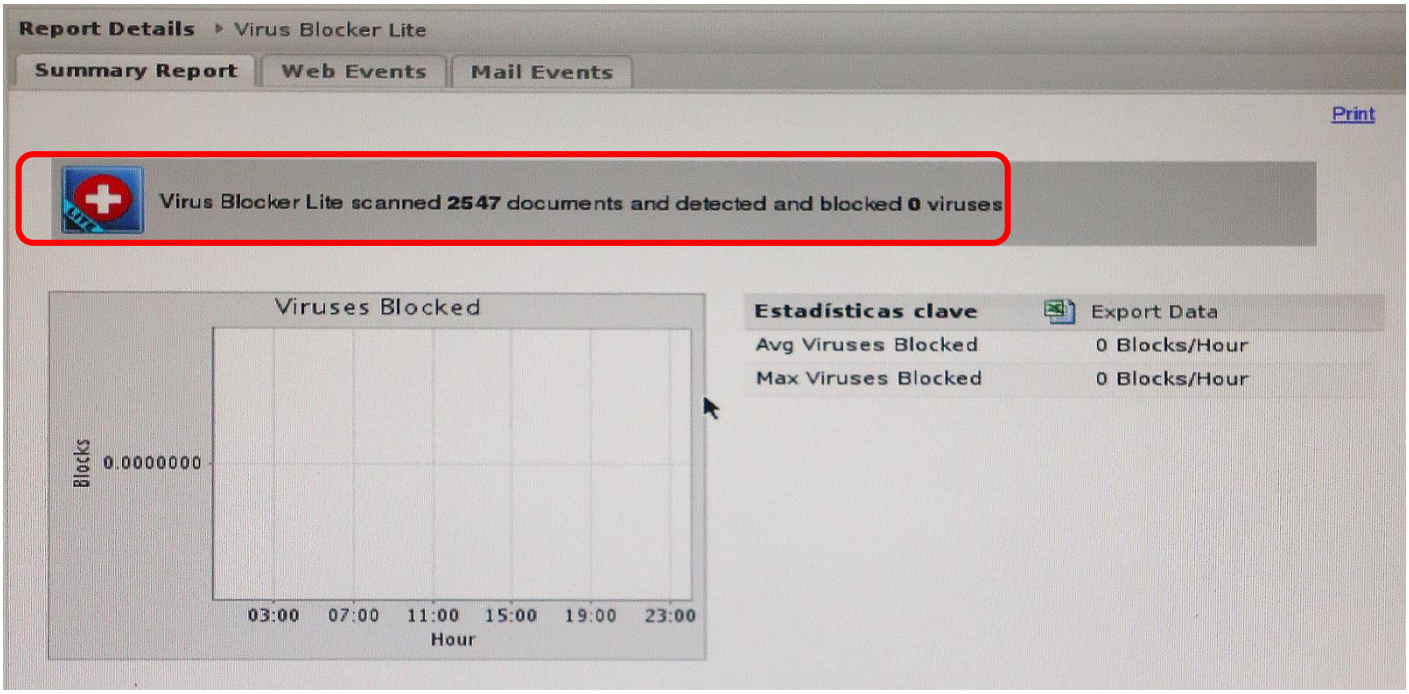


Figura 5.12 Reporte del módulo web

c) Spyware Blocker

Este módulo se encarga de analizar todo el tráfico web, para detectar si contiene algún software espía. Si un spyware trata de infiltrarse a la red de la organización el módulo estaría bloqueándolo antes de que llegue al usuario.

Este módulo utiliza actualizaciones para estar al día con el surgimiento de nuevos spywares, proporciona listas negras para bloquear sitios web que contienen software espía, otra característica es que bloquea los controles ActiveX dañinos que sabe que son spywares, examina las direcciones IP de los sitios web que los usuarios visitan, y compara las direcciones IP con una lista de subredes ofensivas.

Configuración

La opción web permite bloquear el acceso a páginas en las que se detecte el uso de software espía o publicidad. Para activar la opción solo se selecciona la casilla “Bloquear la URL” del *spyware* y publicidad.

La opción de *cookies* permite bloquear el uso de *cookies*, que se instalan en las computadoras para rastrear la navegación del usuario y enviar publicidad.

La opción ActiveX bloquea los controles ActiveX sospechosos que intenten cargarse en ciertas páginas web, estos controles se usan en principalmente en páginas multimedia.

La opción de tráfico permite que se analice el tráfico de todo el segmento de red de la organización en busca de comportamientos que correspondan a un *spyware* que haya sido instalado en algún equipo, véase figura 5.13.

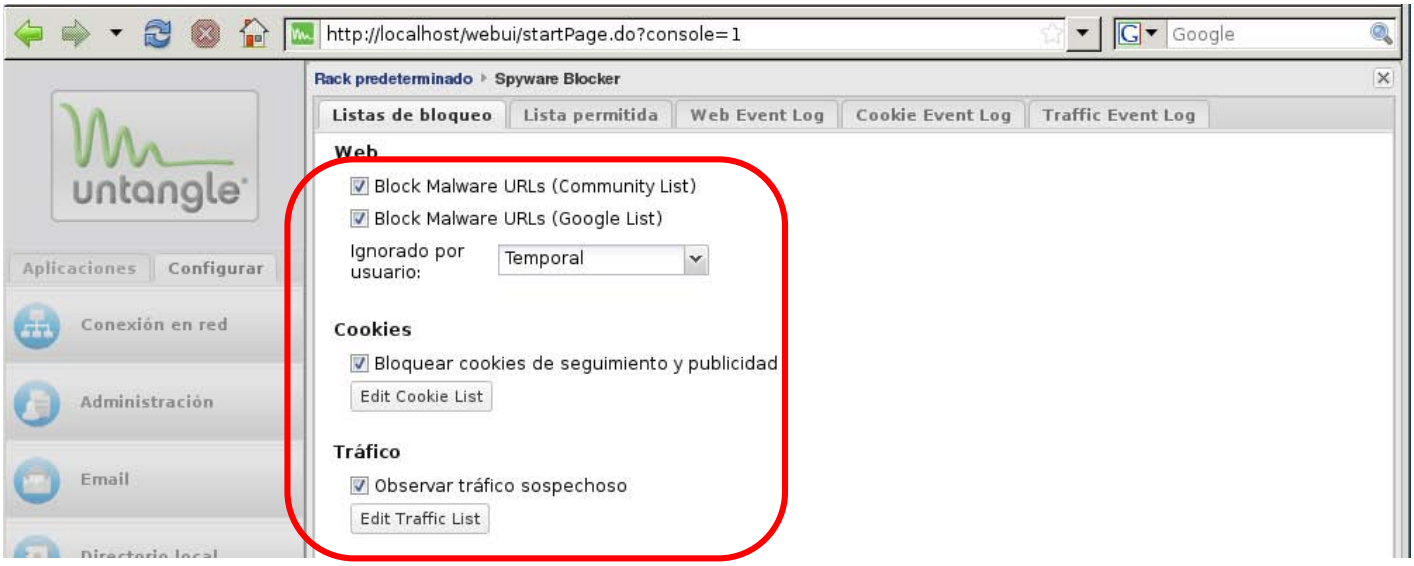


Figura 5.13 Opciones de Lista de bloqueo

En este informe del módulo de *spyware blocker* se observa que se han bloquedo 3 posibles *spywares*, vease figura 5.14.

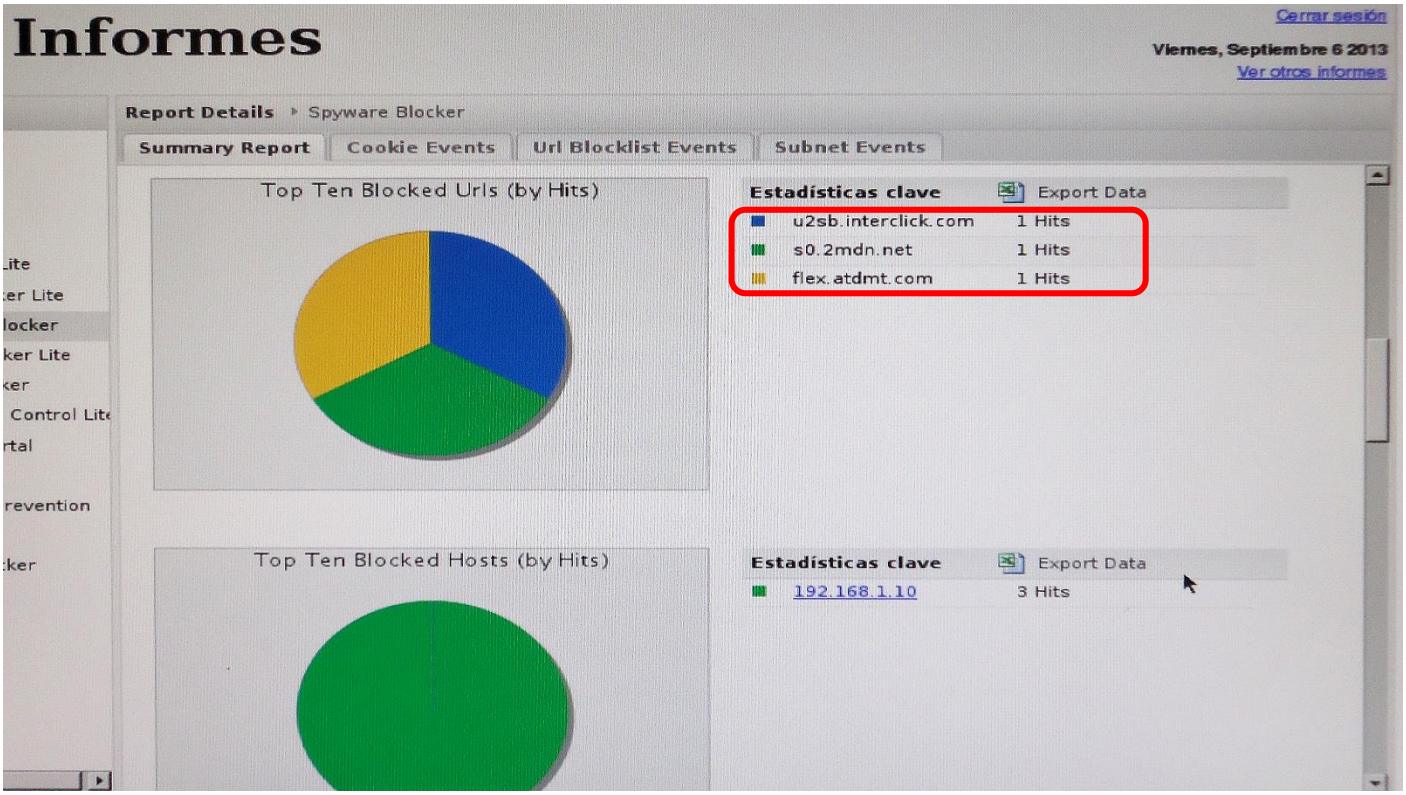


Figura 5.14 Reporte de módulo Spyware Blocker

d) Attack Blocker

Es un módulo que se encarga de evitar ataques de negación de servicio y otros ataques similares, además de crear lista de excepciones de usuarios que pueden comportarse de manera agresiva, separando el tráfico bueno del malo, y si la red está bajo ataque asigna recursos cuidadosamente a los usuarios legítimos.

Configuración

"Estado" es una opción en la que se puede ver el estatus actual del módulo, pero no permite ningún tipo de configuración específica.

En la pestaña "excepciones" se listan las excepciones, esta opción se utiliza en el caso de que haya un segmento de red que comparta la misma dirección saliente (tráfico que pasa por NAT en un router). De modo contrario, el módulo *Attack Blocker* pensará que esa dirección está realizando un ataque de negación de servicio, véase figura 5.15

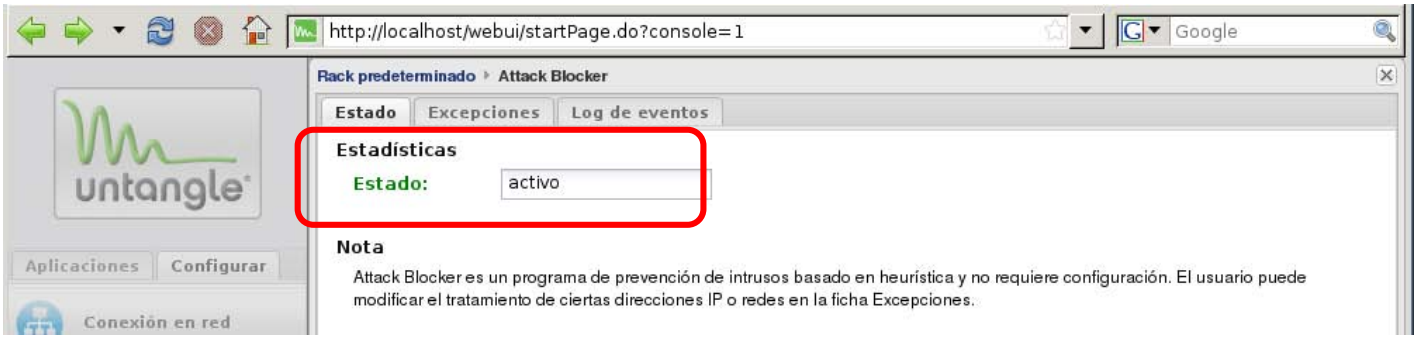


Figura 5.15 Opciones de estado del módulo Attack Blocker

En el reporte de attack blocker muestra que 3370 sesiones que fueron escaneadas, de las cuales 86 fueron limitadas y 124 descartadas, tambien se muestra una gráfica de las peticiones por minuto que se realizaron, en la prueba, véase figura 5.16.

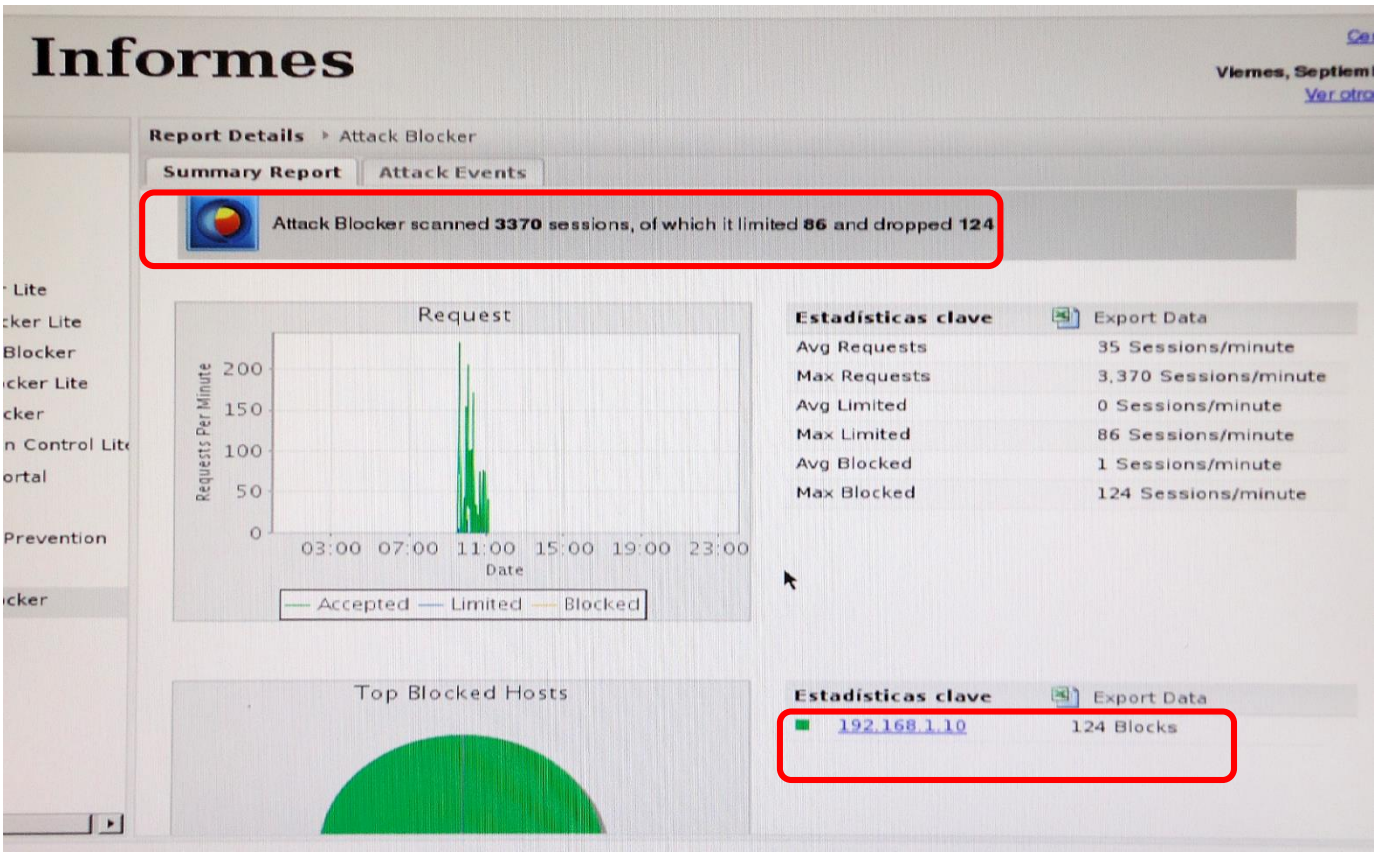


Figura 5.16 Reporte del módulo Attack Blocker

e) Firewall

Este módulo es un firewall que evalúa el tráfico que viaja a través de la red mediante la aplicación de sus reglas, además de la línea que separa a las redes internas y externas.

Se puede ejecutar como puente transparente para complementar los firewalls preexistentes, además permitir bloquear actividades no deseadas y proteger la red de la organización.

Configuración

En la pestaña de reglas se puede copiar, crear y editar nuevas reglas o políticas de filtrado para la red de una organización, para ello se debe pulsar el botón de agregar, y se muestra un formulario para crear una nueva regla, los campos que se pueden configurar son los siguientes: habilitar regla, descripción, medida, log, tipo de tráfico, interfaz de origen, interfaz de destino, dirección de origen, dirección de destino, puerto de origen y puerto de destino, véase figura 5.17.

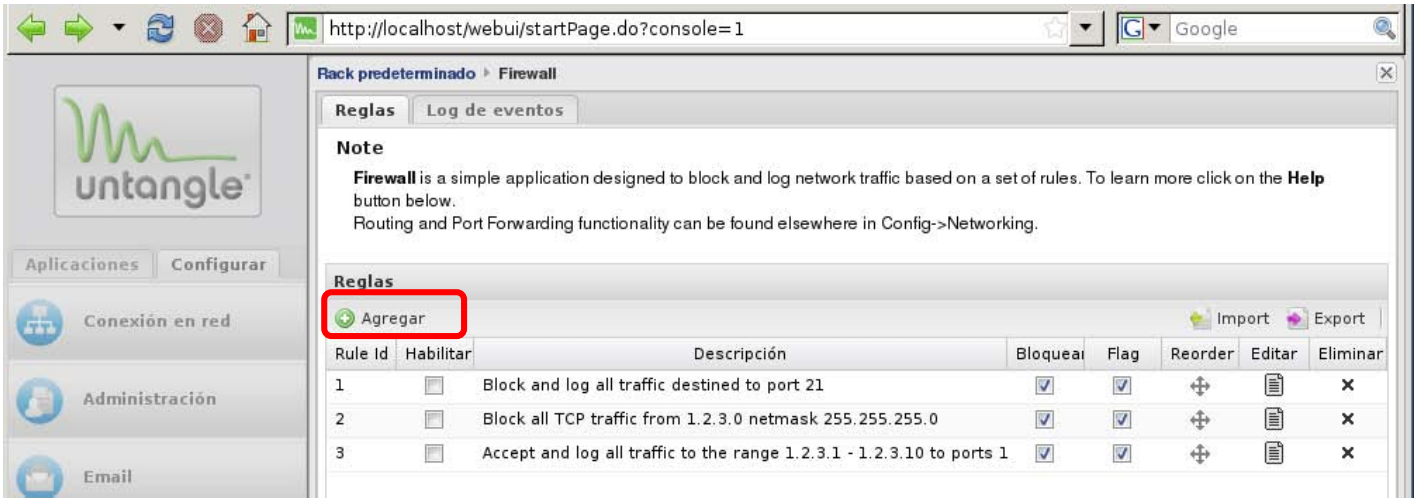


Figura 5.17 Opción Reglas del módulo de firewall

El reporte correspondiente al módulo de Firewall, muestra que no hubo bloqueos, véase figura 5.18

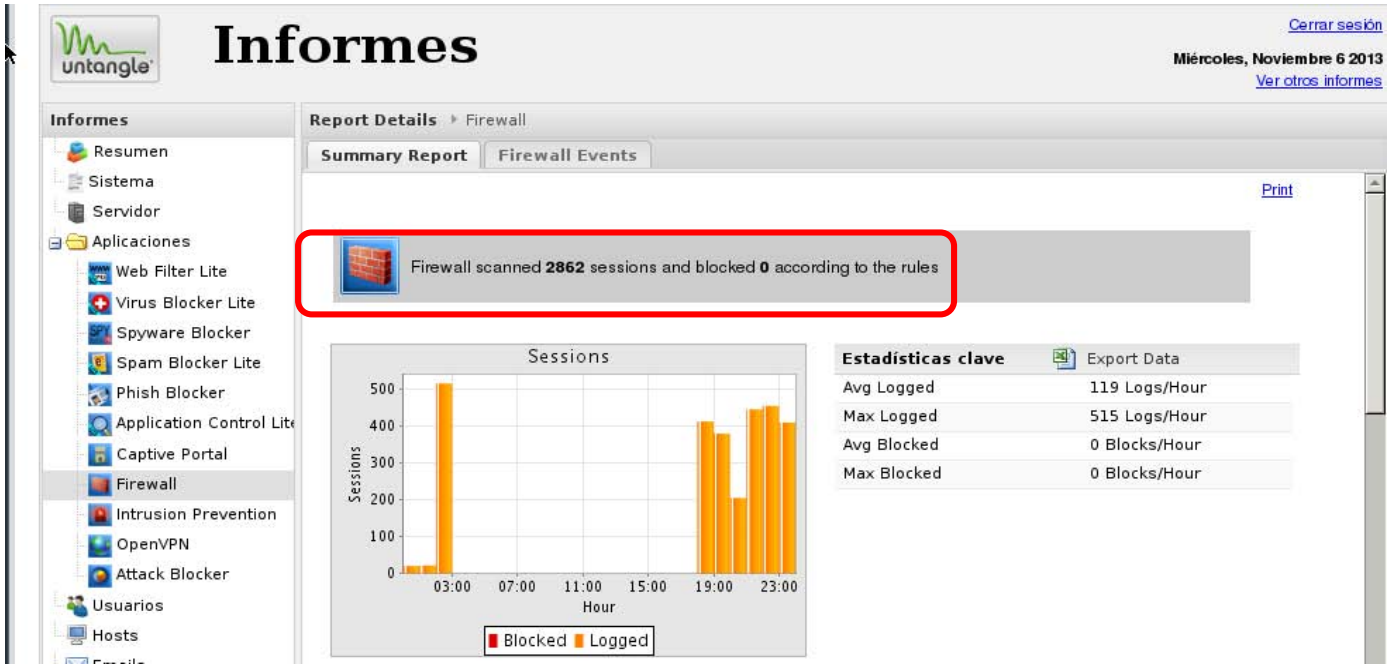


Figura 5.18 Reporte del módulo Firewall

f) Intrusion Prevention

El módulo de prevención de intrusiones (IPS) bloquea los intentos de *hacking* antes de que lleguen a los servidores internos y usuarios dentro de la organización. El IPS está basado en firmas pre-configuradas que hace a que sea más fácil para los administradores de proporcionar protección a la red de los *hackers* o *crackers*.

Configuración

En la pestaña de estado no se puede configurar ningún parámetro del módulo, únicamente se informa del estado del mismo y el número de firmas que se tiene disponibles, figura 5.19.

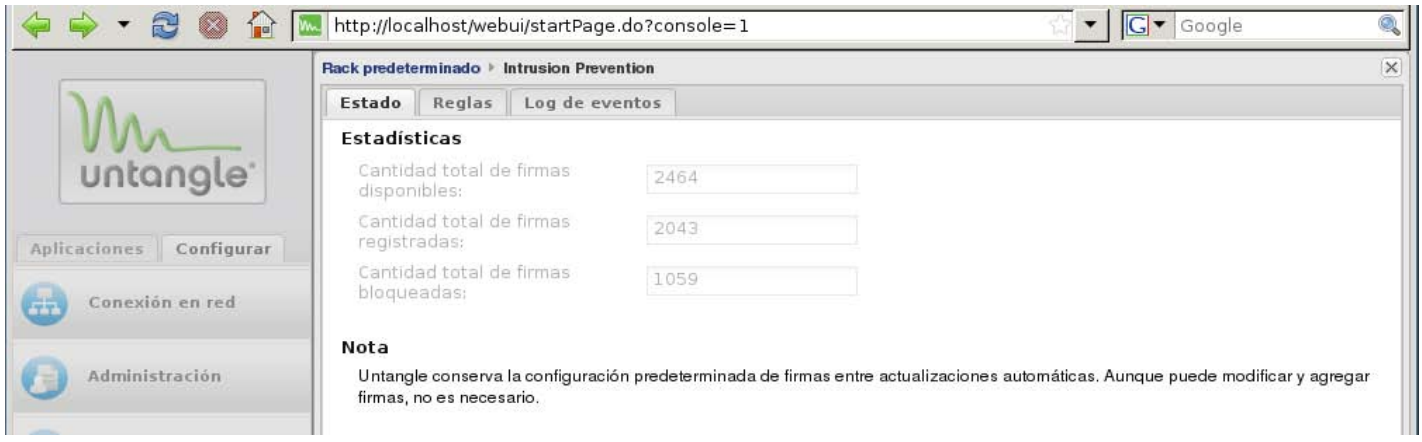


Figura 5.19 Opción de estado del módulo Intrusion Prevention

En la pestaña de reglas se analizan las reglas del sistema, y su comportamiento respecto al tipo de ataque detectado, marcando las casillas Bloquear y Log. Cabe destacar que las reglas se actualizan automáticamente, véase figura 5.22.

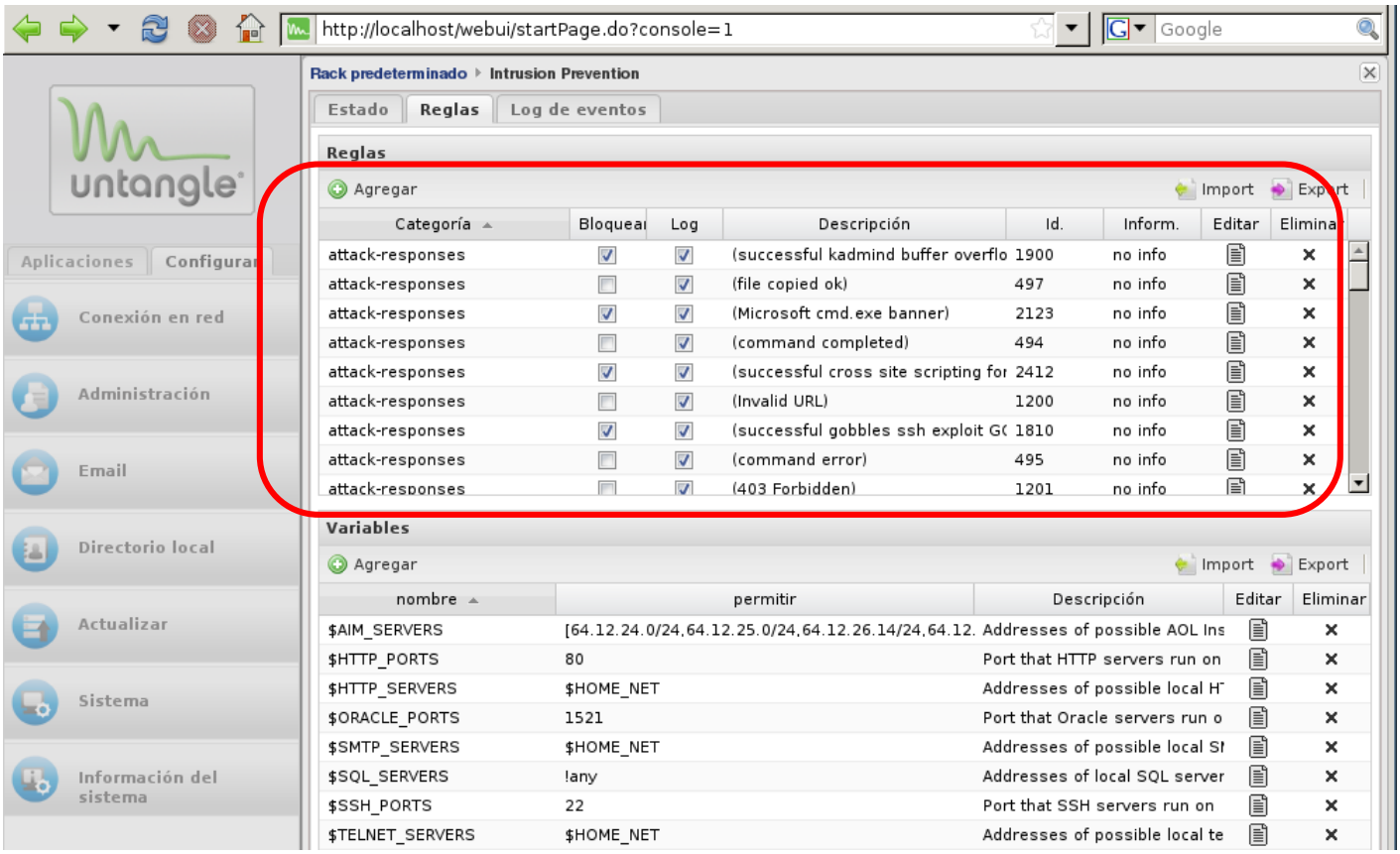


Figura 5.20 Opción Reglas del módulo Intrusion Prevention

El módulo de prevención de intrusiones muestra que se escanearon 2839 sesiones y que no se detectaron ni se bloquearon intrusiones, véase figura 5.21.

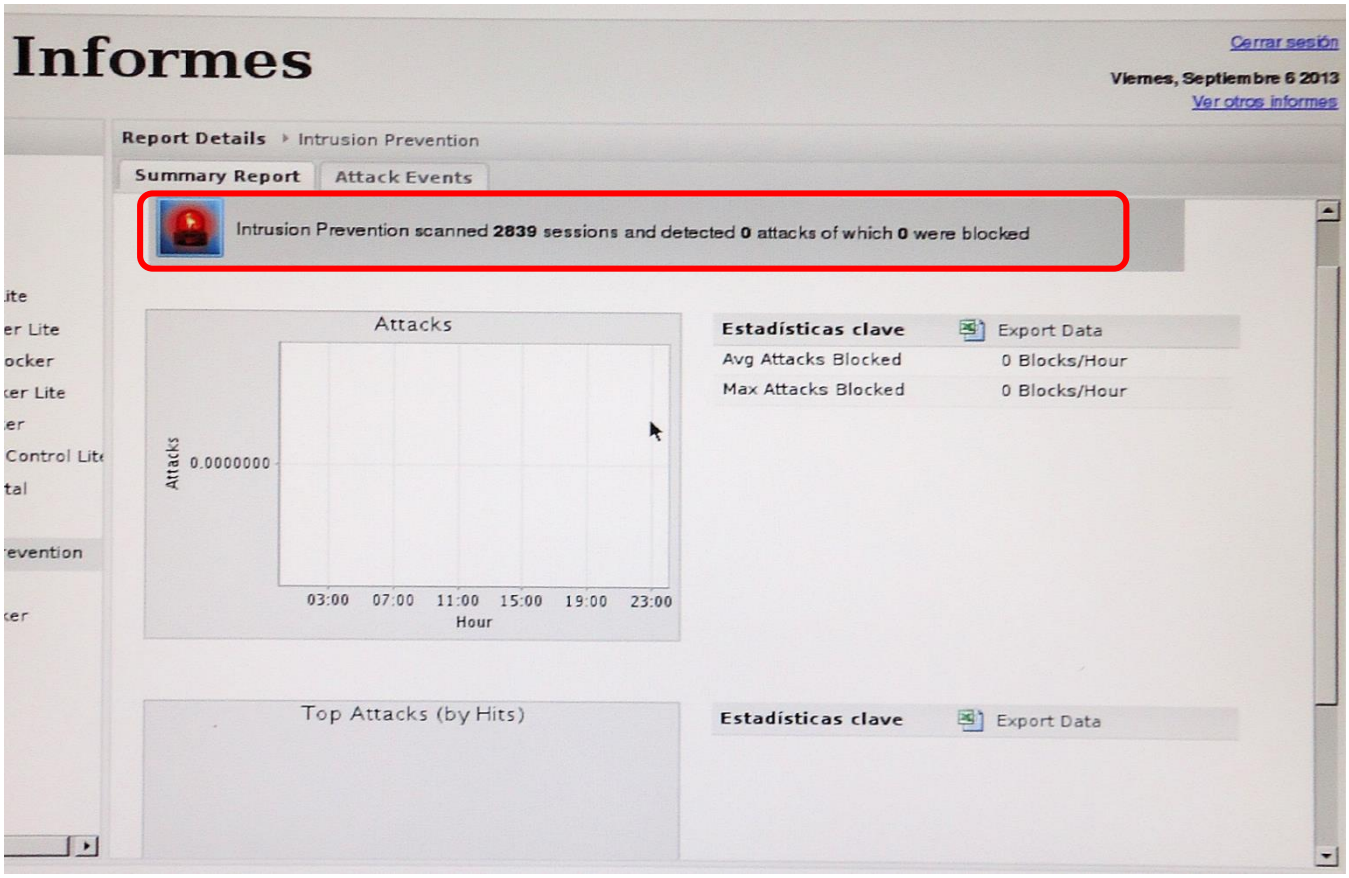


Figure 5.21 Reporte del módulo Intrusion Prevention

g) Spam Blocker

Es una herramienta que permite a los administradores bloquear el *spam* en el *gateway* antes de que llegue a los usuarios, también proporciona una interfaz gráfica para el administrador que facilita el filtro SMTP, POP y IMAP.

Filtrado basado en imágenes, escanea las imágenes en mensajes de correo electrónico para detener una técnica de *spamming* común. Los informes permiten tener una visión completa del correo no deseado en la red, incluyendo la fuente del correo no deseado, tendencias y estadísticas por usuario.

Configuración

En la pestaña de *email* se puede habilitar el análisis de tráfico SMTP, POP3 e IMAP, de este modo se pueden analizar todos los correos electrónicos recibidos y enviados mediante estos protocolos en busca de *spam*.

La opción de analizar correo SMTP es por si se tiene en la organización un servidor de correo local.

El correo descargado por POP3 e IMAP se analiza y se marca como spam en el momento de ser detectado como tal, figura 5.22.

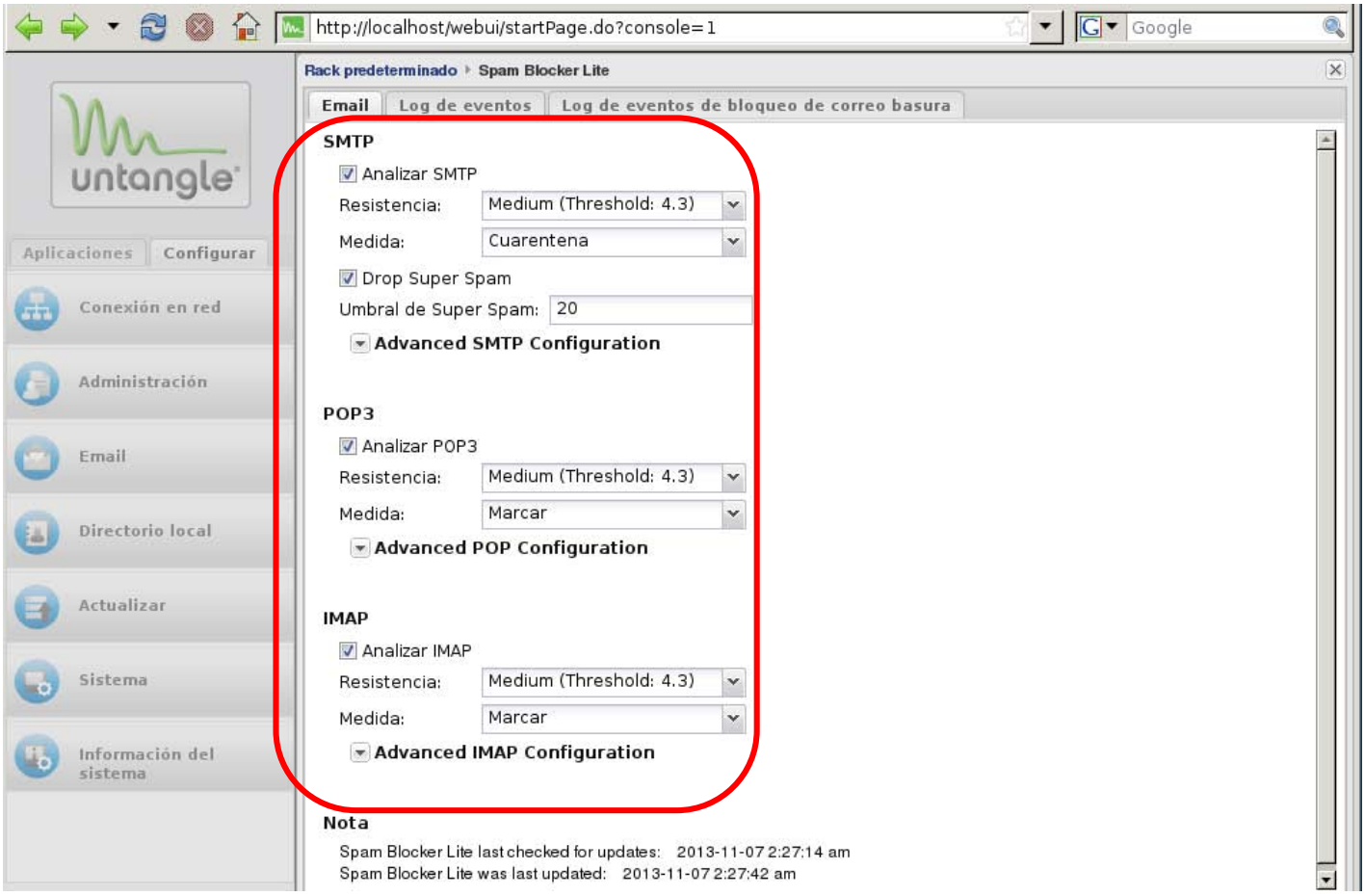


Figura 5.22 Opcion email del módulo Spam Blocker

A continuación se muestran los datos del reporte que se generó para el módulo de Spam Blocker, como se puede observar no hubo ningún correo *spam* que se haya detectado, véase figura 5.23 .

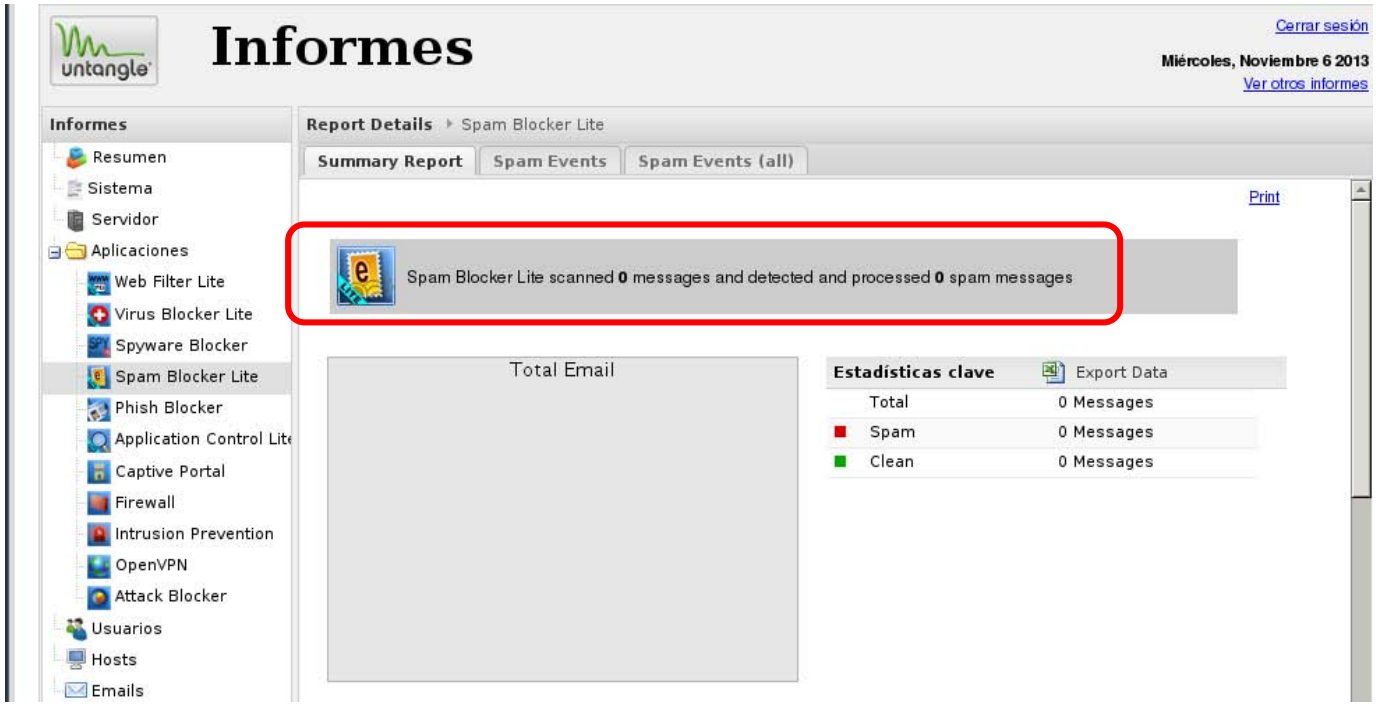


Figura 5.23 Reporte de Spam Blocker

h) Phish Blocker

El *Phish Blocker* permite que los usuarios de correo electrónico estén menos preocupados por los ataques de *phishing* y *pharming* de sitios web fraudulentos. Protege múltiples protocolos, como HTTP, SMTP, POP y IMAP escaneando cualquier correo electrónico transferido por estos protocolos y asegura que las firmas estén siempre al día con actualizaciones automáticas.

Configuración

En la pestaña de email, se puede seleccionar a que protocolos de correo se le puede aplicar el filtro de *Phish Bloker*. Para ello, únicamente se tiene que marcar la casilla de activar, que se encuentra delante de cada uno de los protocolos compatibles. La opción de SMTP es por si se tiene un servidor de correo local.

El correo descargado por protocolos POP3 o IMAP se analiza y se marca como ataques de *phishing* en el momento de ser detectado como tal. El correo marcado como *phishing* es recibido con el asunto modificado con la alerta de que el correo es malicioso, figura 5.24.

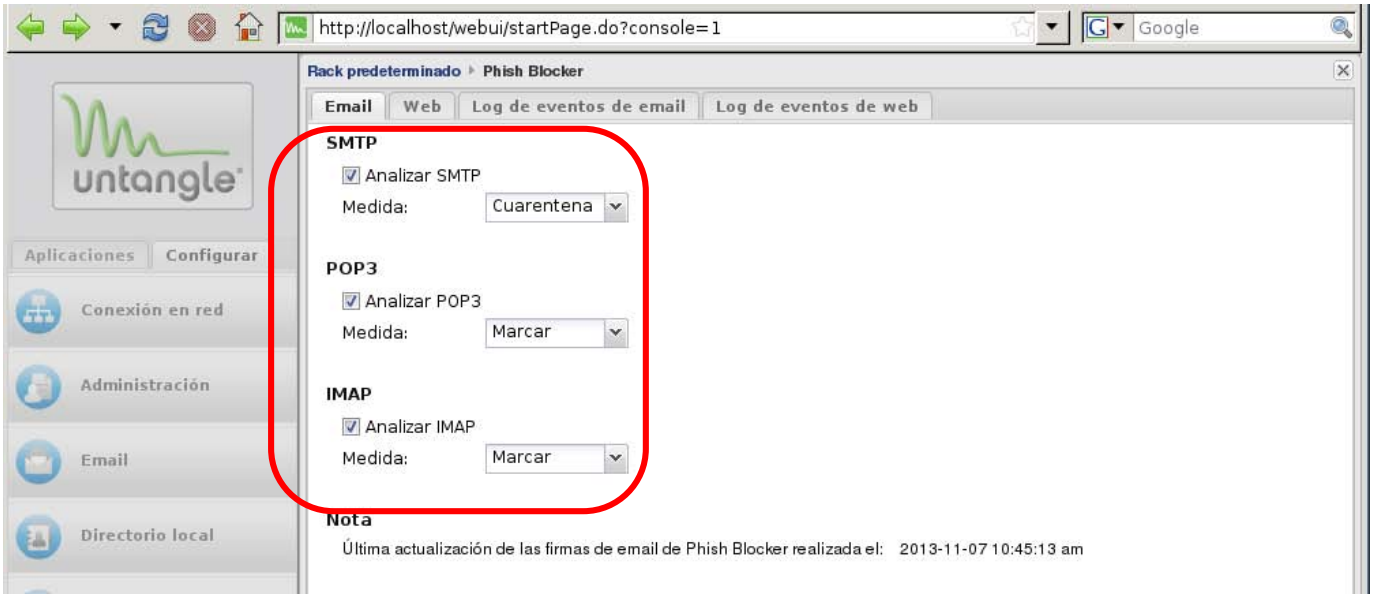


Figura 5.24 Opción email del módulo Phish Blocker

En la pestaña web se selecciona “Activar filtración de páginas web de *phishing*” si se desea que se analicen las páginas web en busca de *phishing* antes de mostrarlas a los usuarios de la red de la organización, véase figura 5.25.

Figura 5.25 Opción web del módulo Phish Blocker

Para el módulo de *Phish blocker*, no se detectó ningún *phishing* tanto en correos como en páginas que se descargaron, Figura 5.26.

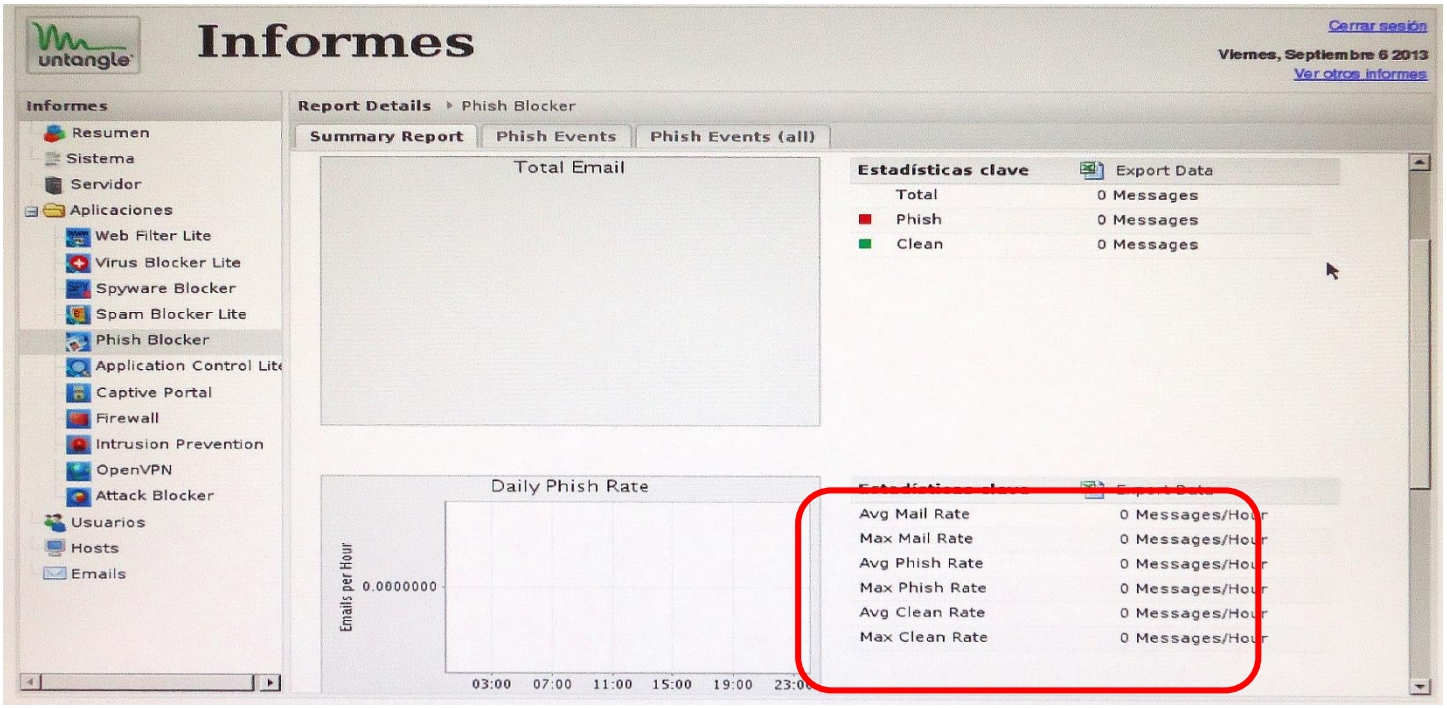


Figura 5.26 Reporte del módulo de Phish Blocker

Finalmente untangle ofrece un reporte general de los módulos que posse, para detectar rapidamente algun tipo de problema y darle solución, se muestra a continuación uno de estos reportes, véase figura 5.27.

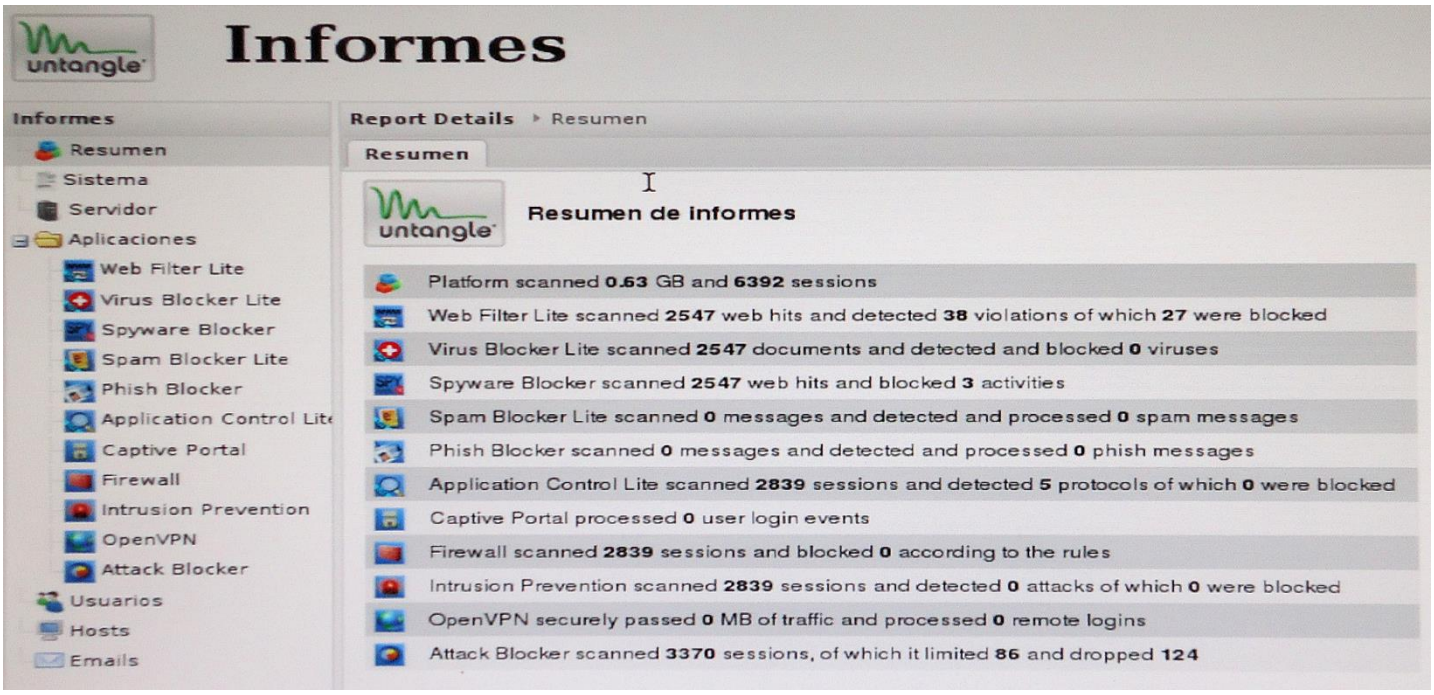


Figura 5.27 Resumen de informes de untangle

Conclusiones

Los incidentes que se producen al no parchar una vulnerabilidad en los sistemas informáticos de una empresa, pueden ir de los más leves, como la obtención de la contraseña de una red inalámbrica de la empresa, hasta el robo de información sensible que afecte la imagen de la organización, por lo cual, lo más sensato es detectar las fallas y darles una solución lo más pronto posible.

Por tanto en el presente trabajo de tesis se propusieron herramientas para descubrir vulnerabilidades, malas configuraciones en dispositivos de red y de análisis de tráfico, las cuales permitieron dar un diagnóstico de algunos fallos comunes que se pueden presentar en la red de una organización, con base a esto se generaron y recomendaron soluciones para parchar los huecos de seguridad que se encuentren.

Una de las soluciones derivadas de las pruebas realizadas al entorno virtualizado, fue reafirmar la importancia de instalar las últimas actualizaciones que el fabricante proporciona a sus sistemas operativos, con esto se pueden mitigan varias vulnerabilidades en los equipos y servidores que posea una PyME. Otra solución fácil de implementar, es la creación de políticas de contraseñas seguras que permita que las claves sean más robustas, de longitud mayor a 8 caracteres alfanuméricos o también una frase que sea fácil de recordar para el usuario.

Además, otra solución que se obtuvo con el trabajo de tesis fue la importancia que presenta la capacitación en cultura de seguridad informática que se les dé a los empleados de la empresa, ya que esta genera conciencia del adecuado y correcto manejo de los activos de la organización, sin dejar de lado la seguridad.

En cuanto a soluciones técnicas, se puede mencionar que hay distintas herramientas de seguridad, que se ofrecen en el mercado tanto de licencia comercial como libre, una propuesta es Untangle que ofrece una versión gratuita, de fácil configuración, implementación y completa, ya que incorpora múltiples funcionalidades en una sola máquina, es recomendable que la organización se ajuste a su presupuesto e identifique que activos son más importantes para ella.

Las PyME´s deben tener conciencia que las configuraciones y credenciales por default con las que vine un dispositivo de red o cualquier otro dispositivo, se pueden encontrar en internet, por lo que cambiar y personalizar la configuración de los dispositivos pone una primera barrara para evitar que atacantes los vulneren y modifiquen a su conveniencia.

Es importante que la organización este al pendiente del tráfico que entra o sale de su red, ya que con esto se pueden descubrir ataques, posibles infecciones de malware o usuarios que están usando indebidamente los recursos de red de la empresa, por lo que es indispensable una herramienta fácil de implementar como la que se mencionó en el trabajo de tesis, para identificar de manera general el problema que se presente y luego actuar para resolverlo.

Como parte de las contribuciones de este trabajo, se proporcionan los pasos para instalar y configurar la solución de Untangle (UTM), NTOP (analizador de tráfico de red) y Nessus (escáner de vulnerabilidades), así como la metodología de pruebas de penetración o auditorías de sistemas de informáticos, para la realización de las pruebas propuestas, según la serie de pasos que le sean más cómodos a la organización de seguir.

Además cabe destacar que el trabajar en un entorno de pruebas virtualizado, permite utilizar sistemas operativos y dispositivos de red a un bajo costo, sin la preocupación de afectar algún servicio informático, y sólo se necesita una computadora con al menos 8 gb de memoria RAM y un procesador con cuatro núcleos, instalar todo el entorno virtual propuesto, y ponerse a trabajar.

Se pretende que este trabajo sirva de referencia y base para posteriores aportaciones, ya que proporciona la flexibilidad de agregar más pruebas para evaluar otros puntos en los que puedan existir huecos de seguridad y generar la solución para el respectivo fallo, básicamente lo que se pretende es ampliar las pruebas para que el trabajo sea cada vez más robusto y pueda solucionar otros problemas relacionados con la seguridad informática tanto de los sistemas informáticos que posea la empresa como de su infraestructura de red.

Así, para darle continuidad al presente trabajo se pretende desarrollar un blog a través del cual se dé a conocer el trabajo aquí desarrollado y las mejoras que se vayan realizando, posteriormente se podrá colocar material de ayuda y temas relacionados con la seguridad informática, de manera que las PyME’s o incluso cualquier otro usuario que lo desee conocer, utilizar, implementar y consultar, asegurando la continuidad del negocio y el ahorro de costos por servicios de evaluación de seguridad para una organización o auxilie a los usuarios de internet.

ANEXO A Explotación de la vulnerabilidad ms08-067

La vulnerabilidad fue publicada en el año 2008, afecta al servicio de servidor y permite la ejecución remota de código sin autenticación. Los sistemas afectados son Windows 2000, Windows XP y Windows 2003.

Desarrollo

Se abre una terminal de comandos en Kali Linux.
En la terminal se introduce **msfconsole** figura A.1:

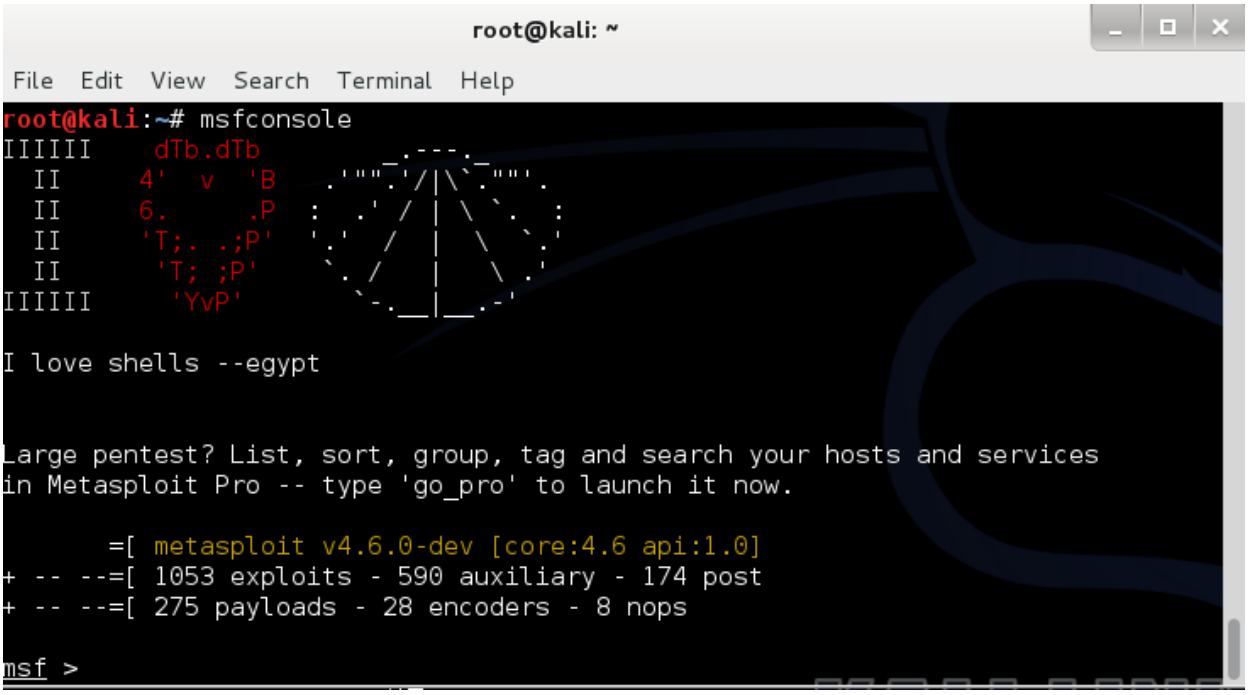
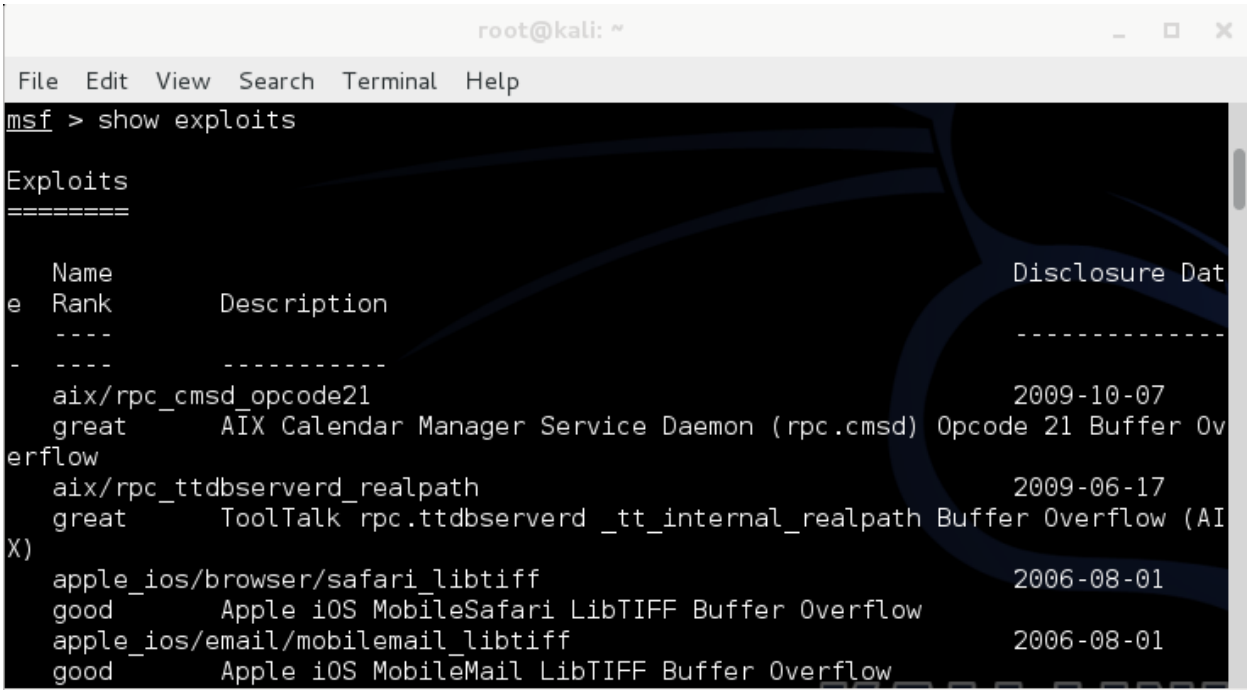


Figura A.1 Inicio de metasploit

Para visualizar los exploits disponibles se usa la opción **show exploits** Figura A.2:



Ficura A.2 Opción de metasploit show options

Para indicarle a metasploit que se va usar un exploit, solo se tiene que colocar el comando **use** seguido de un espacio y la ruta del exploit que se va a utilizar Figura A.3:

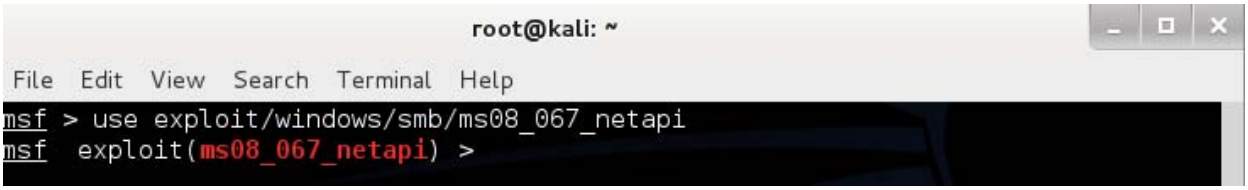


Figura A.3 Comando use de metasploit

Para configurar las opciones el exploit se coloca el comando **show options** Figura A.4.

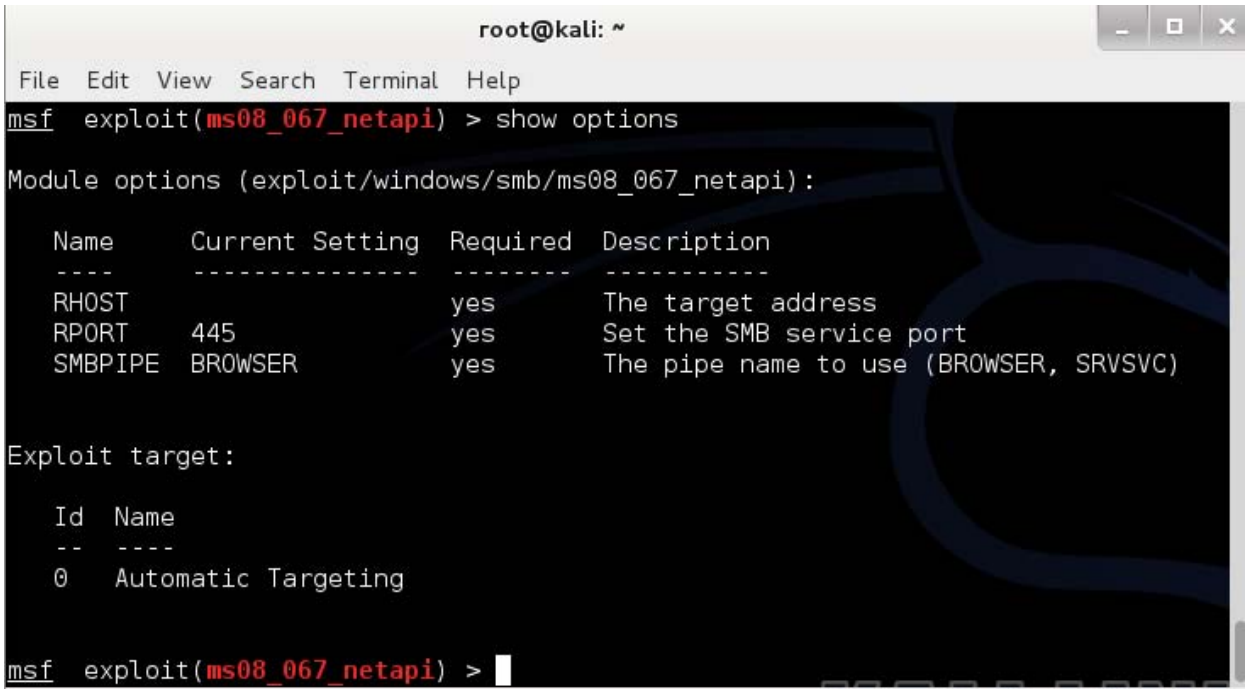


Figura A.4 Opciones a configurar de un exploit

Para este exploit se requiere la dirección IP del objetivo de evaluación (RHOST), el puerto SMB y el nombre del canal de comunicación. Por defecto ya se encuentran configurados los últimos dos parámetros requeridos, para configurar RHOST teclear la siguiente sentencia, véase Figura A.5:

Figura A.5 Configuración de ip en las opciones del exploit

Para la prueba de concepto se usa el payload bind TCP que es una parte muy importante en el exploit el cual pone una conexión en escucha e inyecta la DLL de meterpreter. Para configurar el payload introducir la siguiente sentencia mostrada, Figura A.6:

Figura A.6 Configuración de payload

Para ejecutar el exploit se debe introducir la sentencia **exploit** (Figura A.7):

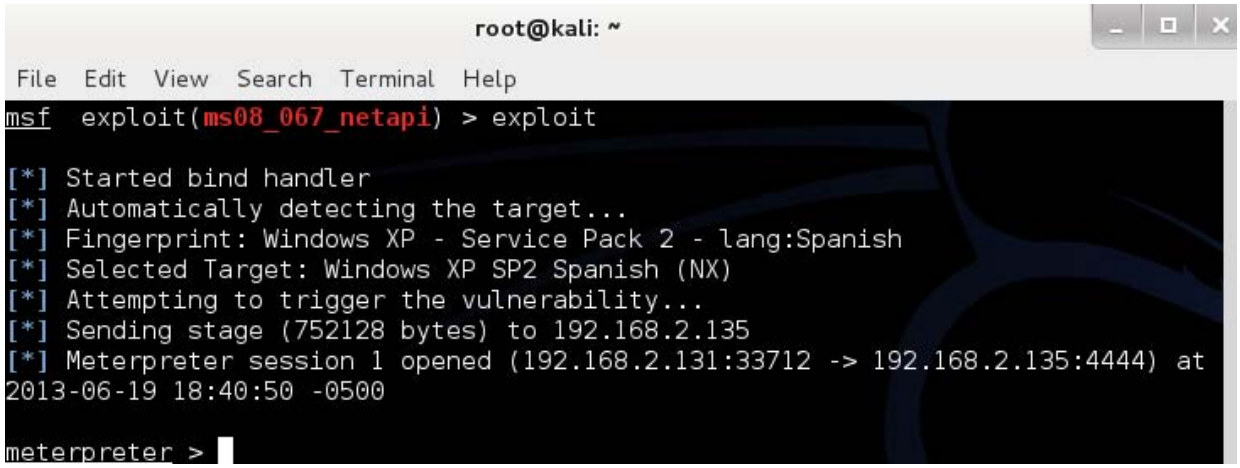


Figura A.7 Ejecución del exploit

Si el exploit es exitoso se crea una nueva sesión y la terminal cambiará a *meterpreter*>, en este momento se tiene control total del sistema y se pueden realizar diversas acciones, para listar los archivos se puede colocar el comando **ls** (Figura A.8):

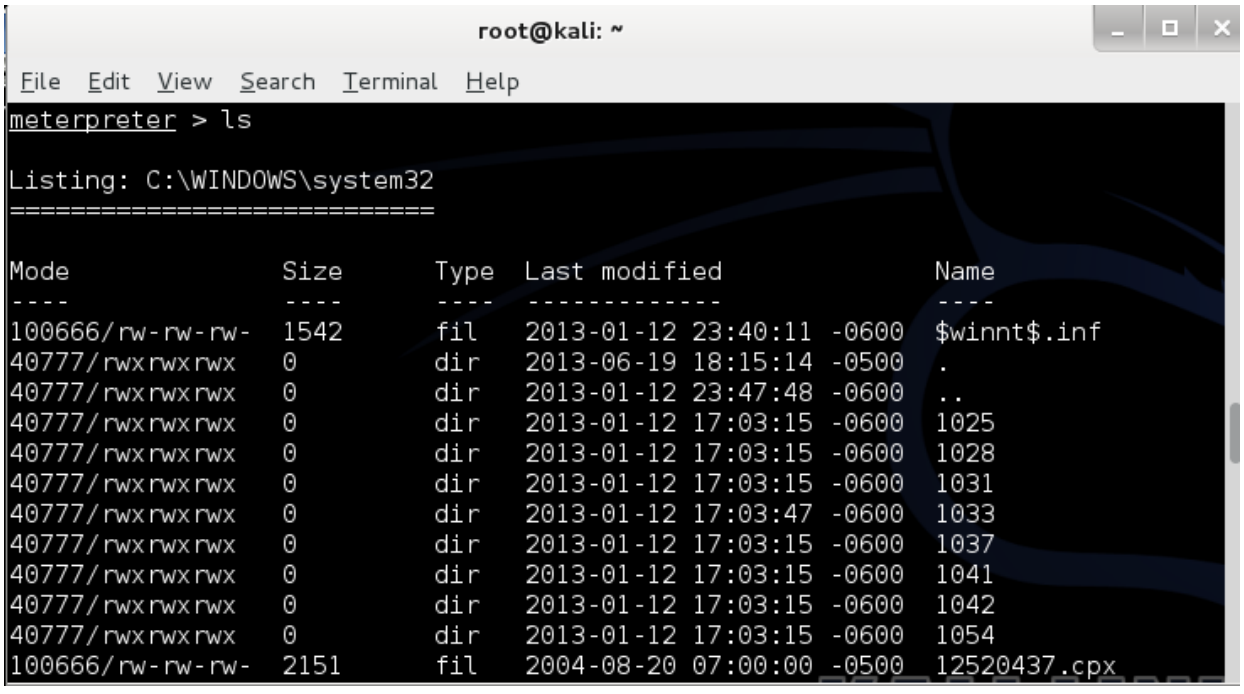


Figura A.8 Sesión en meterpreter con control total del sistema

Para obtener información de sistema se puede utilizar el comando **sysinfo** (Figura A.9):

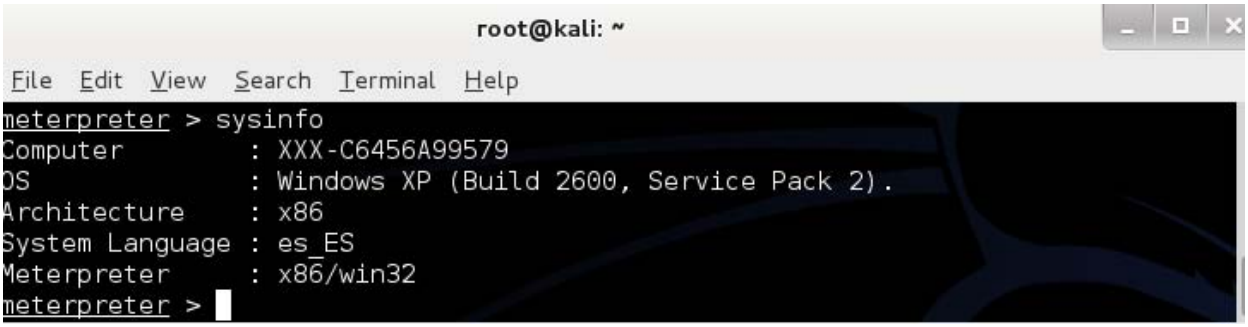


Figura A.9 Comando sysinfo

Para visualizar la configuración de red se debe introducir el comando **ipconfig** (Figura A.10):

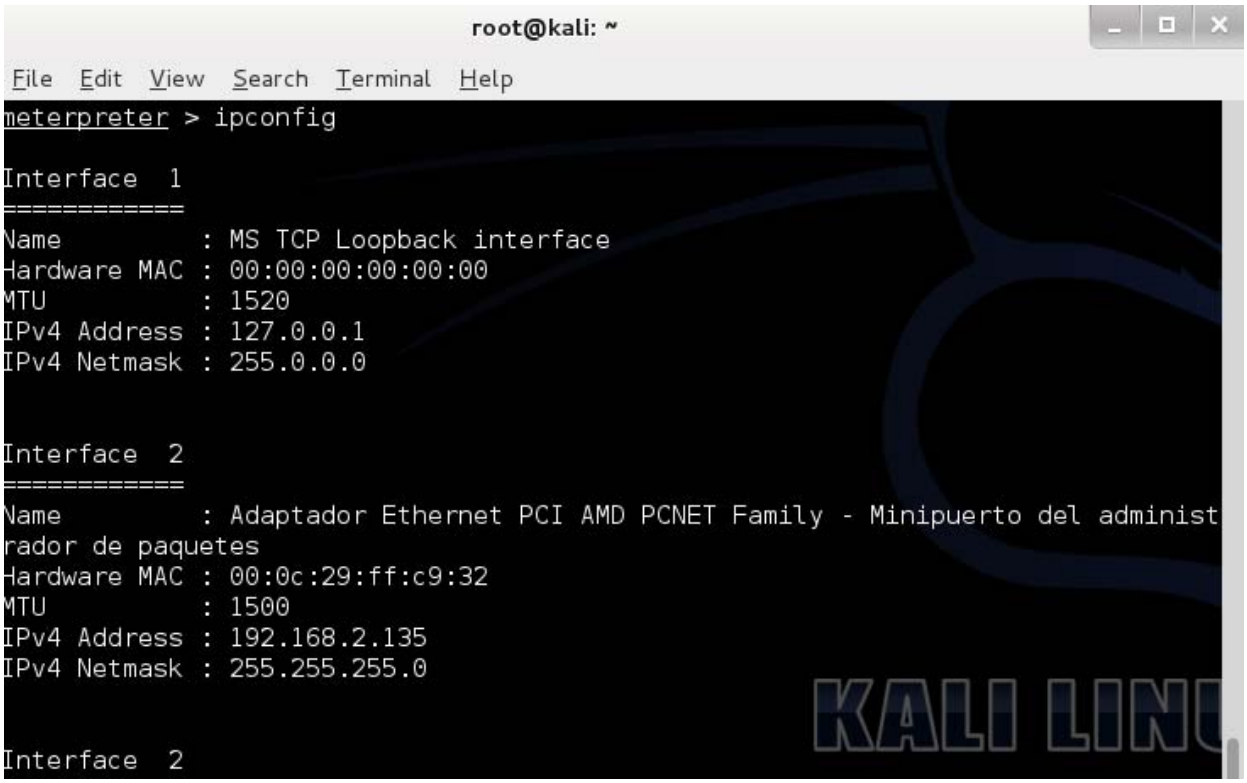


Figura A.10 Comando ipconfig

El comando *route* permite consultar y hacer cambios en la tabla de enrutamiento (Figura A.11).

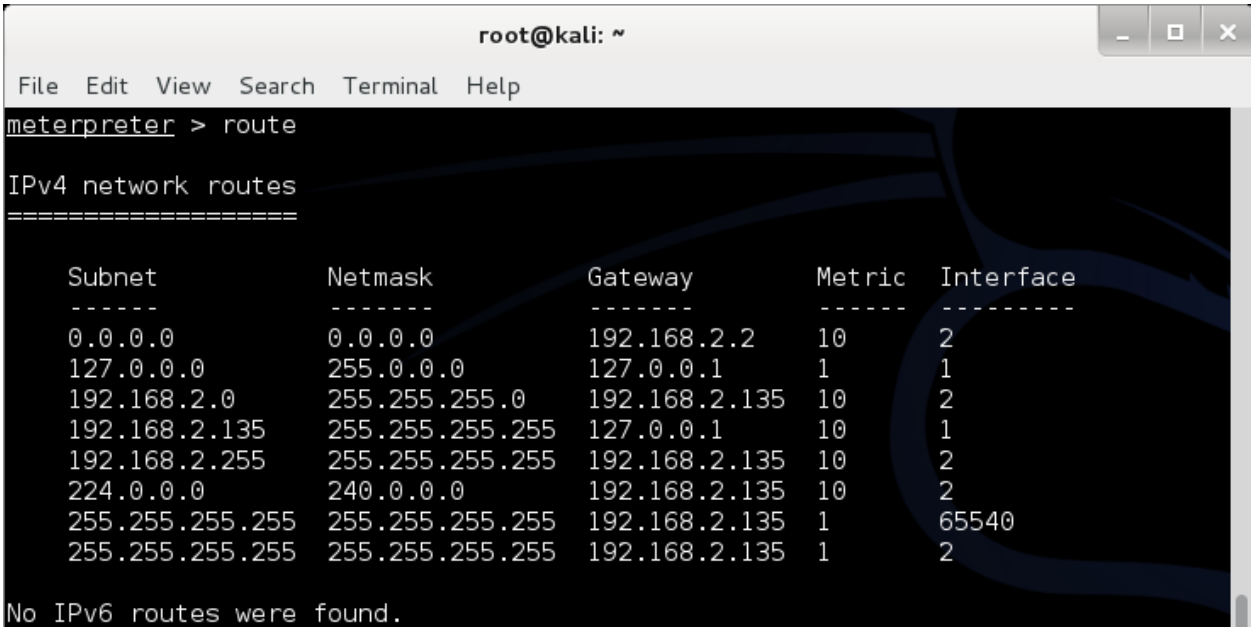


Figura A.11 Comando route

Si se necesita hacer una captura de pantalla se puede utilizar el comando *screenshot*, una vez ejecutado se guardará una captura de pantalla con formato jpeg (Figura A.12). Par visualizar la captura de pantalla se puede usar la utilidad *eog* (Figura A.13). Además se puede visualizar lo que un usuario está realizando en un momento determinado (Figura A.14).

Figura A.12 Comando screenshot

Figura A.13 Utilidad eog

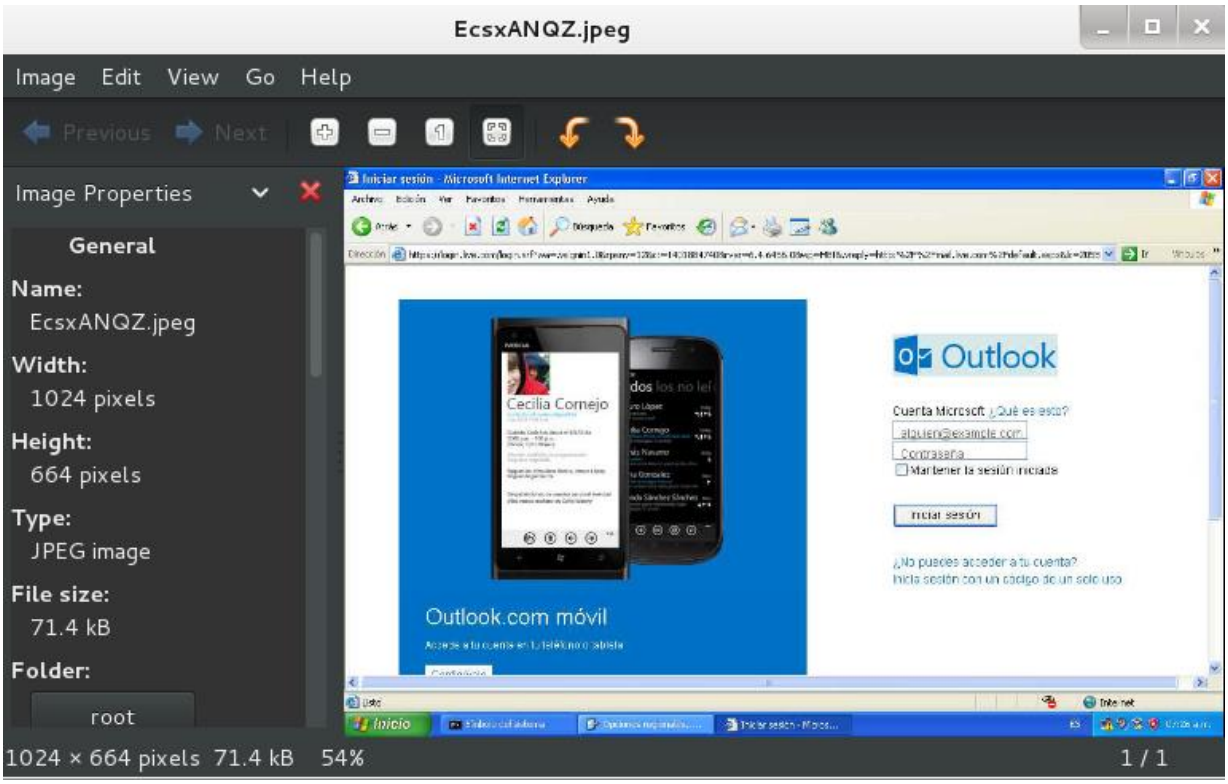


Figura A.14 Captura de pantalla

En los sistemas Windows existe un archivo llamado SAM usado para almacenar las contraseñas en formato de hash en LM y NTLM. Para hacer un volcado de ese archivo se debe utilizar el comando *hashdump* (Figura A.15):

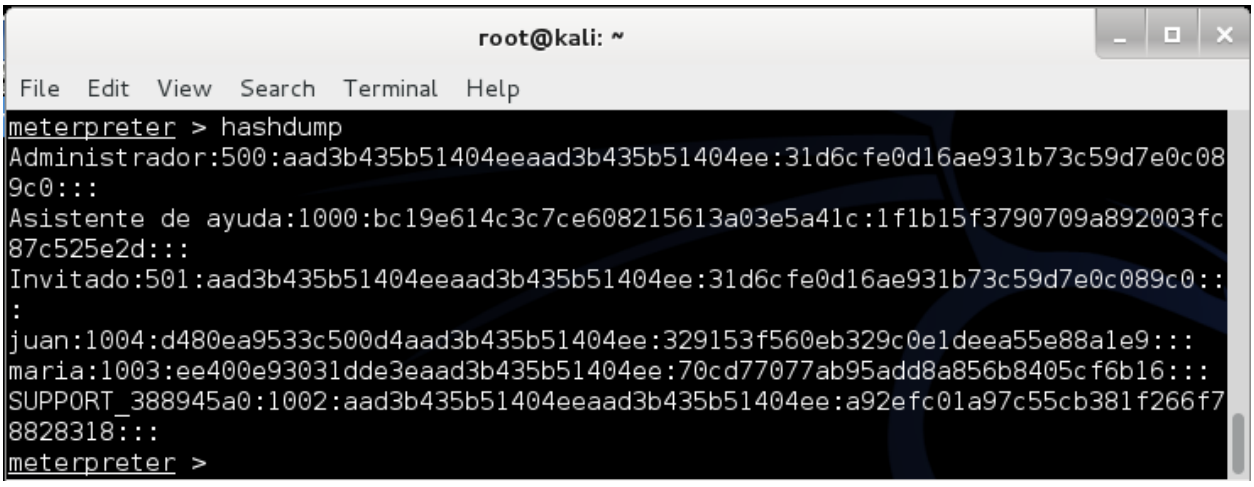


Figura A.15 Contraseñas almacenadas en el archivo SAM

Otra característica de meterpreter es que permite descargar archivos desde el sistema víctima, esto se logra con el comando *download* como se muestra en la Figura A.15.

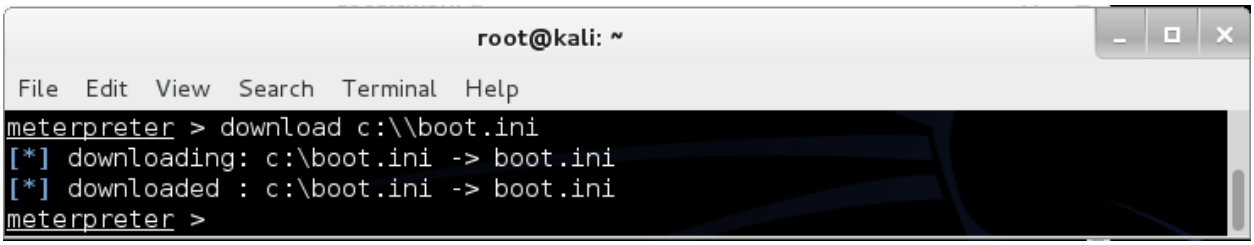


Figura A.15 Descarga de archivos

También se pueden cargar archivos, en este caso nc.exe, considerada como la navaja suiza de los hackers, permite poner puertos a la escucha, Figura A.16.

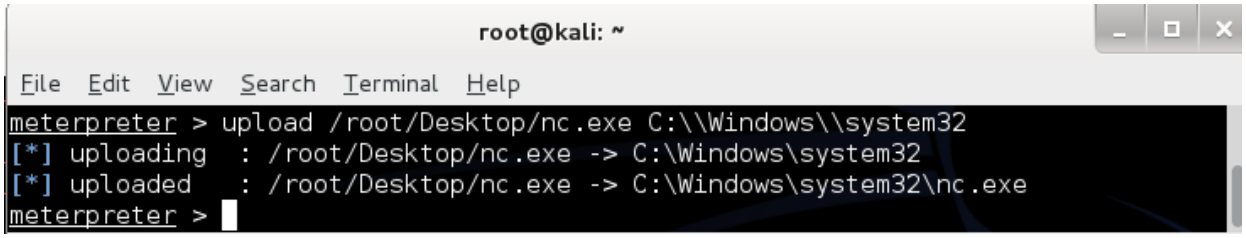


Figura A.16 Carga de archivos

El comando shell permite obtener una línea de comandos de Windows, Figura A.17.

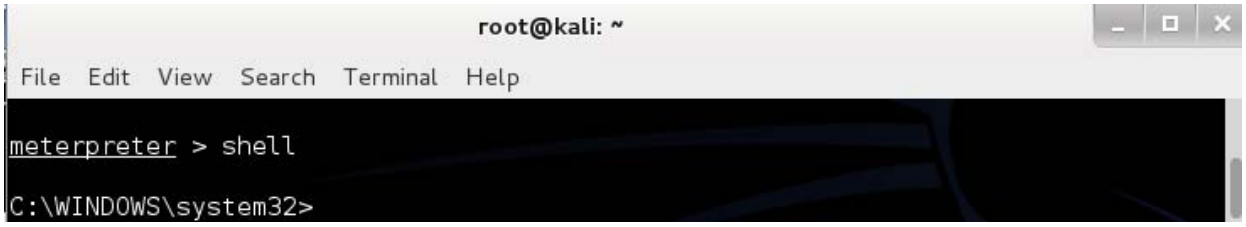


Figura A.17 Comando Shell

Conclusión

Una simple vulnerabilidad puede permitir a un atacante el control total con ayuda de herramientas automatizadas con Metasploit.

ANEXO B Instalación de Nessus y Ntop

Instalación de Nessus

Primeramente descargar nessus del siguiente link:
http://www.tenable.com/products/nessus/select-your-operating-system
Escoger la versión home.

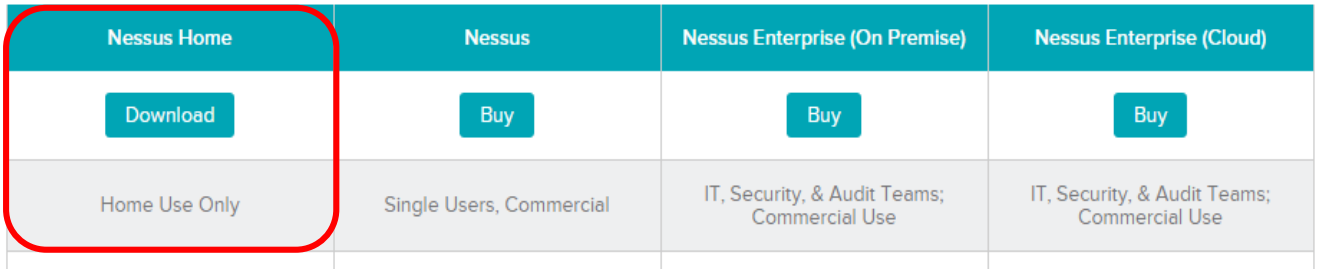


Figura B.1 Selección de version

Para kali Linux o el sistema operativo donde se va a instalar la herramienta se debe seleccionar si es de 32 o 64 bits, en este caso es de 32 bits.

Figura B.2 Selección del sistema operativos entre 32 y 64 bits

Se aceptan las condiciones de uso del producto.

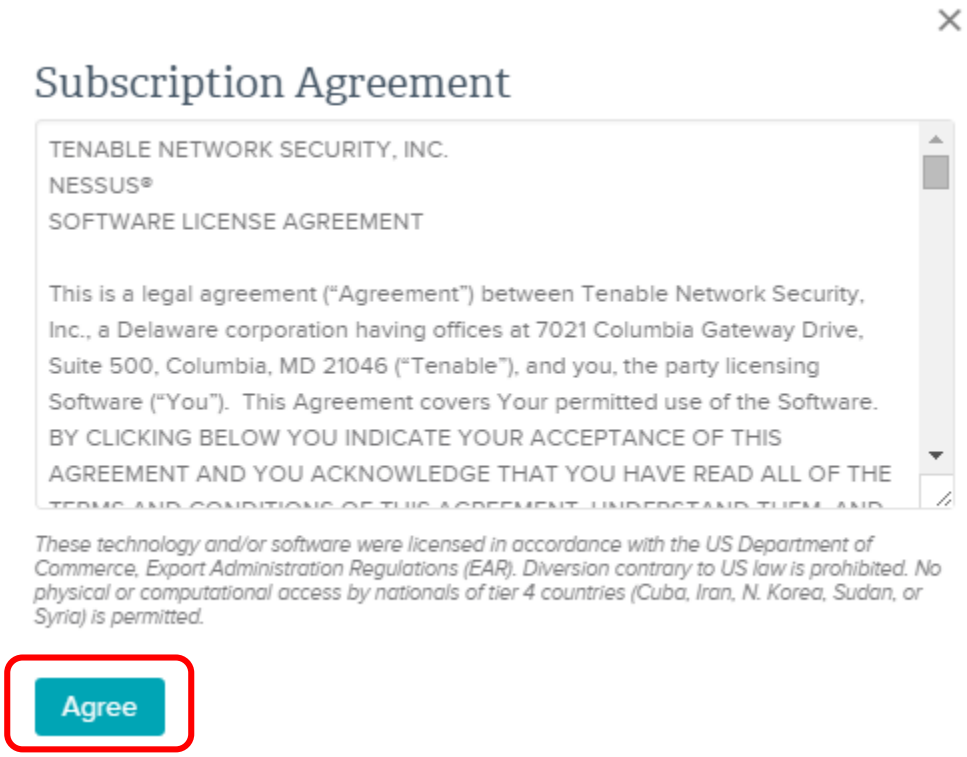


Figura B.3 Condiciones del producto

A continuación dirigirse al directorio donde se descargo el archivo .deb de nessus

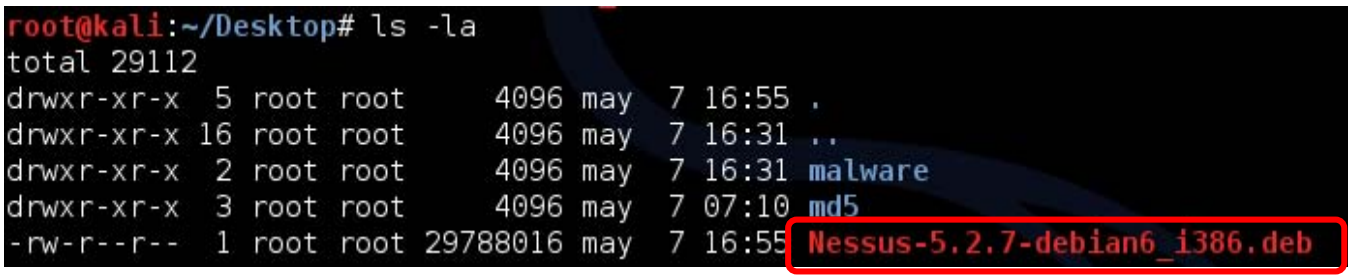


Figura B.4 Archivo empaquetado de nessus

Colocar el siguiente comando para desempaquetar a la herramienta.

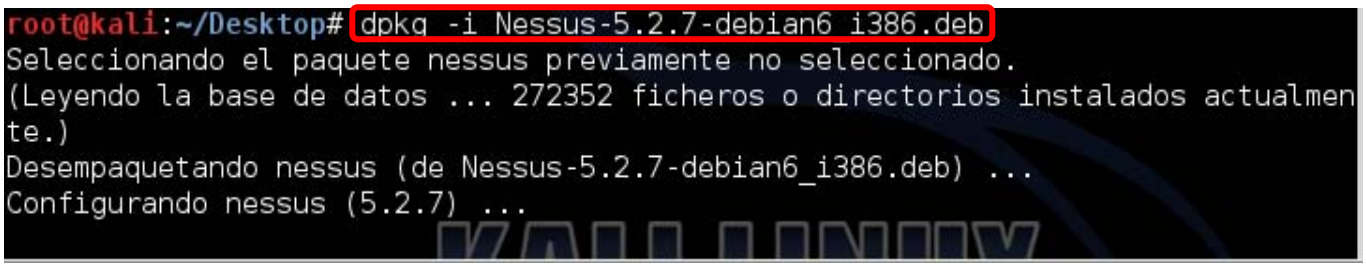


Figura B.5 Desempaquetamiento de nessus

Y esperar hasta que se termine el proceso.
Se deberá obtener un código de activación, para esto hay que registrar el producto en la siguiente url.

http://www.tenable.com/products/nessus-home

Seleccionar Nessus Home.

Figura B.6 Version Nessus Home

Posteriormente colocar los datos que se piden y en el correo que se colocó se recibirá el código de activación.

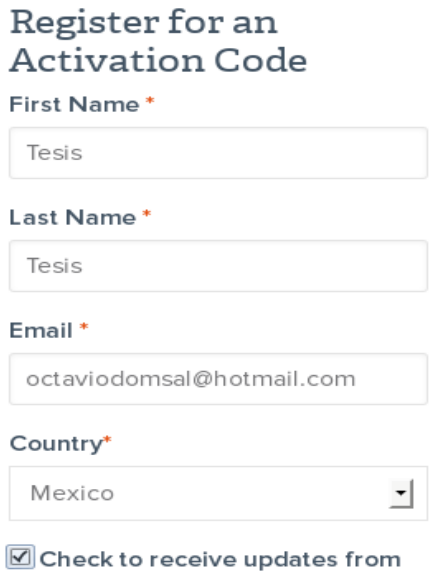


Figura B.7 Registro para el código de activación

Para este caso el código de activación fue:

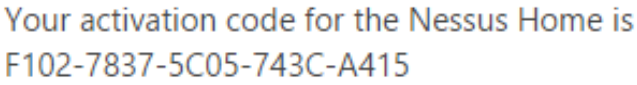


Figura B.8 Código de activación

Se tendra que colocar el código de activación de la siguiente forma:

```
# cd /opt/nessus/bin/
# ./nessus-fetch –register “F102-7837-5C05-743C-A415”
```

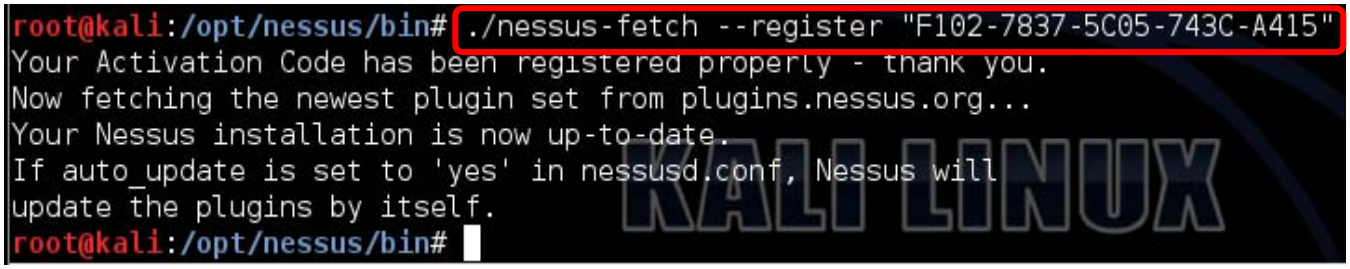


Figura B.9 Registrando a Nessus

Y se descargarán los plugins para realizar los análisis de vulnerabilidades.
Se tiene que iniciar el servicio de la siguiente manera:

```
# service nessusd start
```

Y comenzará a iniciarse Nessus

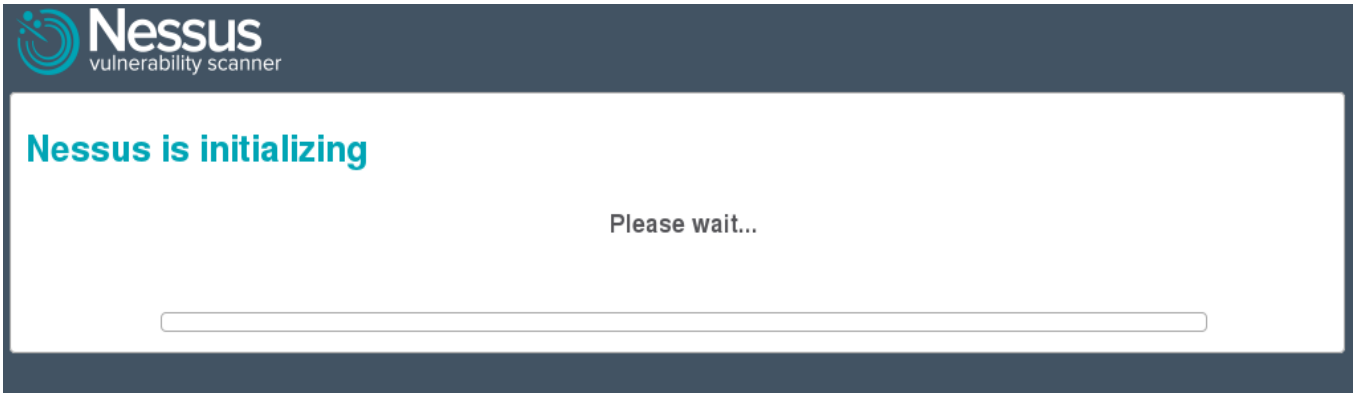


Figura B.10. Inicio de Nessus

Después que termine el proceso de inicialiación hay que configurar el usuario y el password con el que se accederá al servicio de nessus

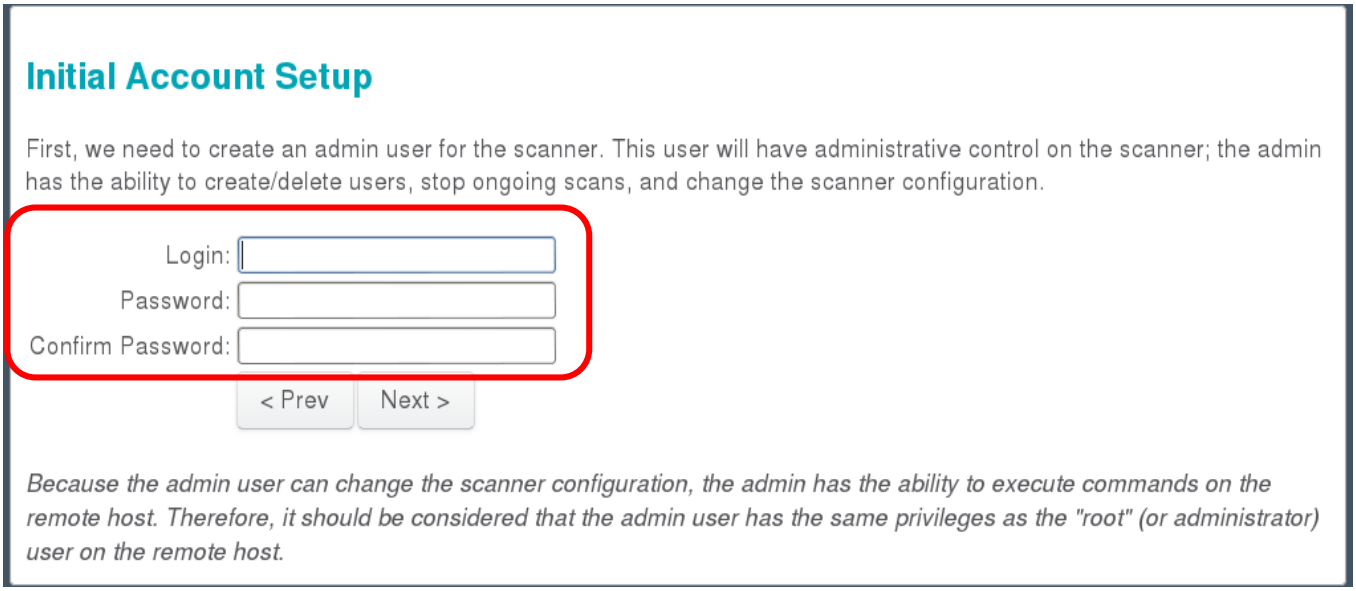


Figura B.11 Configuración inicial de la cuenta

De nuevo se va a colocar el código de activación

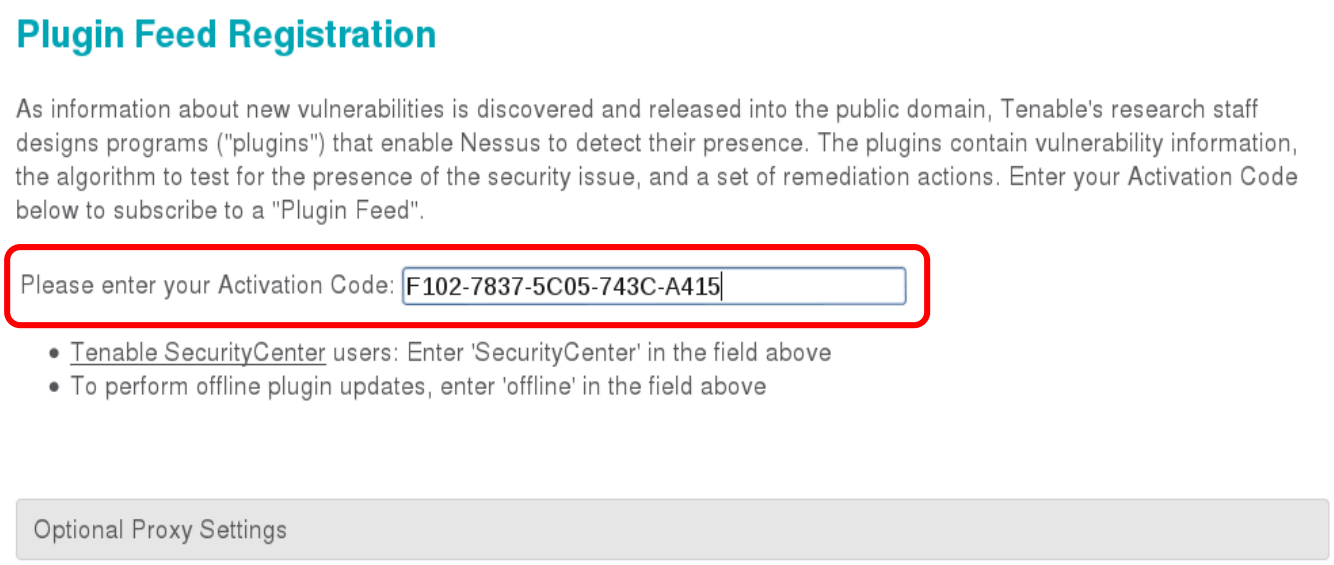


Figura B.12 Registro del producto mediante código de activación

Finalmente si el proceso de instalación se realizó correctamente aparecerá una pantalla para logarse con la credenciales que se configuraron con anterioridad.

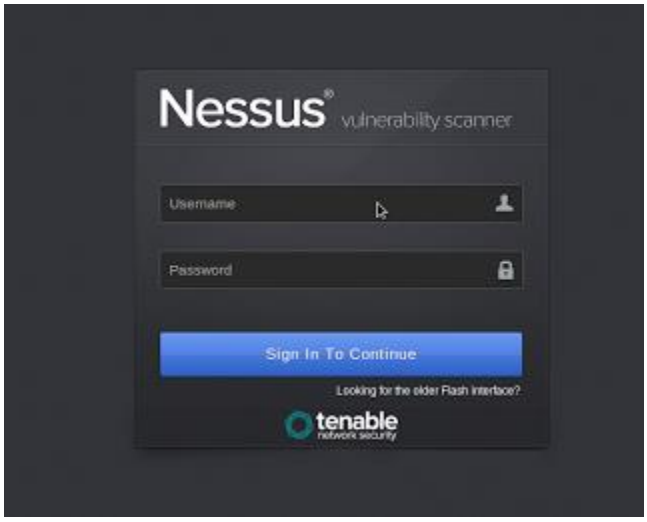


Figura B.13 Login de acceso a nessus

Ntop

Para instalar Ntop en kali Linux primero hay que actualizar los repositorios del SO, de la siguiente manera:

```
# apt-get update
```

Ahora se instala Ntop por paquetes de esta forma:

```
# aptitude install ntop
```

En el transcurso del proceso de instalación, aparecerán unas pantallas, una pedirá que se configure la interfaz y otra con la contraseña de acceso a la herramienta.

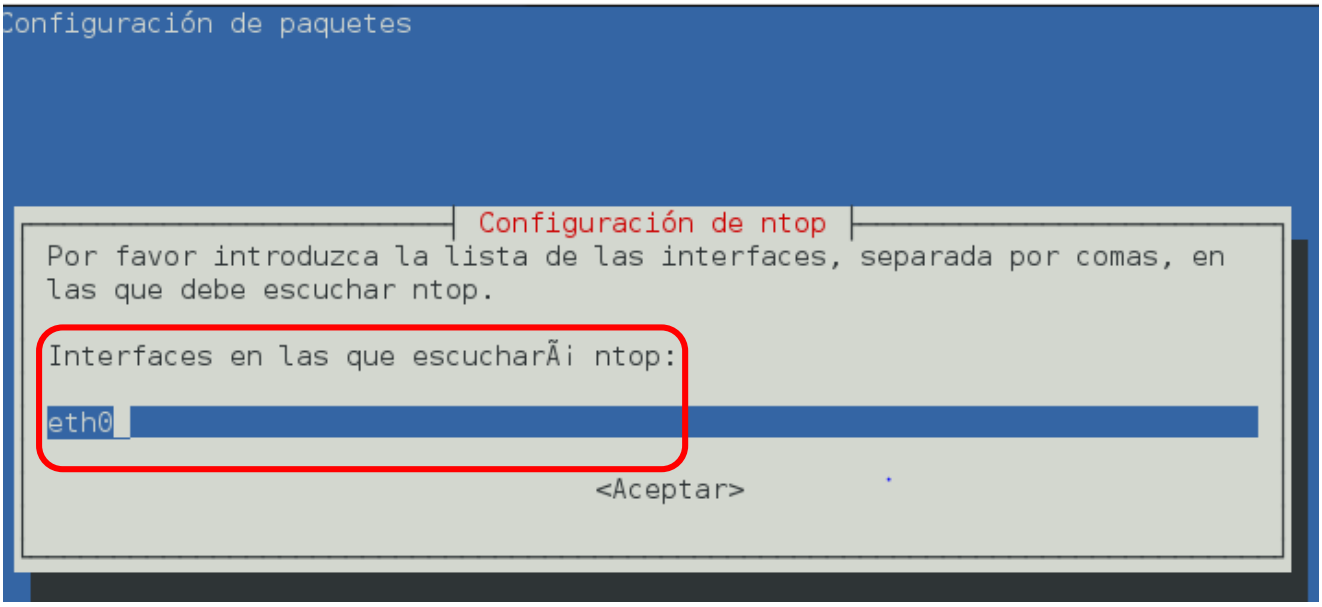


Figura B.14 Selección de interfaz de red

Para entrar a Ntop hay que acceder a:

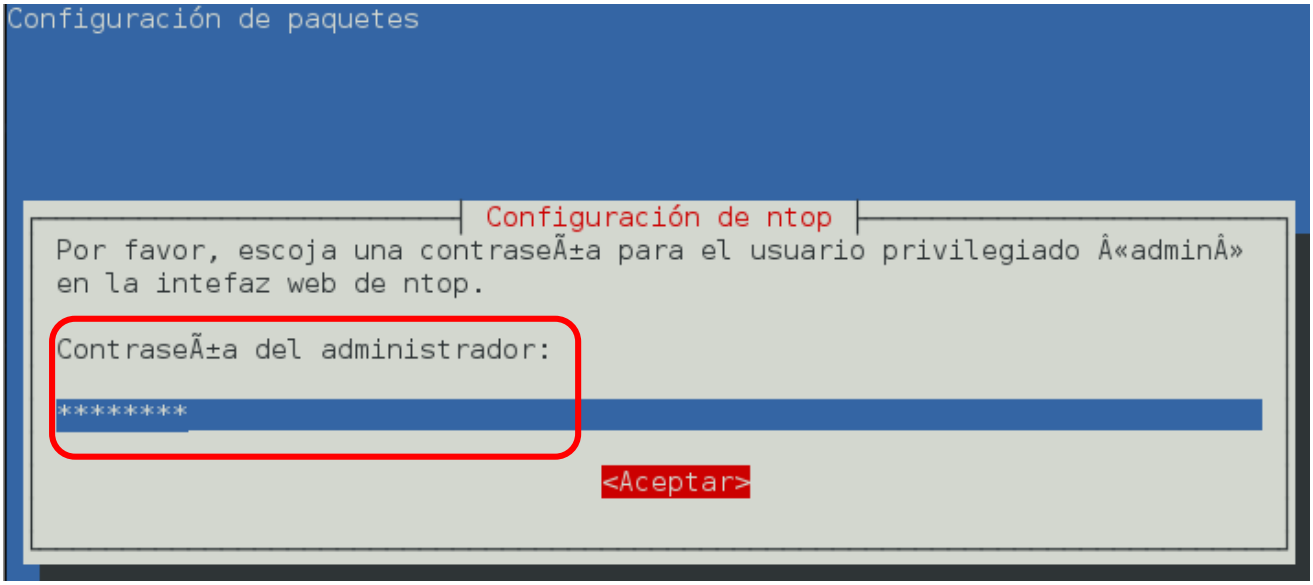
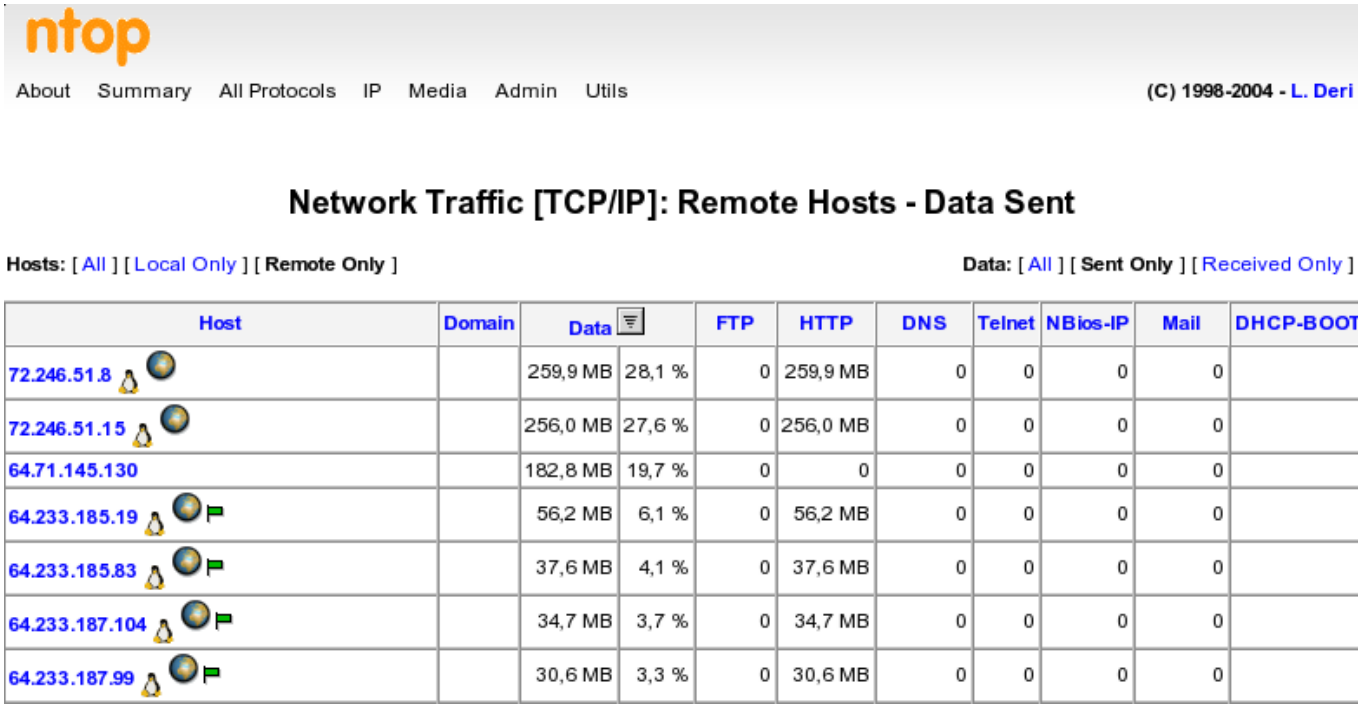


Figura B.15 Contraseña de administrador de Ntop

Finalmente hay que abrir un navegador y colocar la url siguiente:

http://ip-de-la-maquina:3001



Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOT
72.246.51.8		259,9 MB	28,1 %	0	259,9 MB	0	0	0	0	
72.246.51.15		256,0 MB	27,6 %	0	256,0 MB	0	0	0	0	
64.71.145.130		182,8 MB	19,7 %	0	0	0	0	0	0	
64.233.185.19		56,2 MB	6,1 %	0	56,2 MB	0	0	0	0	
64.233.185.83		37,6 MB	4,1 %	0	37,6 MB	0	0	0	0	
64.233.187.104		34,7 MB	3,7 %	0	34,7 MB	0	0	0	0	
64.233.187.99		30,6 MB	3,3 %	0	30,6 MB	0	0	0	0	

Figura B.16 Ntop en funcionamiento

ANEXO C Instalación de Untangle

Después de arrancar el disco de instalación de untangle, preferente se debe instalar en modo gráfico, ya que los reportes y gráficas se observan mejor. Posteriormente de sebe seleccionar un idioma, en este caso español:

Figura C.1 Selección de idioma

Posteriormente Untangle cargará componentes adicionales

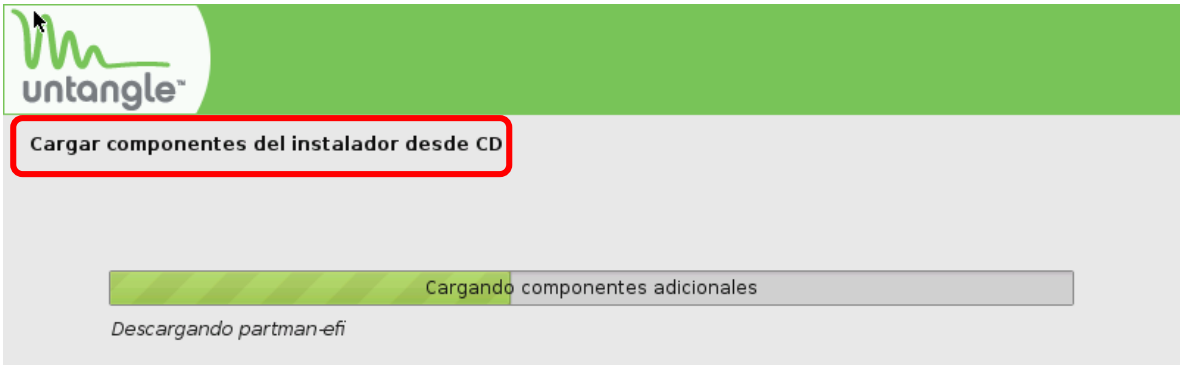


Figura C.2 Carga de componentes adicionales

Untangle pedirá que se le indique una zona horaria:

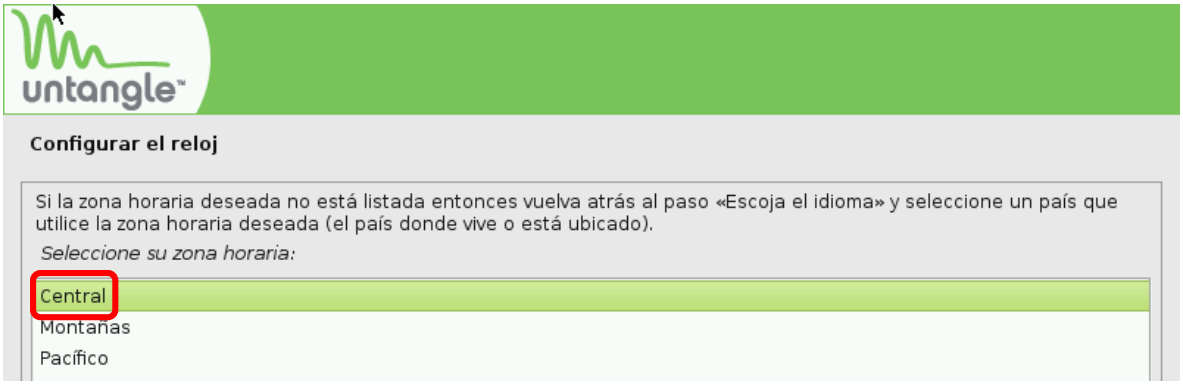


Figura C.3 Zona horaria

Enseguida se procede a dar formato al disco duro:

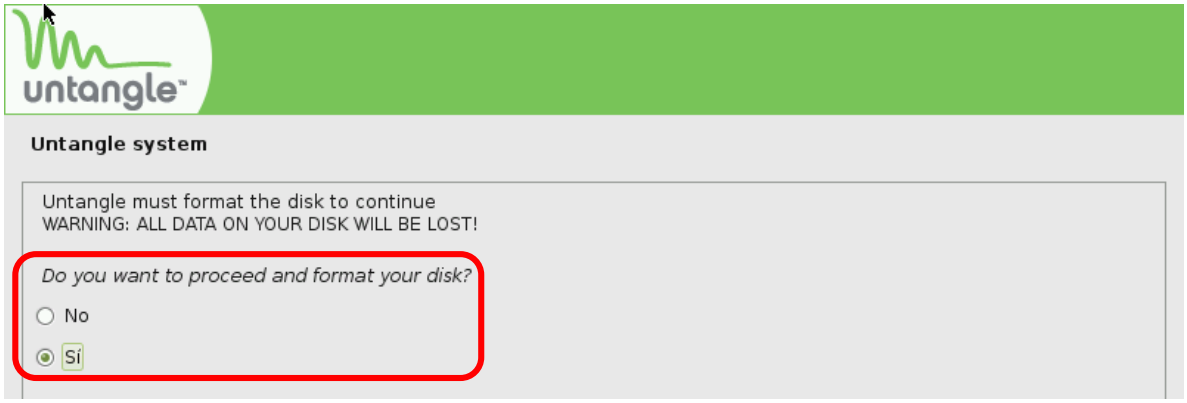


Figura C.4 Formato al disco duro

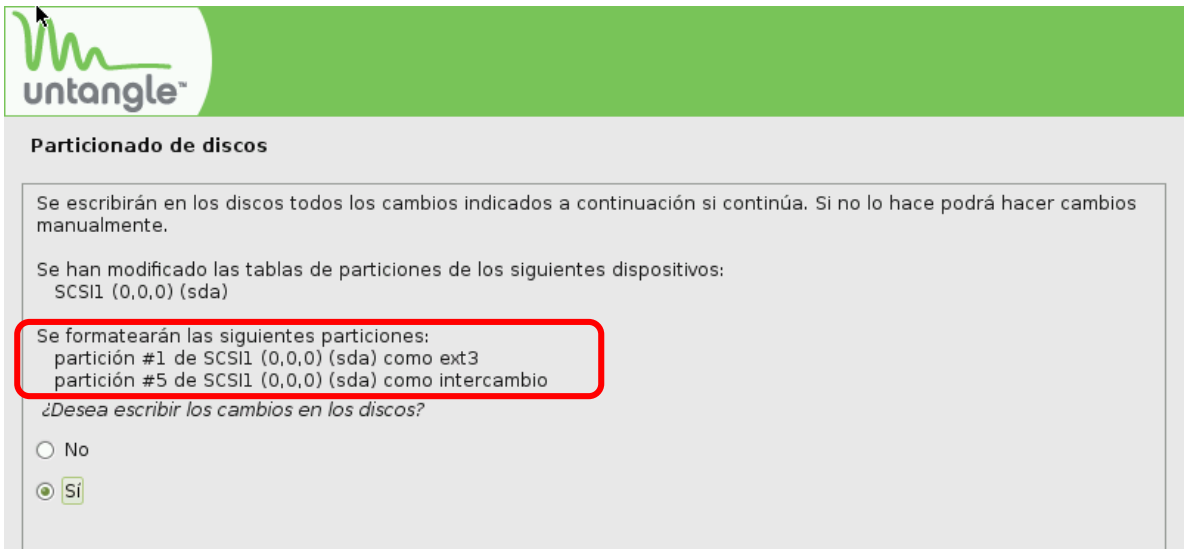


Figura C.5 Partición del disco duro

Después, Untangle instalará todo los archivos de necesarios para funcionar

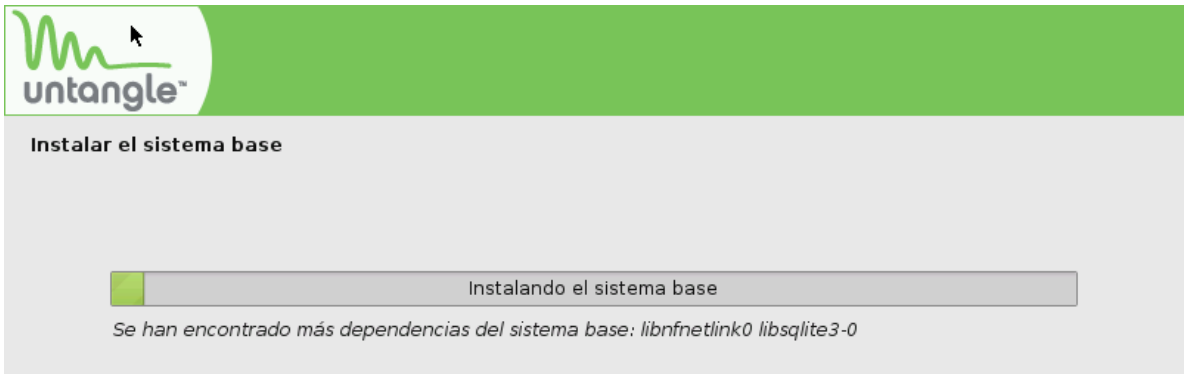


Figura C.6 Instalación de sistema base

Finalmente se muestra un mensaje que la instalación ha sido satisfactoria

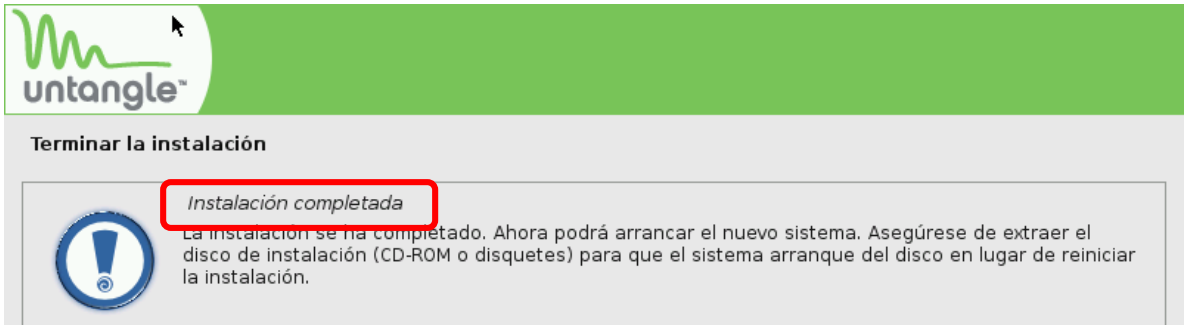


Figura C.7 Instalación completa

Configuración de Untangle

Al iniciar Untangle pedirá aplicar un lenguaje, en este caso se escoge español

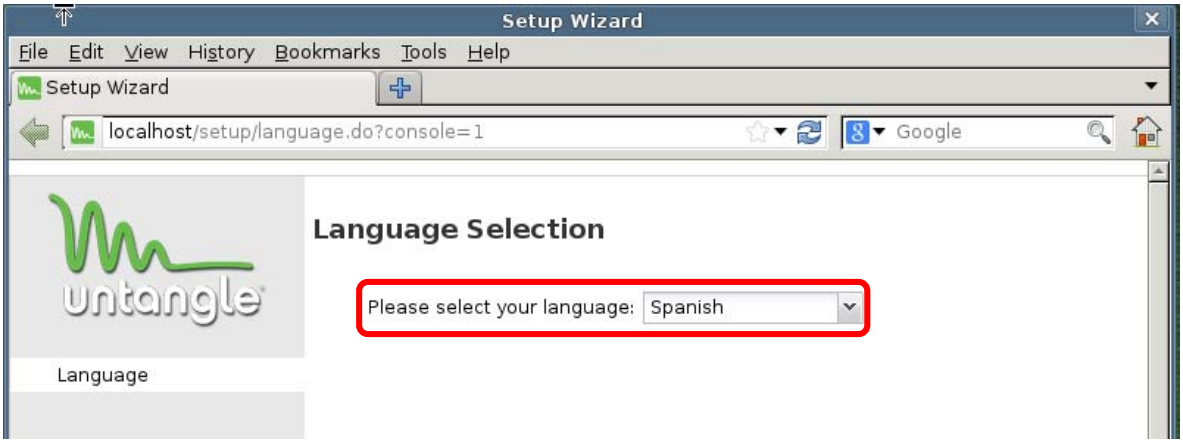


Figura C.8 Configuración del lenguaje

Después se despliega un menú de configuración.

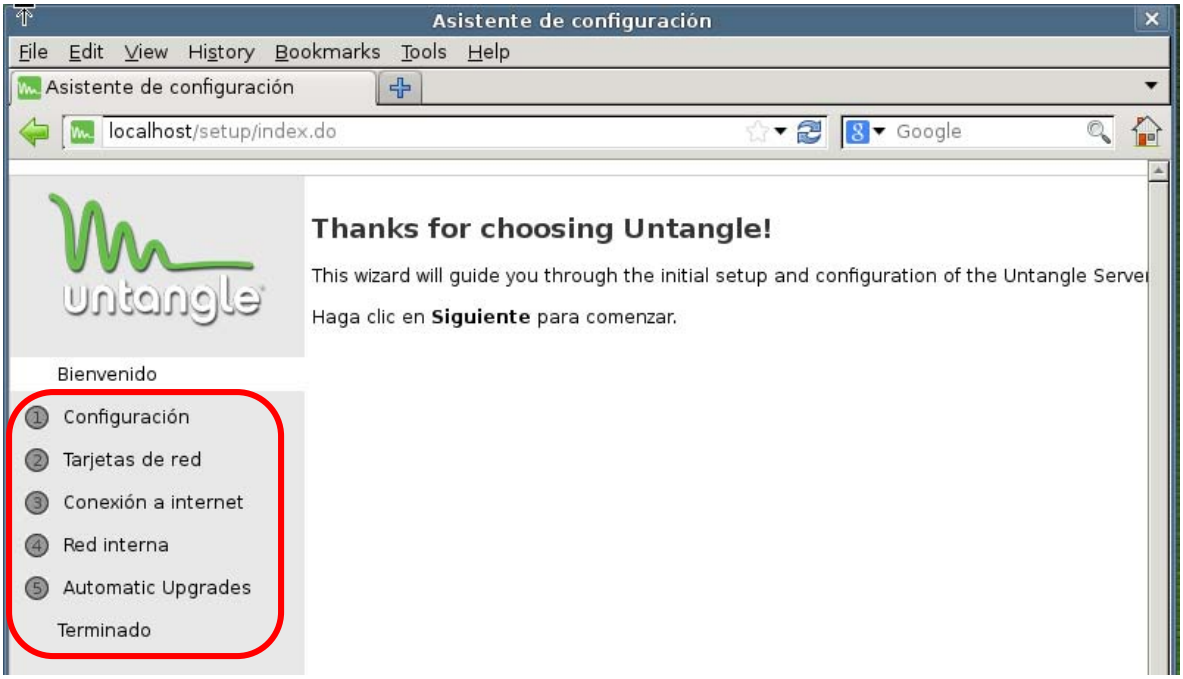


Figura C.9 Menú de configuración

Se identifican las interfaces de red, tanto la externa como la interna

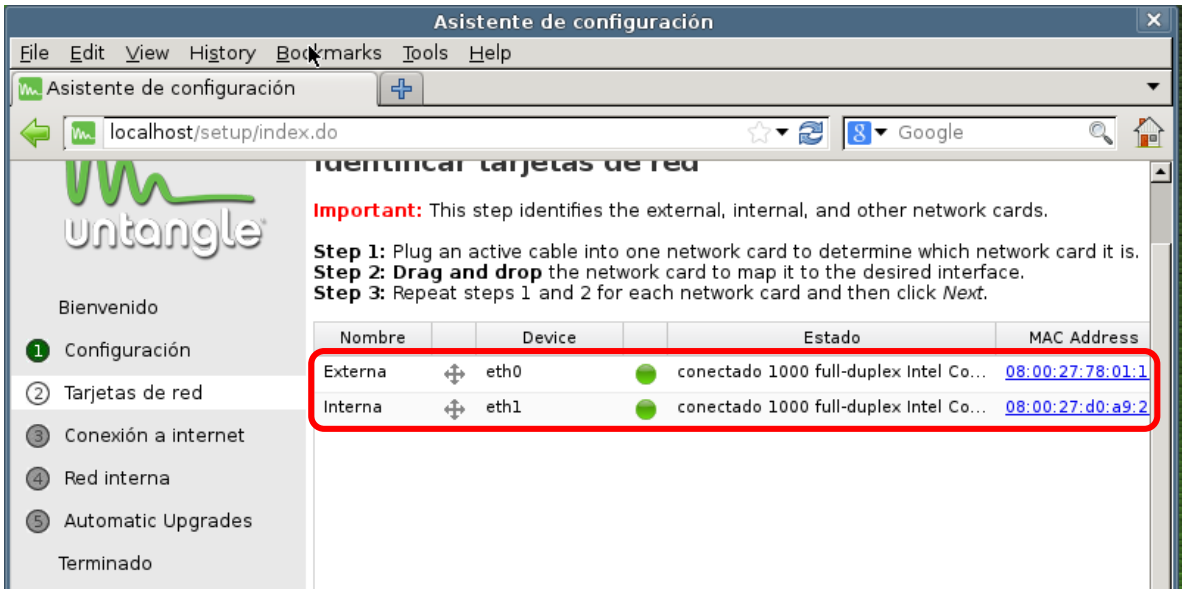


Figura C.10 Configuración de interfaces de red

Se configura la conexión a internet y se selecciona la configuración de DHCP, además se hace puede realizar una prueba de conectividad para internet.

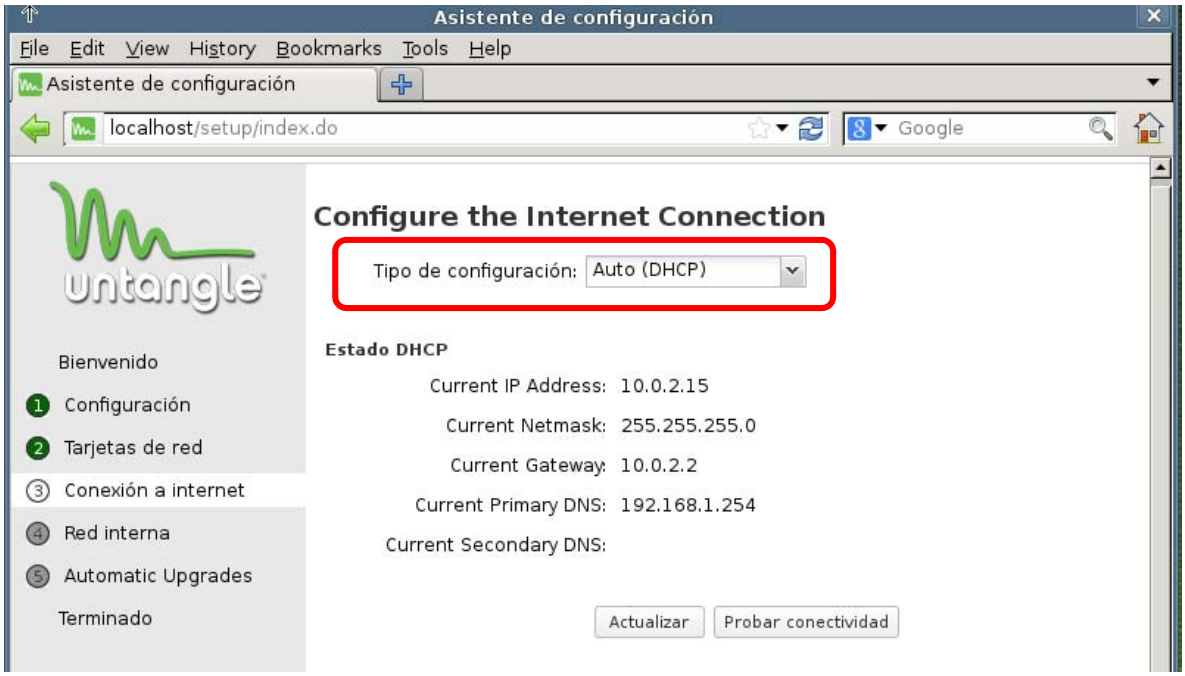


Figura C.11 Configuración del DHCP

Se selecciona la configuración de la red interna, puede ser modo router o el modo puente transparente.

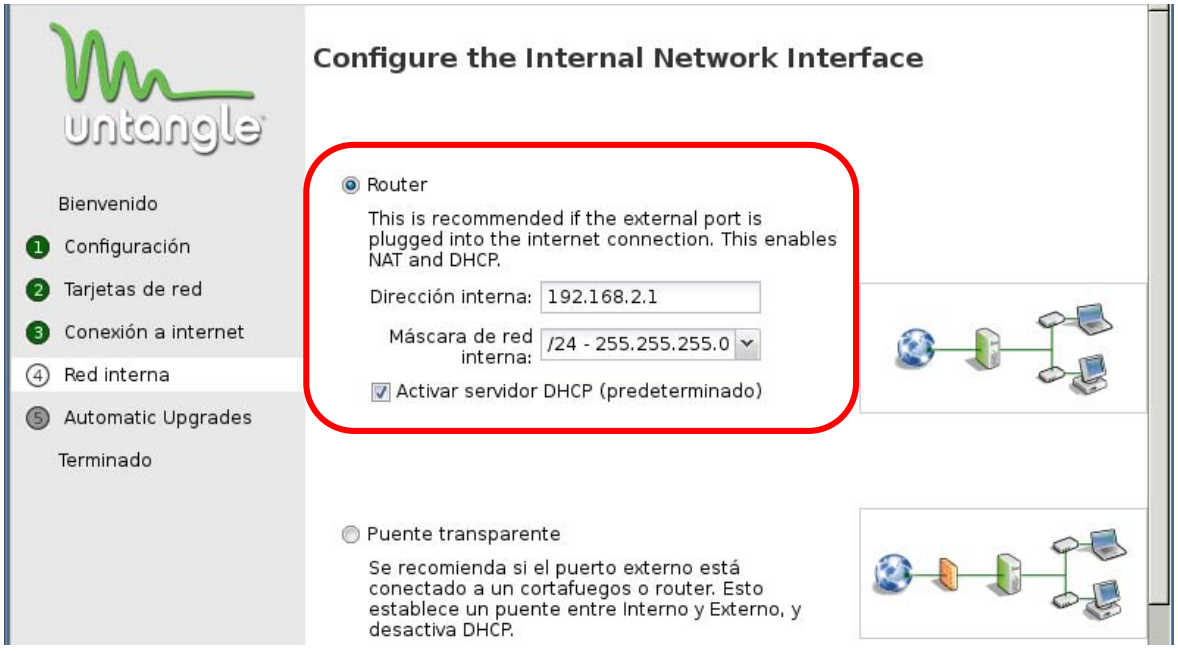


Figura C.12 Configuración de interfaz de la red interna

Se selecciona que las configuraciones sean automáticas.

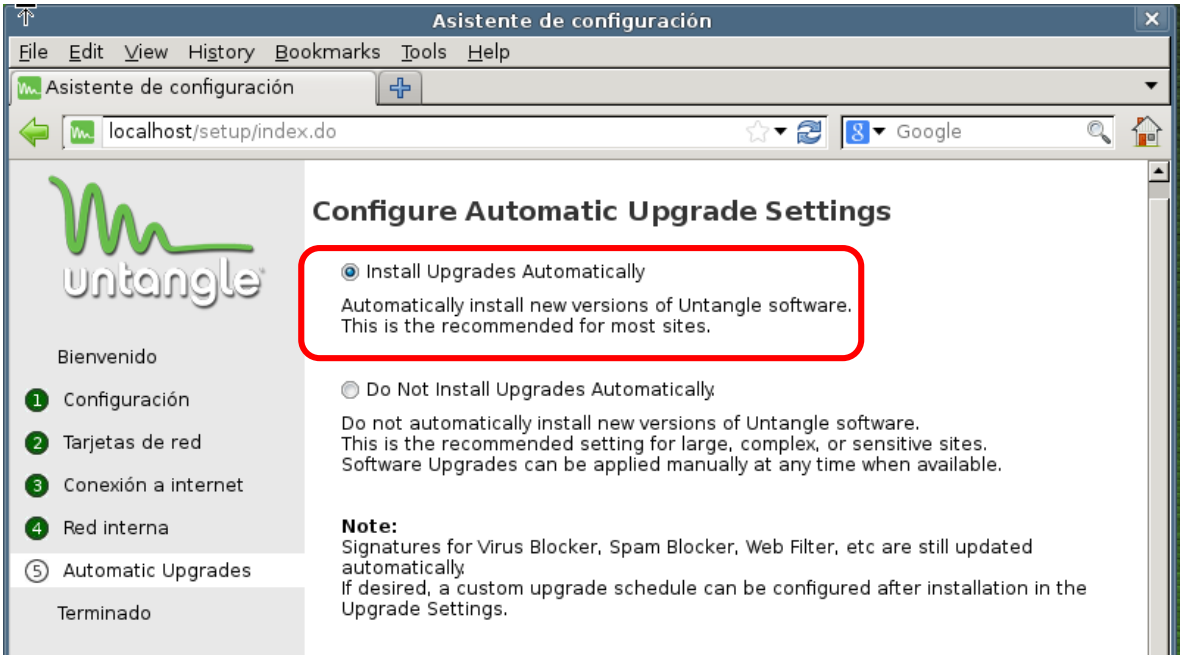


Figura C.13 Configuración de las actualizaciones de Untangle

Finalmente aparece un mensaje de que el servidor Untangle ha sido configurado.

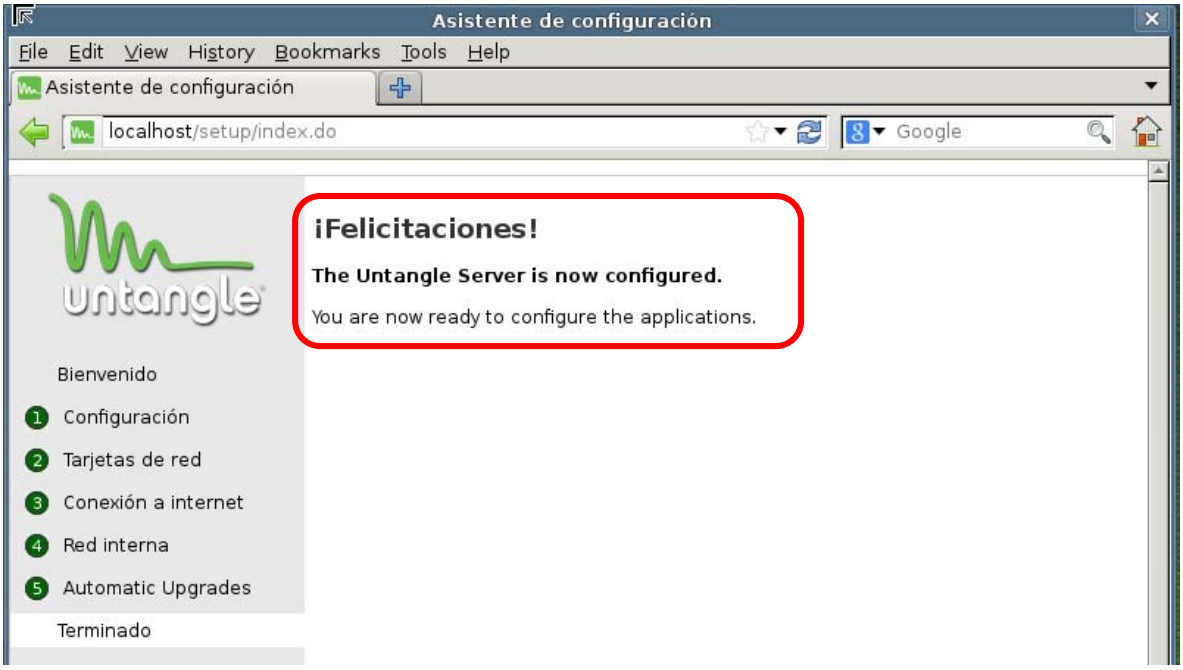


Figura C.14 Configuración exitosa

Se debe tener una cuenta en el sitio de Untangle para descargar los módulos de paga por 14 días.

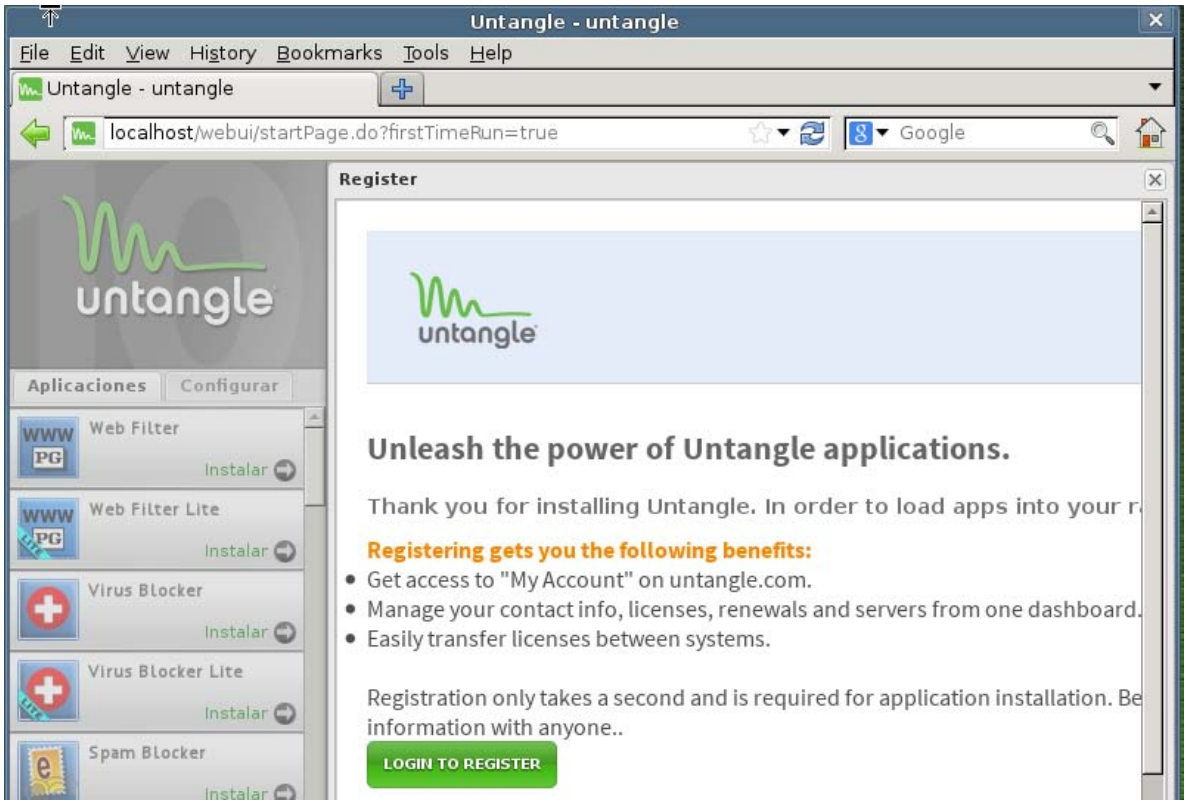


Figura C.15 Módulos de paga

ANEXO D Uso de Software ilegal en las Empresas

Tomando en cuenta una encuesta nacional generada por la consultoría Parametría señala que 7 de cada 10 compañías tiene algún problema de licenciamiento de software. El estudio fue llevado a cabo en 2013, el cual menciona que el 70 por ciento de las empresas tiene prácticas ilegales de uso de software y que la práctica más frecuente es la descarga de software sin licencia.

El software ilegal puede producir vulnerabilidades, el estudio menciona que el 29 por ciento de las empresas tiene problemas de malware, un 22 por ciento tuvo pérdidas de información y un 34 por ciento menciona haber tenido auditorías en sus sistemas informáticos por parte de las autoridades correspondientes.

En cuanto a segmentos empresariales que usan software ilegal, en primer lugar se encuentran las compañías que desarrollan software con un 92 por ciento, el sector educativo con un 80 por ciento y el de construcción con un 80 por ciento, el sector financiero no se encuentra exento con un 53 por ciento y por último el de manufactura con 59 por ciento.

En cuanto acciones legales en contra del uso del software ilegal en las empresas se realizaron 1059 visitas de inspección.

México avanza lentamente en contra del software ilegal, según el Instituto México de la Propiedad Intelectual menciona que desde el año 2000 el instituto ha trabajado con la industria del software, para realizar visitas a las empresas y verificar la legalidad del software que usan, la explicación más frecuente acerca de los usos de software apócrifo es por su bajo precio, la facilidad de obtener los programas y porque consideran las empresas que no generan ningún problema al adquirir el producto.

México es el tercer país con mayor índice de software ilegal a nivel mundial con un 57 por ciento. Para solucionar el problema de software ilegal en las empresas se recomienda que se adquiera la licencia del software que es realmente indispensable para las actividades de la compañía, si no se tiene los recursos para comprar todas las licencias, se pueden buscar alternativas de software libre o de versión gratuita que tal vez no cubran con todas las características del software de paga, pero si una parte para continuar con las actividades de la empresa.

Glosario de términos

Acceso Discrecional: El usuario es dueño de la información o datos y él decide qué usuarios pueden tener acceso al recurso.

Acceso Mandatorio: Se basa en un sistema donde los recursos tienen una etiqueta de seguridad (Secreto, Ultra secreto, Confidencial, etc.)

Activo: Cualquier objeto tangible, intangible o información que tenga valor para alguien o un grupo de personas.

Ataque: Es la culminación de una amenaza al explotar una o varias vulnerabilidades.

Auditoría informática: es el proceso de recolección y evaluación de evidencias utilizadas para determinar cuándo un sistema informático salvaguarda sus activos, mantiene la integridad de sus datos, ejecuta eficazmente los objetivos marcados por la organización con políticas de seguridad y consume los recursos eficientemente.

Autenticación: Es un proceso para comprobar y verificar la identidad de una persona, usuario o programa por medio de información adicional.

Backdoor: Es un proceso que abre un puerto local que se infectó, que permite que posibles personas mal intencionadas se conecten remotamente y así evadir la autenticación del sistema.

Botnet: hace referencia al termino bot que significa “robot”, se puede decir que es robot informático que se ejecutan de manera autónoma, tratándose de apoderar de las computadoras de forma remota, las cuales quedan en un estado zombi después que se introdujo el bot en la computadora, para que después el atacante las pueda usar como le plazca, haciendo negaciones de servicio.

Cifrado: Es un procedimiento que utiliza un algoritmo para transformar un mensaje, de tal forma que sea incomprensible, y que solamente podrá ser comprensible por quienes posean la clave o llave apropiada para el proceso de descifrado.

Confidencialidad: Garantiza que sólo aquellas personas o procesos autorizados puedan acceder a la información.

Cookie: Es una pequeña parte de información enviada por un sitio y almacenada en el navegador del usuario, sus funciones son: control de usuarios e información sobre los hábitos de navegación del usuario.

Disponibilidad: Garantiza que usuarios y procesos autorizados tengan acceso a la información cuando lo necesiten y cuantas veces se requiera.

DMZ: Es una red local ubicada entre la red interna de una organización y la red externa, con el objetivo que la conexión de la DMZ se permita sólo hacia el exterior y las conexiones de red interna y red externa estén permitidas

Firewall: Es un dispositivo (software o hardware) que tiene un conjunto de reglas específicas, con las cuales determina que tráfico de red puede entrar o salir.

Gateway: Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

Gusanos: Programas capaces de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos.

Hacker: Existen 2 principales clasificaciones hacker de sombrero negro, los cuales realizan ataques de penetración contra sistemas de información si autorización y los hackers de sombrero blanco que son personas que llevan a cabo una evolución de seguridad con un contrato establecido por el cliente o beneficiario.

Tree way handshake: Se presenta en el protocolo TCP como el establecimiento de una conexión en 3 pasos entre el cliente y el servidor.

Hash: Es una función en la que un mensaje siempre tiene el mismo valor hash, funciona principalmente para detectar modificaciones de un texto o archivo.

Honeypot: Es un software que atrae atacantes, simulando que es un sistema vulnerable.

Identificación: Es un proceso por el cual una persona, usuario, o programa muestra quien es, en otras palabras muestra su identidad.

Impacto: Es la medición de las consecuencias de la materialización de algún riesgo o de una amenaza.

Integridad: Se encarga de conservar la exactitud y totalidad de la información, esto es, que la información no sea modificada de alguna forma por usuarios o procesos no autorizados.

Intrusos remunerados: Son expertos en informática contratados por terceros para la obtención de información confidencial o hacer ataques.

IPS: Es un software que ejerce un control de acceso para detener amenazas que afecten a la red que protege, por medio de reglas.

ISACA: (Information Systems Audit and control Association). Es una asociación internacional impulsa el desarrollo de metodologías y certificaciones para la realización de auditorías y controles en sistemas de información.

Malware: Es una forma generalizada para llamar a los programas o software que presentan un comportamiento malicioso en los dispositivos o equipos informáticos.

MIB: Es un tipo de base de datos que contiene información en una estructura en forma de árbol de los dispositivos de una red para poderlos monitorear.

MIME: Es una serie de convenciones o especificaciones dirigidas al intercambio a través de internet de todo tipo de archivos de manera transparente para el usuario.

Nessus: Es un escáner de vulnerabilidades de sistemas informáticos, ya sean sistemas operativos, redes de datos, aplicativos, configuraciones y bases de datos.

Ociosos: Son aquellas personas que no forman parte del personal de una organización, ni tampoco tienen intenciones de causar daño, simplemente descargan software de la red y lo ejecutan para ver qué pasa.

Buffer overflow: Es un error de software que se produce cuando un programa no controla adecuadamente el área de memoria reservada.

Pentest: Son una forma de evaluar la seguridad en los sistemas informáticos, por medio de la detección de vulnerabilidades y la explotación de estas de forma controlada, para encontrar cuales son los huecos de seguridad de los sistemas.

Pharming: Es un tipo de ataque que se enfoca en afectar a servidores DNS o a los equipos propios de los usuarios, que permite a un atacante redirigir un nombre de dominio a otro equipo distinto.

Phising: Consiste en un envío de correos electrónicos, que aparentan provenir de fuentes confiables, intentando obtener datos confidenciales del usuario que los recibe, para que posteriormente sea defraudado.

Plug-in: Es un conecto o extensión que sirve como complemento para una aplicación que permite darle una nueva funcionalidad.

Proxy: Es un programa o dispositivo intermediario entre los equipos de cómputo o la red interna y la red externa o el internet.

Pruebas de intrusión: Son ataques controlados a los equipos de una red, tratando de explotar alguna vulnerabilidad

Riesgo: La probabilidad o posibilidad de la pérdida o daño de algún activo.

Seguridad lógica: Es un conjunto de aplicaciones que forma una barrera, además de procedimientos que protegen el acceso al activo, como los datos y la información.

Sniffer: Es un programa (además de una persona) que puede capturar los paquetes que viajan a través de la red, pero sin modificarlos, en otras palabras sólo “fisgonea” qué pasa a través de la red.

Sniffers: Son personas que se dedican a rastrear, recomponer y descifrar los mensajes que viajan a través de la infraestructura de red.

SNMP: (Simple Network Managment Protocol) que es un protocolo que sirve para la gestión de red.

SPAM: Son correos basura o no deseados con un remitente no conocido, por lo regular son publicitarios.

Spyware: Son programas que se instalan en la computadora del usuario desde una página web los cuales pueden capturar o sustraer información almacenada en el equipo, así como contraseñas, nombres de usuario, y más.

Troyanos: Son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecuta funciones ocultas sin el conocimiento del usuario.

Untangle: Es una solución de seguridad perimetral multifuncional que unifica en varias herramientas en un único servidor.

UTM: (Unified Threat Management). Es una herramienta que unifica varias herramientas de seguridad, es una solución, posee software como antivirus, antispam, detector de intrusos, filtrado web, firewall, principalmente.

Virus: Es una secuencia de código que se inserta en un fichero y/o archivo ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

VPN: Es una estructura de red corporativa implantada sobre una red de carácter público, con la ventaja de que es como si el usuario trabajara en su misma red local, guardando la confidencial e integridad de los datos que viajan a través de este tipo de red.

Vulnerabilidad: Es un hueco de seguridad o un fallo que tiene un activo.

FUENTES DE INFORMACIÓN

Bibliografía

[1] García, J., Fernández Y., Martínez, R., Ochoa, A., Ramos, A. A. (2011) *Hacking y seguridad en internet.* España: Alfaomega

[2] Gómez, A. (2011) *Enciclopedia de la seguridad informática.* España: Alfaomega

[3] López, M. J., Quezada, C. (2006) *Fundamentos de seguridad informática.* México: UNAM

[4] Sevilla, J. L. (2014) *Curso Pruebas de penetración y hacking ético*. México: UNAM-CERT

Mesografía

¿Cuáles son incidentes de seguridad informática que se presentan en México y Latinoamérica?
http://www.welivesecurity.com/wp-content/uploads/2014/01/informe_esr13.pdf
¿Qué es una Auditoria en seguridad informática?
http://sergiob.org/unam/DGSCA/aud/Auditorias_de_seguridad_informatica_Manual.pdf
¿Qué son los hackers?
http://www.seguridad.unam.mx/documento/?id=7
Nessus + Metasploit en backtrack 5
http://hotfixed.net/2011/05/18/nessus-metasploit-backtrack-5/
Tendencia en ataques informáticos
http://www.pymempresario.com/temas/ataques-informaticos/
Ataques informáticos en México
https://sites.google.com/site/martinezaviladiegodejesus/4-marco-te/4-4-ataques-informaticos-en-mexico
Vulnerabilidad informática de pequeñas empresas las hace blanco fácil de amenazas
http://www.pymempresario.com/2012/07/vulnerabilidad-informatica-de-pequenas-las-hace-blanco-facil-de-amenazas/
Protégete de los ataques informáticos
http://www.razon.com.mx/spip.php?article92573
Penetration Testing Framework 0.59
http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html
Instalación de Ntop
http://blog.unlugarenelmundo.es/2013/03/25/instalacion-y-primeros-pasos-con-ntop-5-en-debian-6/
¿Qué es ISACA?
http://www.isaca.org.mx/index.html
ESET Security Report Latinoamérica 2013
http://www.welivesecurity.com/wp-content/uploads/2014/01/informe_esr13.pdf