Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Laboratorio de Comunicación y Redes

Implementación de un dispositivo integrado de seguridad UTM y evaluación de la factibilidad de su configuración a través de la metodología de intrusión LPT

Trabajo Especial de Grado
presentado ante la Ilustre
Universidad Central de Venezuela
Por el Bachiller:

Luis A. Dávila B.
C.I.: 17023783
E-mail: luisdabe@gmail.com

Para optar al título de Licenciado en Computación

Tutores:
Eudes Carrero Moreno
Yalal Baladi Chaccour

Caracas, octubre de 2009

ACTA DEL VEREDICTO

Quienes suscriben, Miembros del Jurado designado por el Consejo de la Escuela de Computación para examinar el Trabajo Especial de Grado, presentado por el Bachiller Luis A. Dávila B. C.I.: 17.023.783, con el título **"Implementación de un dispositivo integrado de seguridad UTM y evaluación de la factibilidad de su configuración a través de la metodología de intrusión LPT"**, a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído el trabajo por cada uno de los Miembros del Jurado, se fijó el día 29 de octubre de 2009, a las 2:00 p.m., para que su autor lo defendiera en forma pública, en Planta Baja III de la Escuela de Computación**,** lo cual estos realizaron mediante una exposición oral de su contenido, y luego respondieron satisfactoriamente a las preguntas que les fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió aprobarlo.

En fe de lo cual se levanta la presente acta, en Caracas a los 29 días del mes de octubre de 2009**,** dejándose también constancia de que actuó como Coordinador del Jurado el Profesor Tutor Eudes Carrero Moreno.

Prof. Eudes Carrero Moreno
(Tutor)

Lic. Yalal Baladi Chaccour
(Jurado Principal)

Prof. Omaira *Rodríguez*
(Jurado Principal)

Agradecimientos

Dedicado especialmente a mí madre y hermana, cumpliendo una meta más de muchas por venir les debo mucho.

A Dios, por cada una de las oportunidades que me ha brindado a lo largo de mi vida, por darme la fortaleza para superar los obstáculos y permitirme alcanzar cada una de mis metas.

A mis padres, Hector y Maria, por ofrecerme su apoyo incondicional ante cualquier situación, por cada palabra de aliento y consejo ante los obstáculos, por estar siempre conmigo, por confiar en mi y por ser mis guías y amigos incomparables.

A mis tíos, abuelos, primos y demás familiares, por su apoyo, por tener siempre la disposición de ayudarme y alentarme a continuar en cada uno de los proyectos que me he planteado.

A los tutores, Prof. Eudes Carrero y Yalal Baladi Chaccour, por haberme tomado en cuenta para la creación de este proyecto, por su profesionalismo, por su disposición y guía durante el desarrollo del presente Trabajo Especial de Grado.

A mi compañera de estudio alias DIAZKARA por su gran apoyo y contribución con el desarrollo del presente T.E.G.

A mi compañeros de la universidad, por su gran apoyo y dedicación, por brindarme su confianza y lo más valioso SU AMISTAD.

A mis amigos en general, por los momentos especiales compartidos, porque me han apoyado siempre y han confiado en mí.

A cada uno de los profesores de la Escuela de Computación, por contribuir en mi formación como profesional y ayudarme a alcanzar este objetivo.

A todas aquellas personas que de alguna manera han contribuido en la creación de este proyecto y que nos han apoyado.

RESUMEN

TÍTULO:
Implementación de un dispositivo integrado de seguridad UTM y evaluación de la factibilidad de su configuración a través de la metodología de intrusión LPT.

AUTOR:
Luis A. Dávila B.

TUTORES:
Prof. Eudes Carrero
Lic. Yalal Baladi Chaccour

El presente Trabajo Especial de Grado consiste en evaluar la factibilidad de la configuración de un UTM (*Unified Threat Management*) Firebox 750e *Watchguard*, el cual permite la administración de la red y proporciona seguridad a la misma, a través de la metodología de intrusión LPT (*Licensed Penetration Tester*).

El fuerte de los dispositivos UTM es la integración de los diferentes servicios de seguridad en un solo dispositivo, mediante el cual se provee de manera centralizada la seguridad y administración de la red, facilitando la labor del administrador de red y del analista de seguridad. Es importante acotar que la instalación y configuración descritas en el T.E.G. son genéricas para cualquier dispositivo UTM de la marca *Watchguard*.

El trabajo se inicia con un estudio teórico de los aspectos más relevantes que se deben tomar en consideración en lo que a seguridad informática se refiere y un análisis de las técnicas más comunes utilizadas por los *hackers*.

Para la instalación del dispositivo se utilizan las recomendaciones del fabricante y para su configuración se toma en cuenta la política de uso de internet de la institución y sus requerimientos en cuanto al servicio. Se aplica la metodología LPT al dispositivo para verificar la factibilidad de la configuración del UTM.

Los dispositivos UTM brindan protección de *Firewall* convencional, protección *Antispam* - *Antiphishing* - Filtro de contenidos - Antivirus y Detección/Prevención de Intrusos IDS(*Intrusion Detection System*) / IPS (*Intrusion Prevention System)*. Estos dispositivos también permiten la creación de redes VPN (*Virtual Private Network*), utilizar protocolos de ruteo, traducciones de direcciones y registro de *logs*, entre otros.

La metodología para pruebas de intrusión LPT es propia de la casa de consultores de seguridad EC Council, la cual define una serie de pasos para probar la seguridad de diferentes equipos, aplicaciones y entornos de trabajo.

Palabras Clave: UTM, seguridad informática, LPT, *hackers*, servicios de seguridad.

Contenido

Índice de Figuras

Índice de Tablas

Introducción.

El comercio electrónico, las operaciones entre negocios en línea y la conectividad global se han convertido en componentes vitales de una estrategia comercial de éxito y las empresas u organizaciones públicas y privadas han adoptado procesos y prácticas de seguridad para proteger la información. La mayoría de las empresas u organizaciones mantienen una política de seguridad eficaz para evitar fraude, vandalismo, sabotaje o ataques de denegación de servicio pero subestiman las políticas de seguridad ya que no realizan pruebas de la red ni de los sistemas de seguridad para garantizar que funcionan como se espera.

Las políticas de seguridad de las empresas u organizaciones se basan en los dispositivos a ser utilizados para lograr la seguridad bajo ciertos requerimientos y un esquema organizado. Existen una gran variedad de dispositivos entre los que destacan los *Firewall*, los IPS (Intrusion Prevention Systems), los IDS (Intrusion Detection Systems), los bloqueadores de correo no deseado y los antivirus.

La mayoría de las empresas u organizaciones, han invertido enormemente en productos y servicios de seguridad para proteger sus redes y sistemas de hackers. Muchas de esas empresas no dan el último paso, el cual involucra realizar pruebas de intrusión en redes y dispositivos mediante herramientas y metodologías, las cuales, ayudan a identificar vulnerabilidades que permiten refinar la política de seguridad de una empresa y así poder garantizar que dicha política ofrezca la protección que la empresa u organización necesita y espera.

En el presente trabajo de investigación se consideraron los diferentes esquemas existentes, los ataques y técnicas empleadas por los hackers y toda la información relacionada que respalda a la Propuesta de Trabajo Especial de Grado, la cual se ha estructurado en cinco (5) capítulos que explican los diferentes aspectos tomados en cuenta durante la implementación y verificación del dispositivo integrado de seguridad UTM (Unified Threat Management). A continuación se ofrece un breve resumen del contenido de cada uno de los capítulos:

- **Capítulo 1 (El Problema):** Plantea los diferentes enfoques desde los que puede ser estudiado el problema junto al análisis de la solución, mostrando en detalle los objetivos y el alcance del presente Trabajo Especial de Grado.

- **Capítulo 2 (Marco Conceptual):** Presenta las bases teóricas que fueron estudiadas y sobre las que se fundamenta la implementación y verificación del dispositivo UTM.

- **Capítulo 3 (Marco Metodológico):** Describe la metodología utilizada y otros aspectos relevantes a tomar en cuenta para la implementación y verificación del dispositivo UTM.

- **Capítulo 4 (Marco Aplicativo):** Explica en detalle las diferentes etapas del proceso de implementación mediante las metodologías utilizadas.

- **Capítulo 5 (Pruebas y Resultados):** En este capítulo se presenta la aplicación de la metodología LPT en la institución y los resultados obtenidos.

- **Capítulo 6 (Trabajos a Futuro):** Comprende un conjunto de recomendaciones hechas a la institución para su implementación en el mediano plazo.

- **Capítulo 7 (Conclusiones):** Presenta las conclusiones obtenidas a partir del Trabajo Especial de Grado.

El autor pide disculpas por la utilización de términos no propios del idioma español. Los mismos obedecen a tecnicismos derivados del idioma inglés que imposibilitan su traducción literal

1. El Problema.

1.1 Planteamiento del problema

La vulnerabilidad de las organizaciones en materia de tecnología de la información se hace cada día más crítica, lo que ha impulsado la necesidad de contar con mecanismos eficientes que garanticen la protección del recurso principal de toda organización, como lo es la información.

Los diferentes departamentos que constituyen una institución interactúan constantemente con bases de datos, realizando consultas en tiempo real para el desenvolvimiento de sus funciones propias. Es por ello que se ha incrementado la inversión en tecnologías de punta y en sistemas que garantizan protección a la red contra ataques informáticos mixtos. Esto se logra a través de la integración de diferentes servicios de seguridad en un sólo dispositivo, siendo de nuestro interés la validación de la configuración de los servicios requeridos por la organización a través de un dispositivo UTM(*Unified Threat Management*), tales como: FTP(*File Transfer Protocol*), HTTP(*HyperText Transfer Protocol*) y VPN(*Virtual Private Network*).

1.2 Objetivos

1.2.1 Objetivo general

Implementar un dispositivo UTM y evaluar la factibilidad de su configuración empleando la metodología de intrusión LPT (*Licensed Penetration Tester*).

1.2.2 Objetivos específicos

- Evaluar las vulnerabilidades de la red actual de la institución.

- Proponer un esquema de red para la institución.

- Seleccionar el dispositivo UTM más adecuado para la institución.

- Configurar un dispositivo integrado de seguridad para la protección y administración de la red.

- Verificar la correcta configuración del UTM realizando pruebas de intrusión de acuerdo a la metodología LPT.

1.3 Justificación

En este trabajo se plantea como solución la implementación de un dispositivo UTM, la cual proporciona a través de una administración sencilla, seguridad ante ataques informáticos mixtos mediante la integración de los diferentes servicios de seguridad como lo son: bloqueo de correo no deseado, antivirus, sistema de prevención/detección de intrusos, filtros de contenido web y *firewall*. Procesando y analizando todo el contenido antes de que entre a la red, evitando así la infección por virus, gusanos, troyanos, correos no deseados, páginas web maliciosas y accesos no autorizados.

Una ventaja clave en el empleo de los dispositivos UTM es su bajo costo en adiestramiento al usuario, dado que se muestra los diferentes servicios como un todo y no de manera individual, así mismo, se debe tomar en cuenta los costos relativamente bajos de renovación de las licencias.

1.4 Alcance

Al finalizar el proyecto se espera que la institución cuente con un dispositivo de seguridad UTM funcional y verificado a través de la metodología LPT. Se espera que la administración de la red se realice de forma sencilla y segura.

2. Marco Conceptual

TERMINOLOGIAS Y FASES DE LOS HACKERS

2.1 Qué es una *firewall*

Un *firewall* es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El *firewall* puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con dos o más interfaces de red en la que se establecen unas reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no.

2.1.1 Esquemas de *firewall*

- Esquema de *firewall* típico entre red local e internet

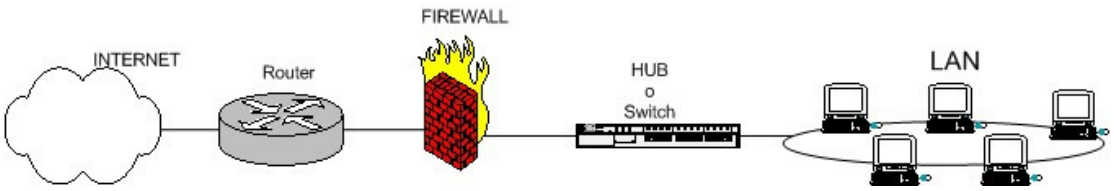


Figura 1. Firewall entre LAN e internet

Fuente: http://www.wikilearning.com/tutorial/iptables_manual_practico-que_es_un_*firewall*/6439-1

Esquema típico de *firewall* para proteger una red local conectada a internet a través de un *router*. El *firewall* debe colocarse entre el *router* (con un único cable) y la red local (conectado al *switch* o al *hub* de la LAN (Local Area Network)). [6]

- Esquema de *firewall* entre red local e internet con zona DMZ (DeMilitarized Zone) para servidores expuestos

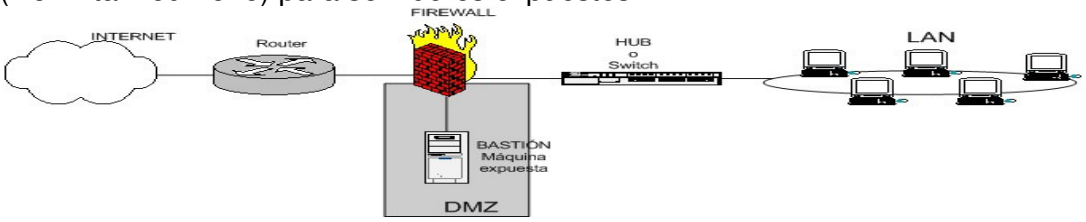


Figura 2. Firewall entre LAN con zona DMZ e internet

Fuente: http://www.wikilearning.com/tutorial/iptables_manual_practico-que_es_un_*firewall*/6439-1

Dependiendo de las necesidades de cada red se puede colocar uno o más *firewall*s para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc.), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en un lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada.

En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el *firewall* [6]

- Esquema de *firewall* entre red local e internet con zona DMZ para servidores expuestos creado con doble *firewall* (perímetro)

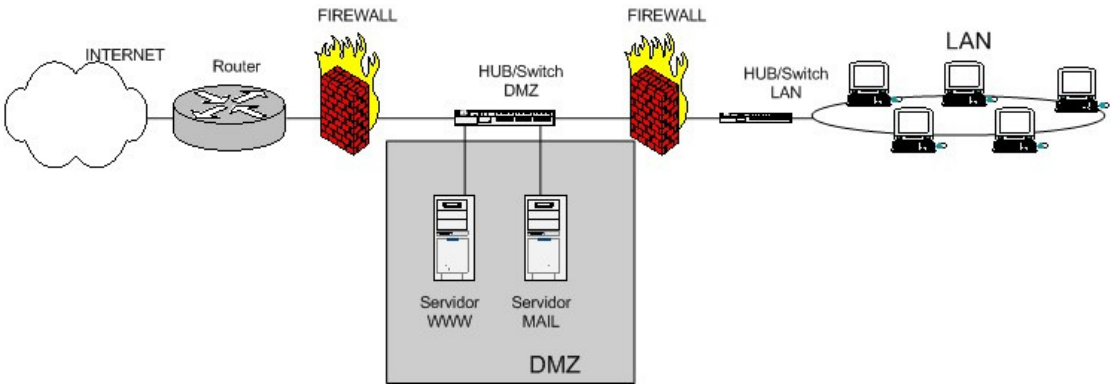


Figura 3. Doble firewall entre zona DMZ con LAN e internet

Fuente: http://www.wikilearning.com/tutorial/iptables_manual_practico-que_es_un_*firewall*/6439-1

Esta estructura de DMZ puede hacerse también con un doble *firewall* (aunque como se ve se puede usar un único dispositivo con al menos tres interfaces de red). Sería un esquema como este:

Los *firewall*s se pueden usar en cualquier red. Es habitual tenerlos como protección de internet en las empresas u organizaciones, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior; esto último se hace con el *firewall* o frecuentemente con un proxy (que también utilizan reglas, aunque de más alto nivel). También, en empresas de hospedaje con muchos servidores alojados lo

normal es encontrarnos uno o más *firewall*s ya sea filtrando toda la instalación o parte de ella. [6]

2.2 Qué es UTM

UTM (*Unified Threat Management*) o **Gestión Unificada de Amenazas** es un dispositivo de red que además de proporcionar los servicios ofrecidos por un *firewall* convencional, incluye también protección Antispam - Antiphishing - Filtro de contenidos - Antivirus - Detección/Prevención de Intrusos (IDS/IPS). La filosofía de un UTM es procesar y analizar todo el contenido antes de que entre a la red corporativa, logrando así limpiar la red de virus, gusanos, troyanos, spyware, correo spam, páginas web maliciosas mediante filtros avanzados y protegiendo contra accesos no autorizados.

El término fue utilizado por primera vez por Charles Kolodgy de International Data Corporation (IDC) en 2004. [8]

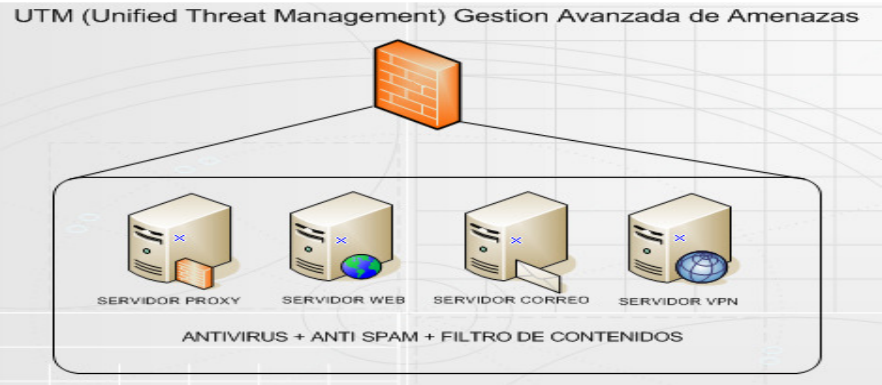


Figura 4. Gestión avanzada de amenazas

Punto de transición a las soluciones de seguridad integradas

Las soluciones de seguridad tradicionales para resolver las principales amenazas y problemas de productividad, son difíciles de implementar, administrar y actualizar, lo que aumenta la complejidad operacional y gastos generales. En su lugar, las organizaciones demandan en la actualidad un enfoque integrado de seguridad de la red y la productividad que combina la gestión de las tecnologías. Todas estas desventajas llevan a las

organizaciones a implementar políticas de seguridad mínimas e inferiores a lo deseado. UTM puede ayudar a superar estos problemas. En resumen, la transición desde dispositivos que utilizan tecnologías individuales a aparatos de seguridad integrada es en gran parte debido a la relación coste-eficacia y facilidad de gestión de dispositivos UTM. [8]

Punto de falla o limitación de UTM

La mayor desventaja de un UTM se encuentra en el hecho de que es un complejo conjunto de soluciones de seguridad y el fracaso de la solución de una sola de las tecnologías puede afectar todo el sistema. Esto se puede remediar mediante el uso de alta disponibilidad (HA: High Availability) de tecnología. [9]

2.2.1 Características de un UTM

Los dispositivos UTM proporcionan de manera general:

- **Filtrado de contenido web:** Mediante el cual se controla e informa de que manera los empleados usan el acceso a la web.

- **Detección y/o prevención de intrusos:** Realiza análisis sobre los ataques convencionales y de denegación de servicio, el cual a través de un conjunto de firmas reacciona proactivamente a dichos eventos y bloquea las actividades sospechosas.

- **VPN (Virtual Private Network):** Permite una conectividad segura entre sucursales y personal móvil.

- **Ruteo:** Capacidad de utilizar protocolos de enrutamiento tanto estáticos como dinámicos como por ejemplo OSPF (Open Shortest Path First), RIP (Routing Information Protocol) V1 y V2, etc.

- **Asignación de dirección IP (Internet Protocol):** Las cuales pueden ser estáticas o dinámicas con DHCP (Dynamic Host Configuration Protocol).

- **Creación de redes:** En el cual se proporciona independencia de puertos, de interfaces, posibilidad de creación de VLAN (Virtual Local Area Network), balanceo de carga y capacidades de VoIP (Voice over Internet Protocol).

- **Traducción de direcciones:** NAT (Network address translation) estática y dinámica, IPSec (Internet Protocol Security) NAT.

- **Logs:** Registro de eventos en general. [10]

Las razones para la implementación de un UTM:

- Reducir el costo de renovación anual de los mantenimientos.

- Reducir el costo en capacitación.

- Reducir el tiempo de administración.

- Seguridad de oficinas centrales, delegaciones, sitios remotos, etc.

- Ampliar las funcionalidades de cortafuegos tradicional

- Mejorar los niveles de servicio.

- Focalizarse en el negocio. [10]

Identidad diferenciada de usuarios

Los dispositivos UTM son la próxima generación de soluciones de seguridad que ofrecen protección completa contra las amenazas mixtas emergentes. En un dispositivo integrado de seguridad UTM es sencillo identificar no sólo las direcciones IP en la red, sino que adicionalmente, proporciona información de la identidad diferenciada de cada usuario en la red junto con los datos de registro de la misma. Permiten la creación de la identidad basada en las políticas de acceso de red para los usuarios individuales, ofreciendo una completa visibilidad y control sobre las actividades de la red. La identidad basada en las políticas comprende todo un conjunto de características que permite a las empresas identificar los patrones de comportamiento de los usuarios o grupos concretos que puede significar el mal uso, intrusiones no autorizadas, o ataques maliciosos desde el interior o fuera de la empresa.

La fuerza de esta tecnología es que está diseñada para ofrecer seguridad global a través de la integración de los diferentes servicios de seguridad existentes, siendo fácil de gestionar. [8]

Cumplimiento de regulaciones

Una de las características más relevante de los dispositivos UTM es que ofrecen lo mejor de la tecnología en su clase y que puede manejar el entorno regulador cada vez más en todo el mundo ya que cumplen con regulaciones como HIPAA(Health Insurance Portability and Accountability Act), GLBA (*Gramm-Leach-Bliley* Financial Services Modernization Act), PCI-DSS (Payment Card Industry Data Security Standard) , FISMA (Federal Information Security Management Act), CIPA (Classified Information Procedures Act), SOX (Sarbanes-Oxley Act). Las cuales exigen controles de acceso y de auditoría que cumplan con los datos de control de fugas. [10]

2.3 Comprendiendo la terminología *hacker*

Para una correcta interpretación del material a continuación expuesto hay que tener claro los siguientes conceptos:

2.3.1 Amenaza: es un entorno o situación que podría conducir a una potencial violación de la seguridad.

2.3.2 Vulnerabilidad: es la existencia de una falla de software, lógica de diseño, o error de aplicación que puede conducir a un acontecimiento inesperado e indeseada mala ejecución de las instrucciones del sistema o dañar el mismo.

2.3.3 Exploit: es una serie de pasos bien definidos para quebrantar la seguridad de los sistemas de información a través de una vulnerabilidad.

Los exploit se clasifican en:

- Exploit remoto: que trabaja a través de una red y explota vulnerabilidades de seguridad sin ningún tipo de acceso al grupo de sistemas vulnerables.
- Exploit local: que requiere acceso al sistema para escalar privilegios. [1] pág. 2

2.4 Identificando los diferentes tipos de áreas del *hacking*

Existen muchos métodos y herramientas para encontrar vulnerabilidades, correr exploits y comprometer sistemas. Troyanos, backdoors, *sniffer*s, rootkits, exploits, buffer overflow e inyecciones SQL (*Structured Query Language)* son las técnicas y herramientas que pueden ser usadas para hackear un sistema o una red. Estas técnicas de ataque se verán posteriormente. La mayoría de las herramientas de hacking se aprovechan de vulnerabilidades en una de las siguientes 4 áreas:

- **Sistemas Operativos**: Muchos administradores de sistema instalan sistemas operativos con las configuraciones por defecto y esto ocasiona una gran vulnerabilidad además de que se encuentran sistemas operativos sin actualizar o parchear lo cual da como resultado una gran facilidad llevar a cabo vulnerabilidades ya conocidas.

- **Aplicaciones**: Las aplicaciones usualmente no son probadas para vulnerabilidades cuando los desarrolladores están escribiendo el código, lo cual puede dejar fallas en la programación del software que un hacker puede aprovechar, como por ejemplo la falta de una validación la cual permita un buffer overflow.

- **"Shrink-wrap" code**: Muchos programas vienen con características extras que el usuario común no conoce, el cual puede ser usado para explotar el sistema. Un ejemplo son los macros en Microsoft Word, el cual le permiten a un hacker la ejecución de programas o rutinas dañinas desde dentro de la aplicación.

- **Configuraciones incorrectas**: Los sistemas pueden estar configurados de manera incorrecta o por debajo de las configuraciones comunes de seguridad para que sea más fácil de usar por parte del usuario, lo cual resulta en vulnerabilidades y ataques.

Adicionalmente, a los varios tipos de áreas del hacking que pueden ser usadas por un hacker, hay diferentes tipos de ataques. Los ataques activos realmente alteran el sistema o la red que están atacando, mientras que los ataques pasivos intentan obtener información del sistema. Los ataques activos afectan la disponibilidad, la integridad y la autenticidad de los datos como por ejemplo una denegación de servicio mientras que los ataques pasivos son rupturas de la confidencialidad. También adicional a las categorías activas y pasivas, ambas pueden ser definidas como un ataque interno o externo, un ataque originado desde adentro de los perímetros de seguridad de una organización es un ataque interno mientras que un ataque externo es originado desde afuera del perímetro de seguridad de la organización, como por ejemplo internet o administración remota. [1] pág. 3

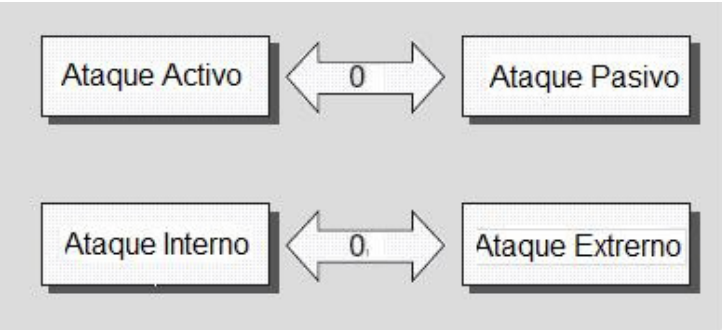


Figura 5. Tipos de atáques

Los hacker siguen 5 pasos para lograr sus objetivos, también conocido como fases del hacking y son:

- **Reconocimiento pasivo y activo**

Reconocimiento pasivo implica la recopilación de información respecto a un objetivo potencial, sin que la persona o empresa tenga conocimiento de ello. Puede ser tan simple como observar un edificio para identificar a qué hora los empleados entran al edificio o salen, sin embargo este se realiza generalmente a través de búsquedas por internet o "googleando" a un individuo o compañía para obtener información. Este proceso es llamado generalmente recopilación de información. La ingeniería social, el "sniffing" y el análisis de basura (dumpster) son también considerados métodos pasivos de recopilación de información.

Reconocimiento activo implica probar la red para descubrir computadoras individuales, direcciones IP y servicios en general de la red. Esto generalmente implica mayor riesgo de detección que un reconocimiento pasivo. El reconocimiento activo le proporciona al hacker las condiciones de las medidas de seguridad del lugar, pero el proceso incrementa la oportunidad de ser capturado o al menos ser sospechoso.

- **Escaneo**

La fase de exploración implica tomar la información descubierta durante la fase de reconocimiento y usar esta para examinar la red. Las herramientas que un hacker puede utilizar durante la fase de exploración incluyen scanner de puertos, creadores de mapas de red, barridos de red y scanner de vulnerabilidades. Los hackers están en búsqueda de cualquier información que pueda ayudarlos a perpetrar el ataque como por ejemplo, nombre de computadoras, direcciones IP y cuentas de usuarios.

- **Ganando acceso**

En esta fase es donde las vulnerabilidades descubiertas durante la fase de reconocimientos y exploración son ahora explotadas para ganar acceso. El método de conexión que el hacker usa puede ser LAN, acceso local a un computador, internet o desconectado. Ejemplos de estos ataques son buffer overflow, DoS (Denial of Service), entre otros.

- **Manteniendo el acceso**

Una vez que los hackers han ganado acceso, ellos desean continuar teniendo acceso en el futuro, a veces, los hackers endurecen el sistema de otros hackers o personal de seguridad asegurando su acceso exclusivo con puertas traseras, rootkits y troyanos. Una vez que el hacker se apodera del computador, puede utilizar dicho computador como base para otros ataques y en ocasiones la computadora en cuestión es llamada sistema zombie.

- **Cubriendo las pistas**

Una vez que los hackers han logrado ganar y mantener acceso, ellos cubren sus pistas para evitar ser detectados por el personal de seguridad, para continuar usando el sistema vulnerado, remover evidencia de hacking o para evitar acciones legales en su contra. Los hackers tratan de remover todos los rastros del ataque como archivos log o alarmas IDS. Como ejemplos de ataques en esta fase se encuentra la esteganografia, la alteración de archivos log y la utilización de túneles, la cual será explicada en los próximos capítulos. [1] pág. 4-6

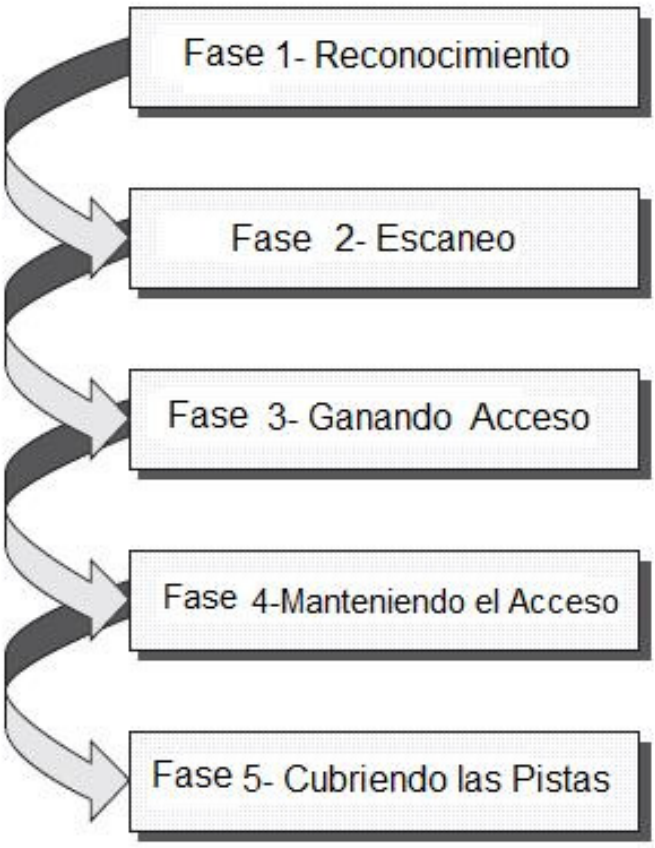


Figura 6. Pasos de un hacker

2.5 Diferentes tipos de clases de *hackers*

- **White hats**: Son los hackers éticos que usan sus habilidades para propósitos defensivos, son generalmente profesionales de la seguridad con conocimiento de hacking que se encargan de encontrar debilidades e implementar contramedidas.

- **Black hats**: Son los hackers o crackers malicioso que utiliza sus habilidades para propósitos maliciosos e ilegales. Ellos rompen y violentan la integridad del sistema de maquinas remotas con intención maliciosa. Habiendo ganado acceso no autorizado, los hackers "black hat" destruyen información vital, deniegan servicios de usuarios legítimos y básicamente causan problemas a la víctima.

- **Grey hats**: Son hackers que pueden trabajar ofensivamente o defensivamente, dependiendo de la situación. Esta es la línea divisora entre hackers y crackers. [1] pág. 6

Una técnica utilizada comúnmente por los hackers es Footprinting, el cual es el proceso de crear un mapa de los sistemas y redes de una organización. Se comienza determinando el sistema del objetivo, sus aplicaciones o la ubicación física del mismo. Por lo general los hackers dedican un 90% del tiempo a la obtención de información de la víctima y 10% del tiempo lanzando el ataque.

La obtención de información puede ser dividido en siete (7) pasos lógicos los dos primeros son cubiertos por la técnica de footprinting mientras que los otros cinco (5) están cubiertos en la parte de escaneo y enumeración y son:

- Descubrir la información inicial.

- Localizar el rango de IP de la red.

- Determinar maquinas activas.

- Descubrir puertos abiertos.

- Detectar sistemas operativos.

- Descubrir servicios en los puertos.

- Mapa de la red.

Algunos de los software más comunes para la obtención de la información incluyen:

- Domain name lookup

- Whois

- Nslookup

- Sam Spade

La técnica de footprinting es muy utilizada por la inteligencia competitiva ya que obtendrían información acerca de los productos del competidor, mercadeo y tecnologías. Para usarse posteriormente para comparación de productos, técnicas de mercadeo y tener una mayor comprensión de cómo los competidores están posicionando sus productos o servicios.

Una poderosa herramienta es Nslookup la cual realiza consultas a los servidores DNS (Domain Name System) para obtener su información registrada.

Whois evolucionó del sistema operativo UNIX y actualmente se puede encontrar en diferentes sistemas operativos así como en herramientas de hacking e internet. Esta herramienta realiza consultas a la base de datos **para** recuperar información de contacto acerca de un individuo u organización que mantiene un registro de dominio.

Traceroute es una herramienta de seguimiento de paquetes que está disponible en la mayoría de los sistemas operativos, trabaja mandando un ICMP (Internet Control Message Protocol) echo a cada *router* o Gateway a lo largo del camino, cuando un mensaje ICMP es enviado de vuelta al *router* el TTL (Time To Live) decrece en uno por cada *router* a lo largo del camino.

La ingeniería social es un método no técnico de irrumpir en sistemas y redes, es el proceso de engañar a usuarios de un sistema y convencerlos de que proporcionen información que puede ser utilizada para vencer o traspasar mecanismos de seguridad, la ingeniería social utiliza la influencia y persuasión para engañar dichas personas con el propósito de obtener información o persuadir a alguna victima de realizar alguna acción.

La ingeniería social se puede dividir en dos tipos

- **Basado en humanos**: este tipo de ingeniería social hace referencia a interacción de persona a persona para la obtención de la información deseada.

- **Basado en computadoras:** este tipo de ingeniería social se refiere a que un software realiza varios intentos para obtener la información deseada, por ejemplo enviando a un usuario un email pidiéndole que ingrese nuevamente su password en una página web para confirmarlo. [1] pág.20-23

2.6 Escaneo y enumeración

Durante la exploración, los hackers continúan recaudando información acerca del objetivo como su IP, sistemas operativos, servicios y aplicaciones instaladas con lo cual los hackers pueden decidir cual tipo de exploit pueden utilizar para hackear el sistema.

2.6.1 Escaneado de puertos: Es el proceso de identificar puertos TCP/IP (Transfer Control Protocol/ Internet Protocol) abiertos y disponibles en un sistema. Las herramientas de escaneo de puertos permiten a los hackers tener conocimientos de que servicios están corriendo en un sistema a través de los puertos *bien conocidos.*

2.6.2 Escaneado de red: es el procedimiento de identificar computadores activos en una red, ya sea para atacarlo o realizar una evaluación de seguridad de la red. Los computadores están identificados de manera univoca por su dirección IP.

2.6.3 Escaneado de vulnerabilidad: es el proceso de identificar proactivamente las vulnerabilidades de un computador en una red, generalmente un escáner de vulnerabilidades primero identifica el sistema operativo y su versión, para así posteriormente identificar debilidades o vulnerabilidades en el sistema operativo y así el hacker poder explotarlas con el objetivo de ganar acceso al sistema.

Un sistema de detección de intrusos IDS por sus siglas en ingles (Intrusion Detection System) o un sofisticado profesional de la seguridad informática con las herramientas apropiadas puede detectar un escaneo de puerto activo. Las herramientas de escaneo de puertos prueban los puertos TCP/IP buscando para ver cuales se encuentran abiertos en un rango de direcciones IP y estos intentos puedes ser reconocidos por la mayoría de los IDS. [1] pág.42

Tipo de Escaneo	**Propósito**
Escaneo de puertos	Determinar puertos abiertos y servicios
Escaneo de red	Determinar computadores activos
Escaneo de vulnerabilidades	Detectar vulnerabilidades conocidas

Tabla 1: Tipos de Escaneos

2.6.4 Metodología de escaneo de los ethical hackers.

Los hackers utilizan básicamente una metodología de escaneo de ocho (8) pasos la cual de igual forma es utilizada por los ethical hackers o “White hats”, la diferencia de estos últimos es que lo realizan para garantizar que ningún sistema o vulnerabilidad es pasada por alto y que los hackers mal intencionados no logren obtener, o al menos no de manera sencilla, la información sobre la red para desarrollar un ataque. Los pasos anteriormente mencionados son:

- Comprobación de sistemas activos.
- Comprobación de puertos abiertos.
- Identificación de servicios.
- Identificación de sistemas operativos.
- Escaneo de vulnerabilidades.
- Dibujar diagrama de red de computadores vulnerables.
- Preparación de proxies.
- Ataque. [1] pág.43

Técnica de barrido de *ping*

La metodología de escaneo comienza verificando cuales sistemas se encuentran activos en la red, lo cual significa que ellos responden a una petición de conexión. La manera más simple, aunque no necesariamente la

más precisa para determinar que sistemas se encuentran activos, es llevando a cabo un barrido de *ping* de un rango de direcciones IP. Todos los sistemas que responden son considerados activos en la red.

El escaneo ICMP es el proceso de mandar una petición ICMP o *ping* a todos las computadoras de una red para determinar cuales se encuentran levantados. Un beneficio del escaneo ICMP es que puede correr en paralelo, lo cual significa que todos los sistemas pueden ser escaneados al mismo tiempo, por lo cual se va a poder identificar las computadoras activas de toda una red de manera mucho más rápida.

Un problema considerable con este método es que un software personal de *firewall* o *firewall*s basados en red pueden bloquear a un sistema de responder a barridos de *ping* y otro problema no menos importante es que el computador tiene que estar prendido y funcionando para que pueda ser escaneado e identificado. [1] pág.44

Como detectar barridos de *ping*

La mayoría de los IDS/IPS detectarán y alertarán a los administradores de seguridad de que un barrido de *ping* está ocurriendo en la red. Muchos *firewall*s y servidores proxy pueden bloquear las respuestas de *ping*, lo cual no va a permitir a los hackers asegurar que computadores se encuentran activos o no, hay que tomar en cuenta que porque se realice un barrido de *ping* y no se obtenga respuesta de las víctimas, no quiere decir que no se encuentren disponibles. [1] pág.44

Escaneando puertos e identificando servicios

Verificar puertos abiertos es el segundo paso en la metodología de escaneo de un “ethical hacker”, el método de escaneo de puertos es la utilizada para buscar puertos abiertos. Este proceso involucra probar cada puerto en un computador para determinar que puertos se encuentran abiertos, por lo general esto proporciona más valor que barrido de *ping* ya que nos puede dar información acerca de un computador y vulnerabilidades en el sistema.

La identificación de los servicios es el tercer paso en la metodología del escaneo de un “ethical hacke”r, es llevada a cabo generalmente utilizando las mismas herramientas que para el escaneo de puertos. Una vez identificados

puertos abiertos, los hackers pueden acceder a los servicios asociados a cada puerto. [1] pág.45

2.7 Herramienta NMAP

NMAP es una herramienta que rápidamente y eficientemente desarrolla barridos de *ping*, escaneo de puertos, identificación de servicios, detección de direcciones IP y detección de sistemas operativos. NMAP tiene la capacidad de escanear un gran número de maquinas en una sola sesión. Esta herramienta es soportada por varios sistemas operativos dentro de los que se incluyen Unix, Windows y Linux.

Los puertos son determinados en NMAP por tres (3) estados que son: abierto, filtrado y no filtrado.

Abierto significa que la maquina acepta entrada de peticiones en determinado puerto, filtrado significa que un *firewall* o un filtro de red está realizando un análisis sobre los puertos evitando así a NMAP descubrir si se encuentra abierto. No filtrado significa que se determinó que el puerto se encuentra cerrado y que no se encuentra ningún *firewall* o filtro interfiriendo con las peticiones de NMAP.

NMAP soporta diversos tipos de escaneos los cuales son los siguientes:

- **SYN (synchrony) o escaneo sigiloso:** es también llamado *medio abierto* porque no completa el enlace de tres vías TCP (Transfer Control Protocol), en este tipo de escaneo el hacker envía un paquete SYN al blanco, si una trama SYN/ACK (synchrony / Acknowledge) es recibida de vuelta entonces se asume que el blanco completaría la conexión y que el puerto se encuentra abierto. Si un RST (Reset) es recibido de vuelta se asume el puerto se encuentra cerrado. La ventaja de este tipo de escaneo es que muy pocos sistemas de IDS registran esto como un ataque o intento de conexión.

- **XMAS:** se envía un paquete con las banderas de FIN (finish), URG (urgent) y PSH (push) encendidas. Si el puerto está abierto no habrá respuesta, pero si el puerto se encuentra cerrado el blanco responde

con un paquete RST/ACK. El escaneo XMAS trabaja solamente en blancos que sigan el RFC (*Request For Comments)* 793. Es decir, que tengan dicha implementación de TCP/IP y hay que tomar en cuenta que este tipo de escaneo no trabaja sobre ninguna versión de Windows.

- **FIN:** Es similar a un escaneo XMAS pero se envía un paquete con solo la bandera de FIN activa. El escaneo FIN recibe la misma respuesta y tiene las mismas limitaciones que XMAS.

- **NULL:** Es similar a XMAS y FIN en cuanto a limitaciones y respuestas, pero se manda un paquete al blanco con ninguna bandera activada.

- **IDLE:** Un escaneo IDLE usa una IP Spoofeada que no es más que hacerse pasar por otro usuario clonando su IP, para enviar un paquete SYN a un blanco. Dependiendo de la respuesta se puede determinar si el puerto se encuentra abierto o cerrado. El escaneo IDLE determina la respuesta del escaneo de puertos monitoreando el numero de secuencia de la cabecera IP. [1] pág.46-48

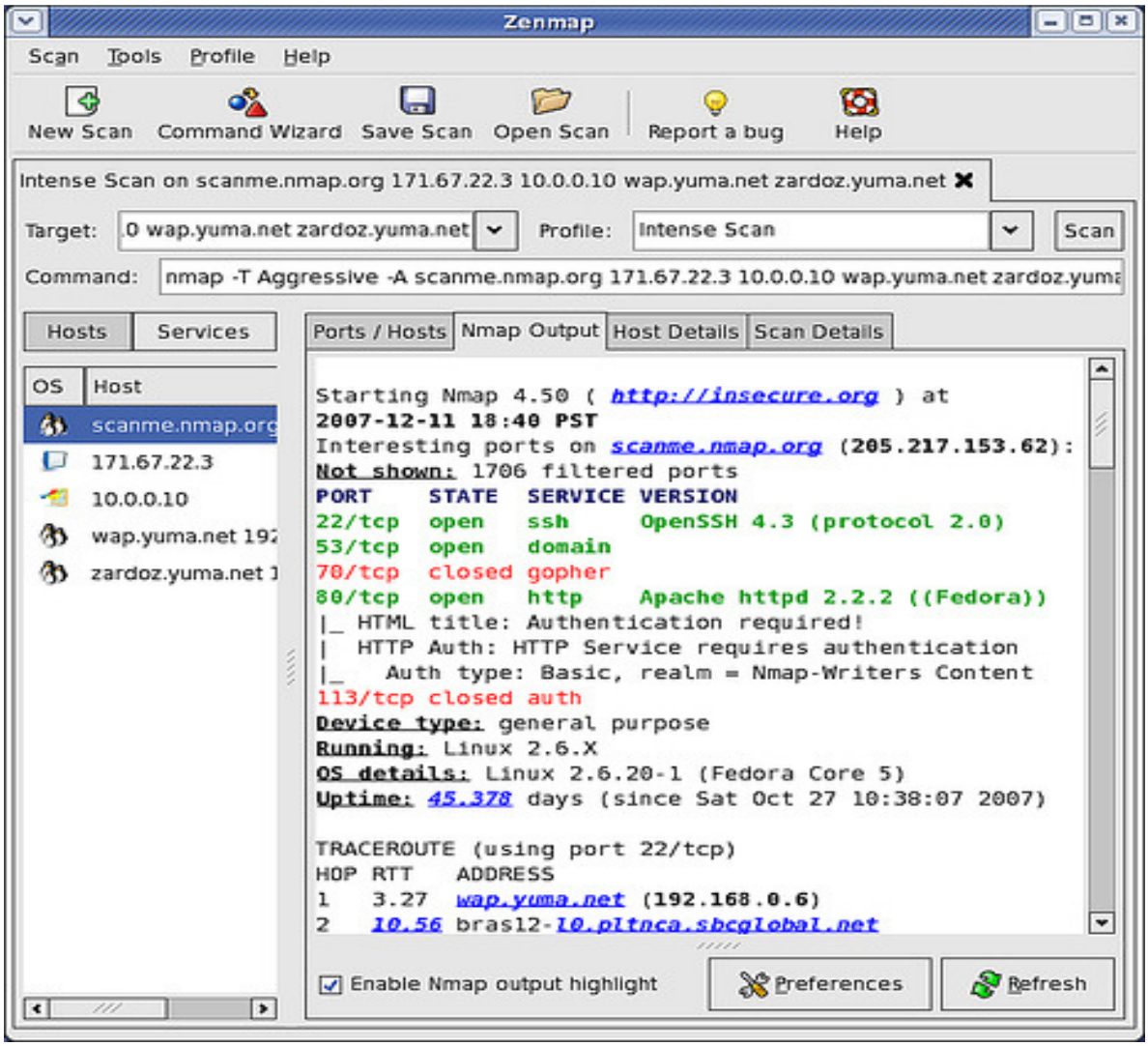


Figura 7. Imagen del programa NMAP

Fuente: http://farm3.static.flickr.com/2061/2109779977_b37fda78b2.jpg

2.8 Comprendiendo como los servidores *Proxy* son usados para lanzar un ataque

Preparar los servidores proxy es el penúltimo paso en la metodología de escaneo de un hacker. Un *servidor proxy* es un computador que actúa como intermediario entre el hacker y la computadora objetivo.

Usando un servidor proxy permite a un hacker volverse anónimo en la red. El hacker primero realiza una conexión al servidor proxy y entonces se envia una petición de conexión a la computadora objetivo a través de la conexión existente al proxy. Básicamente, el proxy es quien realiza las peticiones de

conexión al computador objetivo no desde la computadora del hacker, esto le permite navegar de manera anónima en la red y ocultar sus ataques. [1] pág.53

2.9 Comprendiendo las técnicas de túneles HTTP (*HyperText Transfer Protocol*)

Un método popular de traspasar un *firewall* o IDS o un protocolo bloqueado, como por ejemplo SMTP (*Simple Mail Transfer Protocol),* es a través de un protocolo permitido, como HTTP casi todos los IDS y *firewall* actúan como proxy entre la computadora de un cliente e internet y permite solamente el paso del tráfico definido como permitido, por ejemplo, la mayoría de las compañías permiten el tráfico http para que este sea usado para acceso a la web de manera benigna, sin embargo un hacker utilizando una herramienta que permita la creación de un túnel http puede ocultar protocolos potencialmente destructivos como mensajerías instantáneas, chat, FTP (File Transfer Protocol), entre otros. Haciendo creer al *firewall* y a los IDS que se está utilizando http. [1] pág.54

2.10 Comprendiendo las técnicas de *crackeo* de contraseñas

Muchos intentos de hackeos comienzan tratando de crackear claves o contraseñas. Las contraseñas son piezas claves de información que se necesita para acceder a un sistema. Los usuarios, cuando crean contraseñas con frecuencia seleccionan contraseñas que son propensas a ser crackeadas o en su defecto las reutilizan o son muy simples como por ejemplo el nombre de su perro de manera que le sea fácil de recordar, por consecuencia de esto la mayoría de las contraseñas son posibles de crackear y esto puede ser un trampolín para escalar privilegios, ejecutar aplicaciones, ocultar archivos y cubrir rastros. Las contraseñas pueden ser crackeadas de manera manual o automatizada, a través de herramientas que utilizan diccionarios o métodos de fuerza bruta.

El crackeo de contraseñas de manera manual involucra iniciar sesión con diferentes contraseñas, el hacker sigue los siguientes pasos:

- Encontrar una cuenta de usuario válida

- Crear una lista de contraseñas

- Ordenar las contraseñas comenzando con la de más alta probabilidad hasta la de menor probabilidad

- Probar las contraseñas hasta que se logre iniciar sesión

Una manera más eficiente de crackear contraseñas es obteniendo acceso a los archivos de contraseñas en un sistema, la mayoría de los sistemas usan un HASH de encriptación de una sola vía para almacenar la contraseña. Durante el proceso de inicio de sesión, la contraseña introducida por el usuario se le aplica el mismo proceso usando el mismo algoritmo y es comparado contra los archivos de contraseñas almacenados.

Las contraseñas son almacenadas en el archivo SAM (Security Accounts Management) en un sistema Windows y en un "shadow file" en un sistema Linux. [1] pág.68-72

2.11 Comprendiendo los *keyloggers* y otras tecnologías *spyware*

Si los intentos de obtención de contraseñas han fallado, entonces un keylogger es la herramienta predilecta para ser utilizada por un hacker, esta se puede implementar por hardware o software. Los keyloggers por hardware son pequeños dispositivos que se conectan entre el teclado y el computador, almacenando cada tecla presionada en un archivo o en una memoria del dispositivo, para lograr instalarlo se requiere de acceso físico a los sistemas.

Los keylogger por software son piezas sigilosas de software que se encuentran entre el hardware del teclado y el sistema operativo, de esta manera puede guardar cada pulsación del teclado y este tipo de software se puede desplegar en un sistema a través de troyanos y virus. [1] pág.78

2.12 Comprendiendo el aumento de privilegios

Escalar privilegios es el tercer paso en el ciclo hacking y significa básicamente agregar más derechos o permisos a una cuenta de usuario, dicho de otra forma la escalación de privilegios convierte una cuenta de usuario regular en una cuenta de administrador.

Generalmente, las cuentas de administrador tienen más privilegios y sus contraseñas son guardadas con más recelo. Si no es posible encontrar un nombre de usuario o contraseña de una cuenta con privilegios de administrador, entonces un hacker puede desear usar una cuenta con menores privilegios y en este caso se escalarían los privilegios de la misma. [1] pág.79

2.13 Ejecutando aplicaciones malignas

Una vez que el hacker logra tener acceso a una cuenta con privilegios de administrador el próximo paso a realizar es la ejecución de aplicaciones malignas en el sistema objetivo. El propósito de ejecutar aplicaciones malignas puede ser instalar una puerta trasera en el sistema o instalar un keylogger para obtener información confidencial, esencialmente cualquier cosa que el hacker desea hacer en el sistema. [1] pág.81

2.14 Comprendiendo como ocultar archivos

Un hacker puede desear ocultar archivos en un sistema para prevenir que sean detectados o guardar información de interés para el hacker de manera oculta, estos archivos puede ser usados para lanzar un ataque al sistema. Hay dos maneras de ocultar archivos en Windows, el primero es usando el comando *attrib* un ejemplo seria:

Attrib +h [file/directory]

La segunda forma y más usada para ocultar archivos en Windows es con *NTFS (*New Technology File System) *altérnate data streaming.* El sistema de archivo NTFS usado por Windows 2000, XP y otros sistemas operativos tienen una característica llamada *altérnate data stream* que permite almacenar información en archivos ocultos siendo enlazados a un archivo visible normal, estos no están limitados a tamaño y más de un stream puede ser enlazado a un archivo normal.

2.14.1 NTFS file streaming

Los pasos para crear y probar un NTFS file stream son:

- En la línea de comandos introducir **notepad test.txt.**

- Colocar alguna información en el archivo y guardarlo, posteriormente cerrar notepad.

- En la línea de comandos introducir **dir test.txt** y ver el tamaño del archivo.

- En la línea de comandos introducir **notepad test.txt:hidden.txt.** y escribir algún texto en el notepad guardarlo y cerrarlo.

- Visualizar el tamaño del archivo el cual debería ser el mismo tamaño que en el paso 3.

- Se abre test.txt y se verá solamente la información original.

- Introducir **type test.txt:hidden.txt** en la línea de comandos y se mostrara un mensaje de error de sintaxis.

2.14.2 Contra medida a NTFS stream

Para borrar un archivo stream primero se copia el archivo a una partición FAT (*File Allocation Table)* y luego se copia de vuelta a una partición NTFS. [1] pág.83

2.14.3 Comprendiendo la tecnología de la esteganografìa

Esteganografia es el proceso de ocultar información en otro tipo de archivos como imágenes o archivos de texto. Es un método bastante popular y se puede

ocultar cualquier tipo de información en imágenes, como números de tarjetas de crédito, cuentas bancarias secretas y cualquier tipo de información que pueda ser de interés.

La Esteganografia puede ser detectada por algunos programas pero es algo realmente difícil de lograr. [1] pág.48

2.15 Comprendiendo como cubrir las huellas y borrar rastros o evidencias

Una vez que los intrusos han logrado de manera satisfactoria tener acceso a un sistema con privilegios de administrador, ellos tratan de cubrir sus huellas para prevenir que su presencia sea detectada en el sistema. El hacker trata de borrar evidencia de su identidad y acciones realizadas en el sistema para así no ser identificado o localizado por las autoridades, los hackers usualmente borran cualquier mensaje de error o eventos de seguridad que puede ser almacenado para evitar ser detectado, a continuación se explica cómo se logra borrar los rastros de un hacker. [1] pág.85

2.15.1 Deshabilitando la auditoría

Una vez que un intruso logra ganar privilegios de administrador su último paso es deshabilitar la auditoria. La auditoria de Windows guarda ciertos eventos en un archivo log el cual es almacenado en el visualizador de eventos de Windows y el mismo incluye inicios de sesión en el sistema, una aplicación o un evento. Un administrador puede elegir el nivel de registro de eventos implementado en el sistema.

2.15.2 Borrando el registro de eventos

Los intrusos pueden fácilmente borrar los registros de seguridad en el visualizador de eventos de Windows. Si un registro de eventos que contiene uno o más eventos sospechosos es porque eventualmente indica que otros eventos han sido borrados, esto quiere decir que es estrictamente necesario borrar el registro de eventos después de deshabilitar las auditorias ya que el mismo hecho de deshabilitar la auditoria crea una entrada en el log. Para lograr esto existe una gran gama de herramientas como AuditPol. [1] pág.86

Troyanos, puertas traseras, virus y gusanos

Una puerta trasera es un programa o un conjunto de programas que un hacker instala en el sistema objetivo para permitir acceso al sistema posteriormente, el objetivo de una puerta trasera es remover la evidencia de una entrada inicial al sistema de los archivos del registro del sistema, pero también pueden ser usados para mantener acceso a la maquina que se ha ganado acceso incluso si la intrusión ya fue detectada y remediada por el administrador de sistemas.

Agregando un nuevo servicio es la técnica más común de disfrazar puertas traseras en un sistema operativo Windows, antes de la instalación el hacker investiga el sistema para encontrar servicios que se encuentran corriendo y así tomar la decisión de si agregar un nuevo servicio dándole un nombre no sospechoso o mejor aun emplear un servicio que nunca es utilizado.

También existen los troyanos de administración remota los cuales son una clase de puerta trasera usada para habilitar administración remota a una maquina comprometida.

2.16 Que es un *troyano*

Un troyano es un programa malicioso que aparenta ser benigno, son descargados generalmente con algún programa o paquete de software. Una vez instalado en el sistema este puede causar robo o perdida de información y bajas de desempeño, puede ser usado como punto inicial para otros tipos de ataques como DDoS (*Distributed Denial Of Service* Attack), muchos troyanos son también utilizados para manipular archivos en el computador de la víctima, manejar procesos, correr comandos remotamente, interceptar pulsaciones de teclas, ver fondos de pantalla y reiniciar o apagar las maquinas afectadas. [2] pág.144

2.16.1 *Troyanos* comunes

A continuación se presenta los troyanos más comunes usados por los hackers.

Nombre	Alias del autor	Creación	Comentarios
Back Orifice	Sir Dystic	1998	Troyano de puerta trasera
Back Orifice 2000	Dildog	1999	Sucesor de Back Orifice
Bifrose	KSV	2004	Destructivo troyano TCP
NetBus	Carl-Fredrik Neikter	1997	Troyano TCP
Subseven	MobMan	1999	Troyano TCP
RemoteHak	Hakka	***	Troyano TCP
Abacab	***	***	Abware.F
Downloader-EV	***	2006	***
Pest Trap	***	2005	***
Poison Ivy	***	2007	***

Tabla 2: Tabla de troyanos más comunes

Fuente: http://es.wikipedia.org/wiki/Troyano_%28inform%C3%A1tica%29

2.16.2 Qué se entiende por canal abierto y canal cubierto

Un canal abierto es el normal y legitimo camino mediante el cual programas se comunican entre computadoras o redes, por ejemplo un canal http por puerto 80 en el cual efectivamente viaja dicho protocolo, mientras que un canal cubierto usa programas o comunicaciones por los canales para los cuales no están permitidos, en una situación real se podría tener habilitado un puerto HTTP 80 y a través de ese canal se envía un protocolo diferente como SMTP.

Una demostración de esto es que algunos troyanos usan canales cubiertos para comunicarse y mandar así instrucciones al componente servidor en el sistema comprometido, haciendo creer que están utilizando un protocolo permitido en la red. [1] pág.94

2.16.3 *Tipos de troyanos*

- **Troyanos de acceso remoto (RAT: Remote Access Trojan):** empleados para ganar acceso remoto al sistema

- **Troyanos de envío de datos:** empleados para encontrar información en un sistema y entregarlo al hacker

- **Troyanos destructivos:** empleados para borrar o corromper archivos en un sistema

- **Troyanos de denegación de servicio:** empleados para lanzar ataques de denegación de servicio.

- **Troyanos proxy:** empleados para encaminar tráfico o lanzar ataques a través de otro sistema.

- **Troyanos FTP:** empleados para crear un servidor FTP para copiar archivos en un sistema

- **Troyanos deshabilitadores de software de seguridad:** empleados para desactivar el software antivirus. [1] pág.94

2.16.4 Cómo trabajan los *troyanos* de conexión inversa

Los troyanos de conexión inversa permiten a un atacante acceder a una máquina en la red interna desde afuera, el hacker instala un troyano simple en un sistema de un red interna en el cual el servidor interno trata de tener acceso al sistema maestro externo para recibir comandos. Es peligroso porque son difíciles de detectar ya que por lo general usan canales cubiertos para sus

comunicaciones, dicho en otras palabras, una computadora infectada por un troyano de conexión inversa se conectara a la computadora del hacker para esperar instrucciones del mismo[1] pág.94

2.16.5 Contramedidas para prevenir *troyanos*

La mayoría de programas antivirus comerciales tienen capacidades de detección de troyanos así como de software espía y la capacidad de poder removerlos del sistema.

Otro punto a tomar en cuenta es tratar de utilizar aplicaciones comerciales, ya que existen herramientas gratuitas para remover software espía que terminan siendo a su vez software espía, así como también es adecuado el uso de herramientas de monitoreo de puertos que puedan identificar puertos que han sido abiertos o archivos que hayan cambiado y así como educar a los usuarios a no instalar aplicaciones descargadas de internet o de archivos adjuntos de partes desconocidas por lo cual una solución podría ser sencillamente restringir la permisología de esa cuenta de manera de que no se pueda instalar programas en el sistema, hay que tomar en cuenta que las medidas de seguridad adoptadas dependerán del tipo de activo que se quiera proteger. [1] pág.98

2.17 Virus y *gusanos*

Los virus y los gusanos son usados para infectar un sistema y modificar el mismo para permitir a un hacker tener acceso. Muchos virus y gusanos llevan troyanos o puertas traseras.

Un virus y un gusano son similares ya que ambos son formas de software malicioso (malware). Un virus infecta otros ejecutables y los usa para esparcirse el mismo, el código del virus es inyectado antes del inicio del programa benigno y se extiende cuando el programa corre.

Un gusano es un tipo de virus que se replica a sí mismo, un gusano se extiende de un sistema a otro sistema automáticamente, pero un virus necesita otro programa para extenderse. Los virus y los gusanos ambos se ejecutan sin el conocimiento del usuario o sin el deseo del usuario final. [1] pág.99

2.17.1 Comprendiendo los tipos de virus

Los virus son clasificados de acuerdo a dos factores, que va a infectar y como lo va a infectar. Un virus puede infectar los siguientes componentes de un sistema:

- Clúster de discos
- Archivos
- Macros
- Clústeres del disco
- Archivos BAT [1] pág.100

2.17.2 Cómo un virus se extiende e infecta un sistema

Los virus son categorizados de acuerdo a sus técnicas de infección de la siguiente manera:

- **Virus polimórfico:** Estos tipo de virus encriptan el código de una manera diferente para cada infección y puede cambiar a diferentes formas para tratar de evadir su detección, son los más difíciles de detectar.

- **Virus sigiloso:** Estos virus oculta las características normales del virus, como por ejemplo modificando el tiempo original y día de creación para no prevenir al sistema de que hay un nuevo archivo.

- **Rápidos y lentos causantes de infección:** Estos pueden evadir detección infectando rápidamente o muy lentamente.

- **Virus blindados:** Estos se encuentran encriptados para evitar su detección y usan técnicas que dificultan su desensamblamiento.

- **Virus multipartita:** Estos avanzados virus crean múltiples infecciones que pueden afectar tanto al sistema de arranque como a archivos.

- **Virus de cavidad:** Estos virus se adjuntan a áreas vacías de archivos.

- **Virus de canal cubierto:** Estos son enviados a través de un protocolo diferente o con encriptación para prevenir su detección e incluso permitir pasar a través de un *firewall*.

- **Virus camuflajeado:** Estos virus aparentan ser otro programa.

- **Virus NTFS y directorio activo:** Estos específicamente atacan el sistema de archivos NT o el directorio activo en sistemas Windows. [1] pág.101

2.18 *Sniffers*

Los software *sniffer*s capturan paquetes no destinados para la dirección MAC (Media Access Control) o la tarjeta de red a la que va destinada, esto es

conocido como modo promiscuo normalmente el sistema en la red lee y responde el tráfico enviado directamente a la tarjeta de red en cambio en modo promiscuo el sistema lee todo el tráfico que se envía a través de la red y es procesado por el *sniffer*. El modo promiscuo se habilita en las tarjetas de red mediante la instalación de un driver especial.

Cualquier protocolo no encriptado será susceptible a ser "sniffeado", los protocolos como http, POP3 (Post Office Protocol), SNMP (Simple Network Management Protocol) y FTP son los más comúnmente capturados a través del "sniffeo" y utilizado por los hackers para obtener cuentas de usuarios y contraseñas. [3] pág.157

2.18.1 Métodos de detección de *Sniffers* en la red

El test DNS

En este método, la herramienta de detección en sí misma está en modo promiscuo. Creamos numerosas conexiones TCP falsas en nuestro segmento de red, esperando que un *sniffer* pobremente escrito procese dichas conexiones y resuelva las direcciones IP inexistentes. [3] pág.164

El test del *ping*

En este método construimos una petición tipo "ICMP echo" con la dirección IP de la máquina sospechosa de hospedar un *sniffer*, pero con una dirección MAC deliberadamente errónea.

La mayoría de los sistemas desatenderán este paquete, ya que su dirección MAC es incorrecta. Pero en algunos sistemas Linux, NetBSD y NT, puesto que el NIC (*network interface card*) está en modo promiscuo, el *sniffer* aceptará este paquete de la red como paquete legítimo y responderá por consiguiente. Si el blanco en cuestión responde a nuestra petición, se sabrá que se encuentra en modo promiscuo.[3] pág.165

2.19 Comprendiendo como trabajan los *BOT/BOTNETS*

Un Bot es un robot programado de manera automatizada que tiene un comportamiento inteligente, los spammers utilizan los BOTs para postear automáticamente mensajes spam en nuevos grupos y enviarlos por emails. Los BOTs solo pueden ser utilizados como herramienta para ataques remotos, más frecuentemente como agentes de software web con los cuales obtienen información de diversas paginas.

Los BOTs más peligrosos son aquellos que se instalan de forma automática en las computadoras de los usuarios para propósitos maliciosos, algunos BOTs son capaces de comunicarse con otros usuarios a través de servicios de mensajería instantánea como el IRC (Internet Relay Chat) o algún otro tipo de interfaz web, estos BOTs permiten a los hackers realizarles preguntas en lenguaje común y ellos dar una respuesta.

Un BOTNET es un grupo de sistemas BOTs, estos sirven para varios propósitos incluyendo ataques del tipo DDoS, creación o mal uso de protocolos como SMTP para enviar correos spam, fraude de mercadeo de internet, robo de seriales de aplicaciones, logins e información financiera tales como tarjetas de crédito. Generalmente un BOTNET se refiere a un grupo de sistemas BOT corriendo de forma simultánea, los cuales atacan de manera coordinada generando así un ataque DDoS. [1] pág.123

2.19.1 Contra medidas de ataques *DoS/DDoS*

Existen varias formas de detectar, detener o prevenir ataques DoS/DDoS, tomando en cuenta las siguientes medidas:

- **Filtro de ingreso a la red:** Todas los accesos a la red provienen de la implementación de un filtro de ingreso a la red para detener cualquier tipo de paquete que provengan de inyecciones de paquetes falsas o suplantación de direcciones IP dentro de internet.

- **Controlando la velocidad de ingreso del tráfico:** El número de *router*s que se encuentran disponibles actualmente generan un límite dependiendo del ancho de banda y algunos de ellos dependiendo del tráfico que consumen, esto algunas veces esta referido a la parte del compartimiento del tráfico.

- **Sistemas de detección de intrusión:** Mejor conocido por sus siglas en ingles IDS, se usa comúnmente para detectar a atacantes que se comunican con maquinas que son esclavas, maestra u agentes. Esto permite conocer la existencia de alguna maquina en la red que este siendo utilizada para realizar ataques conocidos pero probablemente no son detectadas variaciones en estos ataques como herramientas implementadas en ellas.

- **Herramientas de auditoría de computadora:** Herramientas de escaneo de archivos disponibles para detectar la existencia de ataques conocidos de DDoS para herramientas clientes y servidores en un sistema.

- **Herramientas de auditoría de la red:** es una herramienta de escaneo de la red disponible para detectar la presencia de agentes de DDoS corriendo en algún computador de la red.

- **Herramientas de rastreo de red automatizada:** Rastreo de paquetes con direcciones suplantadas dentro de la red tanto en consumo de tiempo como en la cantidad de cooperación de todas las redes llevando el tráfico y así completándolo mientras el ataque esta en progreso. [1] pág.124

2.20 Sesión *Hijacking*

Sesión Hijacking ocurre cuando un hacker toma control de alguna sesión de usuario después de que dicho usuario se ha autenticado con el servidor. [1] pág.125

2.20.1 Comparando *Spoofing vs Hijacking*

Los ataques de suplantación se diferencian en que el ataque de suplantación el hacker realiza un “sniffeo” y escucha el tráfico que pasa a lo largo de la red que es enviado y recibido, posteriormente, el hacker utiliza la información para suplantar o utilizar una dirección legitima dentro del sistema, por el contrario, Hijacking involucra activamente la comunicación de algún otro usuario

desconectado para realizar el ataque. El atacante depende del usuario legítimo para realizar la conexión y la autenticación, posterior a eso, el atacante toma posesión de la sesión y la sesión de usuario valida es desconectada. [1] pág.125

2.20.2 Pasos para desarrollar un ataque *Hijacking*

- **Rastreo de la sesión:** El hacker identifica una sesión abierta y predice la secuencia de números del próximo paquete.

- **Desincronización de la conexión:** En la cual el hacker envía al usuario valido del sistema un RST TCP o un paquete con la bandera FIN encendida que causa el cierre de la sesión.

- **Inyección de paquetes por parte del atacante:** El hacker envía al servidor un paquete TCP con la secuencia de números predicha y el servidor las acepta como un próximo paquete valido. [1] pág.125

2.20.3 Comprendiendo la predicción de secuencia

TCP es un protocolo orientado a conexión, responsable de reensamblar cadenas de paquetes en el orden original, allí, cada paquete debe tener un único número de secuencia conocido por sus siglas en ingles como SN (Sequence Number). A cada paquete se le debe asignar un único SN que estará disponible para que al ser recibido por la maquina pueda reensamblar la cadena de paquetes en el orden correspondiente, esto ocurre ya que los paquetes pueden llegar de forma desordenada lo cual ocurre regularmente dentro de internet.

Existen herramientas utilizadas para desarrollar este tipo de ataques de predicción de número de secuencias TCP, el hacker debe “sniffear” el tráfico entre los dos sistemas y luego, el hacker con sus herramientas debe obtener exitosamente el número de secuencia o localizar algún número de secuencia inicial para calcular el próximo número de secuencia. La mayoría de las

herramientas de sesiones Hijacking incluyen características para permitir el "sniffeo" del paquete para determinar la secuencia de números. [1] pág.126-127

Hackeando servidores web, vulnerabilidades de aplicaciones web y técnicas de crackeo de contraseñas basadas en web

Los servidores y aplicaciones web son áreas altamente potenciales para comprometer la seguridad, la principal razón de esto es que sus sistemas corren software de aplicación web publico disponible en internet. Cuando un servidor web ha sido comprometido el sistema puede proveer a los hackers otra puerta de entrada a la red, no únicamente mediante el software de servidor, pero si mediante la aplicación de ejecución de servicios web que son abiertos para el público y que pueden ser explotados, durante su funcionamiento, el servidor web es más accesible que otros sistemas menos protegidos, por eso son más sencillos de explotar. [1] pág.138

2.21 *Hackeando* servidores web

Es importante tener conocimientos acerca de las vulnerabilidades existentes, así como comprender los tipos de ataques que los hackers pueden utilizar, adicionalmente debe ser conocido algún tipo de métodos que fortalezcan la seguridad del servidor. [1] pág.139

2.21.1 Lista de vulnerabilidades en los diferentes tipos de servidores web

Servidores web así como otro tipo de sistemas parecidos, pueden ser comprometidos por los hackers incurriendo en las vulnerabilidades más comúnmente explotadas en servidores web tales como:

- Mala configuración del software del servidor web.

- Sistemas operativos o aplicaciones que tienen fallas o debilidades en la programación de su código.

- Instalación por defecto del sistema operativo y software del servidor web y/o carencia de un conjunto de parches y/o actualizaciones del sistema operativo o software del servidor web.

- Carencia o inexistencia de procedimientos y políticas de seguridad.

Los hackers explotan estas vulnerabilidades para lograr el acceso al servidor web. Debido a que los servidores se encuentran en zonas desmilitarizadas (DMZ). [1] pág.139-140

2.21.2 Comprendiendo los tipos de ataques en contra de servidores web

El tipo de ataque más visible contra servidores web es la desfiguración, los hackers desfiguran un sitio web o un portal web por diversión y como una oportunidad para aumentar su reputación. La desfiguración de un servidor web se basa en que el hacker explote la vulnerabilidad del sistema operativo o software del servidor web y luego altere los archivos de la página web para mostrar que ha sido hackeada colocando comúnmente su nombre en la página inicial.

Ataques comunes que permiten a un hacker desfigurar un sitio web son:

- Capturar las credenciales de administrador a través de un ataque de "hombre en el medio".

- Revelando la contraseña del administrador por ataque de fuerza bruta.

- Usando ataques DNS para re direccionar a los usuarios a un servidor web diferente.

- Comprometiendo mediante FTP o servidor de correo.

- Explotando fallas en la aplicación web que resulte en ser vulnerable.

- Mala configuración de elementos compartidos web.

- Tomando ventaja de permisos débiles.

- Reenrutando a un cliente después de ataque a un *firewall* o a un *router*.

- Usando ataques de inyección SQL.

- Usando intrusión Telnet o Shecure Shell (SSH).

- Envenenando la dirección URL (*Uniform Resource Locator*) para enviar a los usuarios a una página diferente.

- Usando extensión del servidor web o intrusión por servicio remoto.

- A través de la intercepción de cookies de seguridad habilitada entre el servidor y el cliente la cual puede ser modificada para hacer creer al servidor que el usuario tiene mayores privilegios. [1] pág.140

2.21.3 Métodos de fortalecimiento de un servidor web

El administrador del servidor web puede utilizar varias formas para fortalecer el servidor web para incrementar su seguridad mediante las siguientes acciones:

- Renombrar la cuenta de administrador con una contraseña fuerte.

- Deshabilitar por defecto sitios FTP y páginas web.

- Remover aplicaciones no usadas por el servidor, como por ejemplo WebDAV (Web-based Distributed Authoring and Versioning).

- Deshabilitar el directorio de búsqueda en las opciones de configuración del servidor web.

- Agregar un aviso legal el cual diga las implicaciones que puede llevar hackear el sitio web.

- Aplicar los parches y “paños calientes” más actualizados además de las actualizaciones del sistema operativo y software del servidor web.

- Realizar chequeos límites sobre la inserción en formularios web y cadenas de consulta que prevengan desbordamiento de buffer o ataques de inserciones maliciosas.

- Deshabilitar la administración remota.

- Habilitar auditoria y registros.

- Usar un *firewall* entre el servidor web e internet y permitir solo los puertos 80 y 443 a través del mismo.

- Reemplazar el método GET por el método POST cuando se envíe data al servidor web. [1] pág.141

2.22 Comprendiendo cómo trabajan las aplicaciones web

Las aplicaciones web son programas que residen en un servidor web dándole funcionalidad tales como una página web, consultas de bases de datos, mensajería de correos y grupos de discusión son algunos ejemplos de estas aplicaciones. Dichas aplicaciones utilizan arquitecturas cliente – servidor, con un navegador web como cliente y actuando como servidor web la aplicación del servidor. [3] pág.127

2.22.1 Objetivos de hackear una aplicación web

Su principal propósito es obtener información confidencial, las aplicaciones web son críticas en cuanto a la seguridad del sistema porque usualmente están conectadas a la base de datos que contiene información tales como identidades, número de tarjetas de crédito y contraseñas. Las vulnerabilidades de una aplicación web incrementan las amenazas de que los hackers puedan explotar el sistema operativo, el servidor web o el software de aplicación web. Las aplicaciones web son esencialmente otra puerta dentro del sistema y pueden explotar comprometiendo el mismo.[3] pág.128

2.22.2 Anatomía de un ataque

Hackear una aplicación web es similar a hackear algún otro sistema, los hackers siguen un proceso de cinco (5) pasos que incluyen:

- Escanear la red.

- Obtener la información.

- Probar diferentes escenarios de ataques.

- Planificar el ataque.

- Lanzar el ataque. [1] pág.142

2.22.3 Amenazas de aplicaciones web

Muchas amenazas a aplicaciones web existen en un servidor web, las siguientes son las amenazas más comunes:

- **Cross-site scripting:** Un parámetro ingresado en un formulario web que se procesa por la aplicación, la combinación correcta de variables puede resultar en la ejecución arbitraria de algún comando.

- **Inyección SQL:** Inserción de comandos SQL dentro de un URL desde la base de datos del servidor hacia un vertedero, alterando, borrando o creando información dentro de la base de datos.

- **Inyección de comandos:** El hacker introduce comandos de programación dentro del formulario web.
- **Envenenamiento de cookies y fisgoneo:** El hacker corrompe o roba las cookies.

- **Desbordamiento de buffer:** Gran cantidad de datos enviados a la aplicación web mediante el formulario web para ejecutar comandos.

- **Autenticación Hijacking:** El hacker roba la sesión de un usuario que se ha autenticado.

- **Directorio transversal** / **Unicode:** El hacker navega entre los archivos de un sistema vía un navegador web o explorador de Windows. [3] pág.143-147

2.23 Técnicas de *crackeo* de contraseñas basadas en web

Es importante estar familiarizado con las técnicas utilizadas por los hackers para romper contraseñas basadas en web considerando los diferentes tipos de autenticaciones conocidas e identificando las clasificaciones de las diferentes técnicas de crackeo de contraseñas. [1] pág.144

2.23.1 Qué es un *crackeador* de contraseñas

Un *crackeador* de contraseñas es un programa diseñado para desencriptar contraseñas o deshabilitar protección de contraseñas. Estos cuentan con diccionarios de búsqueda o métodos de fuerza bruta para "crackearlas". [1] pág.144

2.23.2 Cómo trabaja un *crackeador* de contraseñas

El primer paso un ataque de diccionario es por lo general una lista de las potenciales contraseñas que pueden ser encontradas en los diccionarios. El hacker, usualmente crea esta lista con un programa generador de diccionarios o diccionarios que pueden ser descargados desde el internet y la lista es comparada contra la contraseña que el hacker quiere crackear. [1] pág.145

2.23.3 Comprendiendo clasificación de ataques a contraseñas

Existen tres (3) tipos de ataques de contraseñas los cuales son:

- **Diccionario:** Usa contraseñas que pueden ser encontrados en un diccionario.

- **Fuerza bruta:** Supone contraseñas complejas que use letras, números y caracteres especiales.

- **Híbridos:** Usa palabras del diccionario con números o caracteres especiales como sustitutos de las letras. [1] pág.145

2.24 Inyección SQL

Inyección SQL es una vulnerabilidad informática en el nivel de la validación de las entradas a la base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o de script que esté incrustado dentro de otro.

Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal, y hacer que se ejecute maliciosamente el código "invasor" en la base de datos.

La inyección SQL es un problema de seguridad informática que debe ser tomado en cuenta por el programador para prevenirlo. Un programa hecho con descuido o por ignorancia sobre el problema, podrá ser vulnerable y la seguridad del sistema puede quedar ciertamente comprometida. Esto puede suceder tanto en programas ejecutándose en computadores de escritorio, como en páginas Web, ya que éstas pueden funcionar mediante programas ejecutándose en el servidor que las aloja.

Al ejecutarse una consulta en la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar código malicioso en el computador. [1] pág.152-153

2.25 Desbordamiento de *buffer*

En seguridad informática y programación, un desbordamiento de buffer (del inglés *buffer overflow* o *buffer overrun*) es un error de software que se produce cuando se copia una cantidad de datos sobre un área que no es lo

suficientemente grande para contenerlos, sobrescribiendo de esta manera otras zonas de memoria. Esto se debe en general a un fallo de programación. La consecuencia de escribir en una zona de memoria imprevista puede resultar impredecible. Existen zonas de memoria protegidas por el sistema operativo, si se produce la escritura fuera de una zona de memoria protegida se producirá una excepción del sistema de acceso a memoria seguido de la terminación del programa. Bajo ciertas condiciones, un usuario obrando con malas intenciones puede aprovecharse de este mal funcionamiento o una vulnerabilidad para tener control sobre el sistema.

En algunas ocasiones eso puede suponer la posibilidad de alterar el flujo del programa pudiendo hacer que éste realice operaciones no previstas. Esto es posible dado que en las arquitecturas comunes de computadoras, la memoria no tiene separación entre la dedicada a datos y a programa.

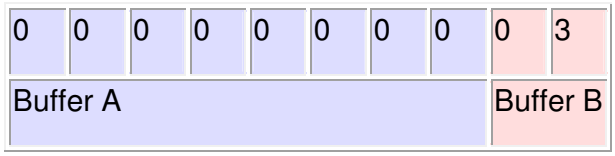
Si el programa que tiene el error en cuestión tiene privilegios especiales se convierte además en un fallo de seguridad. El código copiado especialmente preparado para obtener los privilegios del programa atacado se llama “shellcode”.

2.25.1 Descripción técnica

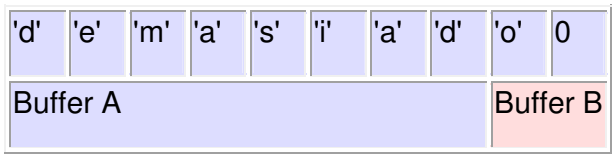
Un desbordamiento de búfer ocurre cuando los datos que se escriben en un búfer corrompen aquellos datos en direcciones de memoria adyacentes a los destinados para el búfer, debido a una falta de validación de los datos de entrada. Esto se da comúnmente al copiar cadenas de caracteres de un búfer a otro.

2.25.2 Ejemplo básico

En este ejemplo, un programa tiene definidos dos elementos de datos continuos en memoria: un buffer de 8 bytes tipo string, A, y otro de dos bytes tipo entero, B. Al comienzo, A contiene bytes nulos y B contiene el número 3 (cada carácter se representa mediante un byte).



A continuación, el programa intenta almacenar la cadena de caracteres "demasiado" en el buffer A, seguido de bytes nulos para marcar el fin de string. Al no validarse la longitud de la cadena, se sobrescribe el valor de B:



A pesar de que el programador no quería cambiar el contenido del búfer B, el valor de éste ha sido reemplazado por un número equivalente a parte de la cadena de caracteres. Para este ejemplo, en un sistema “big-endian” que use ASCII (*American Standard Code for Information Interchange)*, el carácter 'o' seguido del byte nulo equivale al número 28416.

Si B fuese la única variable aparte de A definida en el programa, la escritura de datos que sobrepasen los límites de B generarían un error como “segmentation fault”, concluyendo así el programa. [3] 167-174

2.26 *Hackeando* las conexiones inalámbricas

Las redes inalámbricas agregan otro punto de entradas a los hackers. Mucho se ha escrito sobre la seguridad inalámbrica y su hackeo ya que esta es una tecnología relativamente nueva y contiene muchos hoyos de seguridad, debido a su naturaleza de emisión a través de la radio frecuencia las redes inalámbricas obtuvieron una rápida adopción en cuanto a tecnologías tanto para redes caseras como de oficinas en las cuales existen muchas vulnerabilidades que pueden ser explotadas.

Dos métodos que existen para la autenticación de clientes en redes inalámbricas de área local en un punto de acceso: que son sistema abierto o autenticación de llave compartida. Los sistemas abiertos no proveen ningún mecanismo de seguridad pero es simple, una solicitud para realizar una conexión a la red. En la Autenticación de llave compartida el cliente inalámbrico divide una cadena de texto con la llave WEP (Wired Equivalent Privacy) para autenticarse en la red.

El WEP es la primera opción de seguridad para el 802.11 en redes inalámbrica de área local, es utilizado para encriptar la data y opcionalmente para

autenticación de llave compartida vinculada en clientes inalámbricos de área local.

WPA (Wi-Fi Protected Access) sustituye en seguridad a WEP, este utiliza protocolo de integridad para llave temporal (TKIP: Temporal Key Integrity Protocol) que protege la implementación del RC4 (*Rivest Cipher 4*), la encriptación de la data y tanto WPA Personal como WPA Empresarial para autenticación. El WPA Personal utiliza frases de acceso ASCII para su autenticación mientras que WPA Empresarial utiliza servidor RADIUS para autenticación de usuarios, este último es más robusto a nivel de seguridad pero este último depende de la creación e instalaciones más complejas del servidor RADIUS. TKIP rota la clave encriptada para prevenir vulnerabilidades en WEP y por consecuencia ataques de crackeo.

WPA2 es similar al 802.11i y utiliza estándares avanzados de encriptación (AES: *Advanced Encryption Standard*) para proteger las cabeceras encriptandolas. AES es considerado un algoritmo de encriptación incrackeable, WPA2 también permite usar el TKIP durante un periodo de transición llamado modo de seguridad mixto, este periodo de transición significa que tanto TKIP como AES pueden ser usados para encriptar la data. AES requiere de un procesador rápido, esto implica que dispositivos tales como los PDA solo pueden soportar TKIP. El WPA Personal y WPA2 Personal utilizan contraseña de autenticación para clientes inalámbricos de área local. El WPA Empresarial y WPA2 Empresarial autentican las redes inalámbricas de área local vía el servidor RADIUS usando el protocolo de autenticación extensible 802.1X (EAP: Extensible Authentication Protocol).

2.26.1 Comprendiendo las técnicas para el *hackeo* de redes inalámbricas

La mayoría de los ataques inalámbricos pueden ser categorizados de la siguiente forma:

- ***"Crackeando"* encriptación y mecanismos de autenticación:** Estos mecanismos incluyen crackear WEP, WPA llave de autenticación de contraseña pre compartida. De esta forma los hackers logran conectarse a las redes inalámbricas de área local usando credenciales robadas o pueden capturar data de otros usuarios y desencriptar/encriptar la misma.

- ***"Sniffeando"*:** Esto involucra capturar contraseñas u otra información confidencial de una red inalámbrica de área local desencriptada.

- **Denegación de servicio:** DoS puede ser llevado a cabo a nivel de la capa física. [4] pág.189-197

2.27 Seguridad Física

La seguridad física es un punto crítico que se presenta en la mayoría de las organizaciones y en muchas ocasiones se pasan por alto. Bajo el concepto de seguridad física nos referimos a las medidas preventivas que evitan la pérdida parcial o total de los recursos informáticos. [1] pág. 170

2.27.1 Comprendiendo la seguridad física

Generalmente las medidas de seguridad pueden ser categorizadas de las siguientes tres (3) maneras:

- **Física:** Medidas físicas para prevenir el acceso a los sistemas incluyendo guardias de seguridad, alumbrado, cercas, cerraduras y alarmas. Los puntos de acceso a las instalaciones deben ser limitadas y a su vez deben ser monitoreadas y protegidas por circuito cerrado de televisión y alarmas, la entrada a las instalaciones debe estar restringida solo a personal autorizado debidamente identificado y computadoras con información sensible deben estar protegidas bajo llave en una habitación con acceso a través de credenciales.

- **Técnico:** Medidas de seguridad técnica como por ejemplo *firewall*s, IDS, Filtro de contenido Spyware y escaneo contra virus y troyanos el cual debe ser implementado en todos los clientes remotos, redes y servidores.

- **Operacional:** Medidas de seguridad operacional para analizar amenazas y realizar evaluaciones de riesgo el cual debe ser un proceso documentado en las políticas de seguridad de la organización. [1] pág.171

2.27.2 Por qué es necesaria la seguridad física

Las necesidades de la seguridad física por la misma razón que se necesitan otros tipos de seguridad como la técnica o la operacional son para prevenir que usuarios no deseados logren ganar acceso a la red y a la información que en ella se encuentra. Los hackers pueden ganar acceso fácil consecuencia de una seguridad física débil, adicionalmente información puede ser pérdida o dañada por causas naturales, la necesidad de la implementación de la seguridad física viene dada por las siguientes razones:

- Acceso no autorizado a las computadoras

- Robo de información desde los sistemas

- Manipulación de la data almacenada en un sistema

- Perdida de información o daño causado a sistemas por causas naturales como terremotos, incendios, inundaciones, etc. [1] pág.172

2.28 Metodología LPT (*Licensed Penetration Tester*) para pruebas de intrusión

La metodología para pruebas de intrusión LPT es de la casa EC Council, la cual define una serie de pasos para probar la seguridad de diferentes equipos, aplicaciones y entornos de trabajo.

3. Marco Metodológico

Para el logro exitoso de los objetivos planteados en el capítulo 1, es necesario definir un esquema o metodología de trabajo que permita evaluar el nivel de seguridad de diferentes dispositivos o servicios de seguridad, así como el procedimiento de instalación de un dispositivo UTM *Watchguard*. A continuación, se presenta la especificación de las metodologías utilizadas.

3.1 Procedimientos para lograr objetivo del T.E.G.

3.1.1 Vulnerabilidad de la red

Para evaluar la vulnerabilidad de la red se debe emplear una herramienta que permite la identificación de las debilidades de una red. En nuestro caso se emplea la herramienta Nessus V4.0.1 la cual toma como parámetro de entrada la dirección IP de un servidor o computador de la red y da como resultado un informe ejecutivo que muestra la severidad del impacto de las vulnerabilidades en la red de la institución.

Cabe destacar que esta herramienta está basada en estándares abiertos de software libre para su uso no comercial.

3.1.2 Esquema de red

El esquema de red a utilizar consiste en la creación de un segmento de red local e internet con zona DMZ (*DeMilitarized Zone*) para servidores expuestos. Esto se logra con el dispositivo UTM, definiendo en una interfaz la zona DMZ y en otra interfaz del dispositivo la LAN (*Local Area Network*).

3.1.3Selección del UTM

Para seleccionar el UTM se debe consultar estudios realizados por organizaciones independientes reconocidas a nivel internacional. En nuestro

caso de estudio se consulta la información de estudios realizados por MIERCOM [11] (compañía independiente encargada de probar diferentes dispositivos de red) basados en los diferentes UTM existentes en el mercado[12], la cual muestra a *Watchguard* [13] como la solución más eficiente dentro de los UTM para las soluciones de seguridad informática.

3.1.4 Configuración del UTM

Para configurar el UTM de manera adecuada se debe realizar un curso de capacitación que dicta la casa fabricante del producto. Adicionalmente, se toma en consideración las políticas de uso de internet definidas por la institución [Anexo A].

3.1.5 Pruebas de intrusión LPT

Se realizan pruebas de intrusión a redes inalámbricas, dispositivos IDS y *firewall* empleando la metodología LPT.

3.2 Procedimiento de instalación *Watchguard* sobre Windows

1. Se instala el programa base "*Watchguard* System Manager".

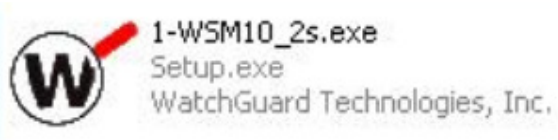


Figura 8. Icono de programa base de WSM

2. Se aplica la actualización correspondiente al programa base.

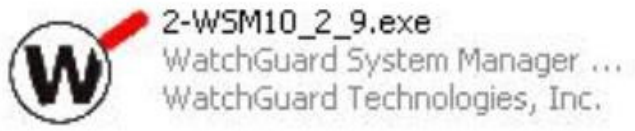


Figura 9. Icono de actualización del WSM

3. Se instala el firmware de la versión actualizada sincronizándola con el dispositivo para su correcto funcionamiento.

Figura 10. Icono de instalación del fireware WSM

3.3 Metodología LPT

Para la metodología aplicada, en cada uno de los pasos de cada método se espera un resultado.

3.3.1 Método para *firewall*

1. Localizar el *firewall*. Se logra enviando un paquete SYN empleando la herramienta "HPing2" al *firewall*, si se obtiene un ICMP tipo 13 con la dirección fuente del dispositivo, entonces se trata de un *firewall*. Un ejemplo del comando a aplicar es **hping2 www.xsecurity.com –c2 –S –p23 –n** y la respuesta deseada es **ICMP Unreachable type 13 from 10 10 2 3.**

2. Se aplica el comando "*traceroute*" o "*tracert*" para identificar el rango de la red. Esto permite identificar el camino a la red, *routers* o dispositivos intermediarios e Información sobre los dispositivos de filtrado y protocolos permitidos o denegados. Se ejecuta el comando de la siguiente manera: **tracert www.xsecurity.com.**

3. Se realiza un escaneo de puertos del *router*. La mayoría de los *firewall* poseen por defecto puertos abiertos con el propósito de hacer administración remota, por ejemplo: VPN, administración, autenticación de usuarios, entre otros. Para lograr esto se usa la herramienta "NMAP". Se logra ejecutando el siguiente comando:

   nmap –n –vv –P0 –p256, 1080 <www.xsecurity.com>.

4. Se Identifican los servicios. Se realiza un "grab the banner". Esto se logra empleando la herramienta "Netcat". Se logra ejecutando el siguiente comando:

   C:\>nc -nvv 10.0.0.1 80

   HEAD / HTTP/1.0
   HTTP/1.1 503 Service Unavailable
   MIME-Version: 1.0
   Server: Simple, Secure Web Server 1.1
   Date: Tue, 12 Dec 2008 19:08:35 GMT
   Connection: close
   Content-Type: text/html
   <HTML>
   <HEAD><TITLE>*Firewall* Error: Service Unavailable</TITLE></HEAD>.

5. Se crean paquetes personalizados. Se envían paquetes al *firewall* y se puede obtener un único tipo de respuesta que permite determinar su tipo. Se logra ejecutando el siguiente comando: **hping 10.0.0.5 –c 2 –S –p 23 –n.**

6. Se prueba la enumeración del control de acceso. Para ello se emplea la herramienta "NMAP" para enumerar la lista de control del acceso del *firewall*. A continuación un ejemplo de cómo ejecutar la herramienta "NMAP" para probar la enumeración del control de acceso y su resultado:

   #nmap –sA 192.168.0.1
   Interesting ports on 192.168.0.1:
   (The 65530 ports scanned but not shown below are in state: filtered)
   PORT STATE SERVICE

   110/tcp UNfiltered pop-3
   13701/tcp UNfiltered VeritasNetbackup
   13711/tcp UNfiltered VeritasNetbackup
   13721/tcp UNfiltered VeritasNetbackup

13782/tcp UNfiltered VeritasNetbackup

Nmap run completed -- 1 IP address (1 host up) scanned in 12205.371 seconds.

7. Se prueban las políticas del *firewall* Existen dos métodos de verificación de las políticas de un *firewall*:

    i) Se obtienen las copias impresas de la configuración del *firewall* y se contrasta con la configuración deseada.

    ii) Se realizan pruebas en el sitio, las cuales se desarrollan probando la configuración del *firewall*, con la ejecución de operaciones que deben estar prohibidas.

8. Se prueba el *firewall* con una herramienta que permita descubrir aquellos puertos abiertos, así como la lista de control de acceso. Para nuestro caso se emplea la herramienta "Firewalk". Si un mensaje "error TTL excedido" se obtiene de vuelta significa que el puerto en el *firewall* se encuentra abierto.

9. Se prueba la redirección de puertos. En caso de obtenerse acceso directo al mismo entonces se prueba su redirección. Este tipo de redireccionamiento es usualmente empleado para "evadir" los *firewall* de tipo *filtro de puertos*. El método consiste en especificar al redireccionador de puertos que "escuche" en un puerto seleccionado, permitiendo que los paquetes recibidos en el puerto abierto sean redireccionados o enviados al puerto deseado en la computadora remota. Se logra empleando herramientas como "*Fpipe*" o "*Datapipe*". Un ejemplo del uso de estas herramientas es la siguiente:

fpipe –l 80 –r 139 192.168.10.40

datapipe 80 139 192.168.10.40.

10. Se prueban los canales cubiertos. Se instala una "puerta trasera" (*backdoor*) en una máquina victima de la red interna y se intenta una conexión inversa a una máquina ubicada fuera del *firewall*. La herramienta a emplearse es "*WWW Reverse Shell*".

11. Se prueba el túnel HTTP, donde se intenta una conexión a la red interna empleando la técnica de túnel HTTP. Las herramientas a emplearse para lograr esto son: "*HTTPORT*" y "*HTTHOST*".

12. Se prueba el *firewall* contra vulnerabilidades específicas. Usualmente los *firewall* tienen vulnerabilidades conocidas que son de conocimiento general y que se encuentran publicadas. Si el dispositivo no se encuentra actualizado ante esas vulnerabilidades, entonces este se considera susceptible.

3.3.2 Método para los dispositivos IDS/IPS

1. Se prueba el agotamiento de los recursos del dispositivo, inundando con peticiones ARP (*Address Resolution Protocol*). Cualesquiera de los dispositivos son propensos a ataques por agotamiento de sus recursos, provocando una degradación del servicio o falla una vez que sus recursos son consumidos. En este punto se aplica la herramienta "*ARP Request Stress Tool*".

2. Se prueba la detección de MAC e IP "*Spoofing*". Esto se logra mediante la generación de peticiones con una dirección MAC suplantada a una dirección existente de la red interna. Esto provoca en la mayoría de los casos perturbación del tráfico, siempre y cuando existan dos direcciones MAC idénticas. Así mismo, se realiza la suplantación de una dirección IP legítima de la red para inundar con peticiones a los dispositivos. Las herramientas adecuadas para lograr esto son: "*HPing2*" y "*MAC Spoofer*".

3. Se prueba el envío de paquetes a la dirección de *broadcast*. Esto se realiza con la finalidad de causar una amplificación de la inundación de paquetes, tal como se describe en el paso anterior, se logra el objetivo con la herramienta "*HPing2*".
4. Se prueba la respuesta del dispositivo ante fragmentos duplicados. Esperando como respuesta tres posibles resultados. Siendo: salvar el primer fragmento,

salvar el segundo fragmento o descartar ambos fragmentos. Se emplea la herramienta "*HPing2*".

5. Se prueba la resistencia al *ping de la muerte*. Este ataque consiste en la creación de un datagrama IP cuyo tamaño supera el máximo permitido (> 65.536 bytes). Esto se logra ejecutando el comando *Ping* –t (dirección victima) –l 65.596.

6. Se prueba para tamaños de paquetes impares. Es muy sospechoso si un paquete fragmentado tiene un tamaño que no es múltiplo de 8, ya que los paquetes son fragmentados en múltiplos de 8. Se emplea la herramienta "*HPing2*" y "*FragRoute*".

7. Se prueba el envío de paquetes a través del puerto cero (0). Tanto para el protocolo TCP como UDP, el tráfico a través del puerto cero (0) es considerado inusual, ya que es un puerto reservado oficialmente y no debería usarse para comunicaciones de red. Cualquier tráfico que utilice el puerto cero probablemente no sea tráfico legítimo y sus paquetes sean generados de manera sintética (paquetes personalizados). Para la verificación de este paso se utiliza la herramienta "*HPing2*" dirigiendo paquetes al puerto cero (0).

8. Se prueba la retransmisión de paquetes a través del protocolo TCP. El protocolo TCP retransmite paquetes para introducir un nivel de fiabilidad al mecanismo de transporte IP que es poco fiable. Si un IDS/IPS encuentra un paquete retransmitido que tiene diferente contenido al paquete original, el dispositivo puede asumir o bien que es un proceso normal de la implementación de TCP/IP o la existencia de un ataque malicioso. Esto se logra enviando un paquete con la herramienta "*HPing2*" y enviando una retransmisión del mismo paquete con una carga diferente al original.

9. Se manipulan las banderas de la cabecera TCP. Existen varias pilas de TCP, las cuales reaccionan diferente a estas entradas ilegales, en este paso se probará diferentes combinaciones de las banderas TCP utilizando las herramientas "*NMAP*" y "*HPing2*". Se prueban las diferentes manipulaciones de las banderas:

- Se prueba para ninguna bandera

- SYN/FIN

- SYN/RST

- SYN/FIN/ACK

- SYN/RST/ACK

- Todas las banderas

10. Se prueba la inundación de peticiones SYN. Muchas implementaciones TCP son vulnerables a un ataque de agotamiento de recursos conocido como inundación SYN, en el cual se en envía una gran cantidad de peticiones SYN para crear sesiones, causando así el agotamiento de los recursos de memoria. Esto se realiza con la herramienta "*thunderFlood V1.1*".

11. Se prueba la detección o prevención de codificación del URL. El protocolo HTTP específica que caracteres arbitrarios binarios pueden ser pasados en un URL usando la notación %XX, donde "XX" es el valor hexadecimal del carácter. Por ejemplo:

    "cgi-bin" es equivalente a**: "%63%67%69%2d%62%69%6e".**

12. Se prueba la tolerancia al doble slash (//). Se reemplaza cada "/" por "//", por ejemplo:

"**/cgi-bin/some.cgi"** se modifica por **//cgi-bin//some.cgi".**

13. Se prueba para solicitud de recorrido de directorio inverso. Un ejemplo de este tipo de solicitudes es "/cgi-bin/some.cgi" y mediante la solicitud de recorrido del directorio inverso queda una solicitud como la siguiente:

    GET /cgi-bin/blahblah/. ./some.cgi HTTP 1.0 lo cual es equivalente a **"/cgi-bin/some.cgi".** La mayoría de los IDS/IPS detectan este tipo de técnica.

14. Se prueba para culminaciones de peticiones prematuras. Dado que algunos IDS/IPS dejan de buscar código malicioso o firmas malignas conocidas después de "**HTTP/1.0\r\n**". Un ejemplo es:

    /%20HTTP/1.0%0d%0aHeader:%20/../../cgi-bin/some.cgi HTTP/1.0\r\n\r\n

    Puede ser modificado por:

    GET / HTTP/1.0\r\nHeader: /../../cgi-bin/some.cgi HTTP/1.0\r\n\r\n

    Ambos son equivalentes y válidos, un IDS/IPS decodifica el primer código y deja de escanear, consecuencia de un final prematuro en lugar del real.

15. Se prueba para URL largos.

    Algunos IDS/IPS solamente verifican los primeros XX bytes de una petición. Generalmente, esto trabaja bien siempre y cuando la primera línea de la solicitud contenga la dirección. Sin embargo, se puede explotar con una solicitud como la siguiente:

    GET /rfprfp<varios caracteres>rfprfp/../cgibin/some.cgi HTTP/1.0.

16. Se prueba el método de procesamiento nulo.

Muchas bibliotecas de cadena de caracteres del lenguaje C/C++ usan el carácter “NULL” para denotar el fin de una cadena de caracteres, algunas implementaciones de IDS/IPS utilizan estas librerías y los hackers toman ventaja de esto haciendo peticiones como la siguiente:

GET%00 /cgi-bin/some.cgi HTTP/1.0.

17. Se prueba el empalme de sesión.

Muchos IDS/IPS solamente verifican firmas particulares y no toman en cuenta el empalme de paquetes o el chequeo a través de múltiples paquetes un ejemplo de esto es:

"GET / **HTTP/1.0"** que puede ser dividido en múltiples paquetes como **"GE", "T ", "/", " H", "T","TP", "/1", ".0".**

3.3.3 Método para redes inalámbricas

1. Como primer paso se captura el tráfico entre el punto de acceso y los dispositivos vinculados, para así determinar que dispositivos se encuentran conectados al punto de acceso inalámbrico. Esto se logra utilizando “*Airdump*” en modo de escaneo, la cual forma parte de la suite de herramientas de “*Aircrack*”.

2. Se verifica la encriptación.

Se verifica qué tráfico no encriptado atraviesa la red inalámbrica. Para lograr esto se utiliza un *sniffer* como por ejemplo “*AiroPeek*”.

3. Se desencripta las llaves estáticas WEP.

Se utiliza la herramienta "*AirSnort*" para la obtención de paquetes de interés que son los que contienen vectores de inicialización débiles, se necesita obtener entre 1200 y 4000 paquetes IV (*Initialitation Vector*), en promedio de 16 millones de paquetes IV 9000 de estos son débiles.

4. Se aplica fuerza bruta a las llaves usando "*Aircrack*."

   Se utiliza la herramienta "*Aircrack*" la cual es una herramienta de *hacking* para redes inalámbricas que es empleada para desencriptar contraseñas WEP a través de fuerza bruta.

5. Se suplanta la dirección MAC.

   Suplantar una dirección MAC de un paquete capturado y tratar obtener acceso. Esto solo es aplicable cuando el ACL (Access Control List) basado en direcciones MAC está configurado.

6. Se Interrumpe la señal. A través de un dispositivo llamado "*Jammer*" se interrumpe la frecuencia 2.4 Ghz la cual es utilizada por las redes inalámbricas. Dependiendo de las capacidades del dispositivo se puede bloquear frecuencias de celulares o cualquier otra frecuencia que se desee.

7. Se captura el tráfico inalámbrico.

   Se captura el tráfico en busca de contraseñas e información sensible que viaje en texto plano. Esto se logra a través del *Sniffer* "*AirDump*".

8. Se prueba generación rápida de tráfico. Se emplea la herramienta "*Airplay*" para generar tráfico una vez conocidas dirección MAC destino y fuente de dos (2) computadores de la red inalámbrica, de manera de poder verificar la tolerancia de agotamiento de los recursos de memoria y banda ancha.

9. Se prueba la inyección de paquetes encriptados.

   Se utiliza la herramienta "*WEPWedgie*" para inyectar paquetes encriptados.

10. Se descifra un paquete WEP.

    Se utiliza la herramienta "*chopchop*" que permite desencriptar un solo paquete sin tener conocimiento de la contraseña WEP. [5]

4. Marco aplicativo

En el capítulo 3 se describió la metodología a utilizar para la instalación del dispositivo integrado de seguridad UTM y la metodología LPT la cual permite evaluar la factibilidad del mismo. A continuación, se describe el proceso práctico que se siguió a lo largo de la implementación del UTM y el proceso de intrusión realizado a los diferentes servicios.

La implementación de la metodología se llevo a cabo en una institución pública relacionada con la economía y finanzas del Estado, que requiere protección ante ataques informáticos mixtos y una administración sencilla de la red, a través de un esquema que permite la segmentación de la red LAN y DMZ para servidores expuestos de forma independiente.

4.1 Análisis de vulnerabilidades

Antes de iniciar la implementación del dispositivo UTM, se lleva a cabo un análisis de vulnerabilidades donde se determina las vulnerabilidades informáticas presentes en la institución, las cuales son solventadas cubriendo los objetivos definidos en el capítulo 1.

Para realizar el escaneo de vulnerabilidades se emplea la herramienta "*NESSUS*" [14]. A través de esta herramienta se detectan vulnerabilidades potenciales en el sistema escaneado, también identifica malas configuraciones y falta de actualizaciones, así como pruebas de denegación de servicio contra la pila TCP/IP.

"*NESSUS*" consiste en un demonio *nessusd* que realiza el escaneo en el sistema objetivo y un cliente *nessus* la cual es una interfaz gráfica que muestra el avance y reporte de los escaneos.

El análisis de vulnerabilidades se encuentra como anexo al documento de TEG [Anexo B].

4.2 Selección de esquema de red

Dado que la institución va a hacer uso de servidores web los cuales se desean sean independientes de la red local, se utiliza un esquema de red que permite la creación de un segmento de red local e internet con zona DMZ para servidores expuestos.

4.3 Implementación del UTM

Una vez identificadas las vulnerabilidades de la institución se hace un contraste que muestre las mejorías tras la implementación del dispositivo UTM.

La configuración del dispositivo integrado de seguridad UTM se basa en la política de uso de internet definida por la institución, la cual se encuentra en el anexo A del documento del T.E.G [Anexo A].

Para la instalación del dispositivo se utiliza el procedimiento de instalación *Watchguard* la cual fue descrita en el capítulo 3. Como indica el primer paso del procedimiento, se procede a la instalación del programa base "*Watchguard* System Manager" al cual se le hace referencia como WSM en el resto del documento. Este es un ejecutable que contempla los siguientes pasos:

1. Pantalla de presentación que indica el programa a instalar.

2. Lectura del contrato de licencia del programa, la cual se tiene que aceptar para continuar con la instalación.

3. Selección de la ruta o directorio donde se desea instalar la aplicación, por defecto el directorio de instalación es: C:\Archivos de programa*Watchguard*.

4. Se seleccionan los componentes a instalar en el sistema, el cual se divide en las siguientes dos categorías:

    I. Software del cliente, el cual contiene el WSM.

    II. Software del servidor, el cual contiene el "*Log Server*" que se encarga de almacenar los logs de eventos, el "*WebBlocker Server*" que contiene la base de datos de las categorías que se pueden bloquear, el "*Quarantine Server*" que contiene los archivos infectados detectados por el antivirus y el "*Report Server*" que genera los reportes en base a los *logs* registrados.

5. Una vez seleccionado los componentes se da comienzo a la instalación.

6. Pantalla que muestra progreso de la instalación.

7. Pantalla que indica culminación satisfactoria o no de la instalación.

Seguidamente, como segundo paso del procedimiento, se actualiza el WSM a través de un ejecutable que contempla los siguientes pasos:

1. Pantalla de presentación, que indica a que versión de WSM se le va a realizar la actualización.

2. Al dar clic en *siguiente* se comienza la actualización del WSM.

3. Pantalla que muestra progreso de la actualización.

4. Pantalla que indica culminación satisfactoria o no de la instalación.

Posteriormente, como tercer paso del procedimiento, se instala el firmware de la versión actualizada la cual es sincronizada con el dispositivo UTM para su correcto funcionamiento, esto a través de un ejecutable que contempla los siguientes pasos:

1. Pantalla de presentación que indica el programa a instalar.

2. Selección de la ruta o directorio donde se desea instalar la aplicación, por defecto el directorio de instalación es: C:\Archivos de programa\Archivos comunes*Watchguard*\resources\Fireware.

3. Al dar clic en *siguiente* se procede a la instalación del firmeware.

4. Pantalla que muestra progreso de la instalación.

5. Pantalla que indica culminación satisfactoria o no de la instalación.

Se procede a la configuración del WSM en base a las políticas de uso de internet definidas por la institución. A continuación se muestra la Figura 11 que muestra la interfaz gráfica principal del WSM

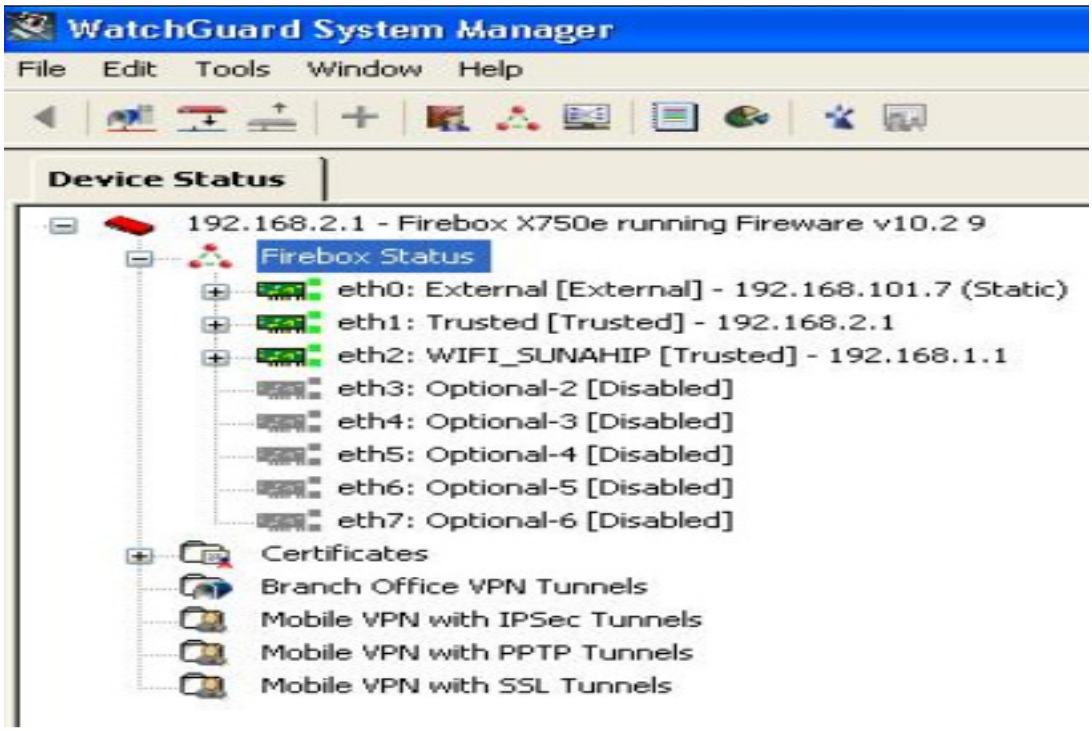


Figura 11. Interfaz del WSM

Se procede a la apertura del "*Policy Manager*" tal como indica la Figura 12.

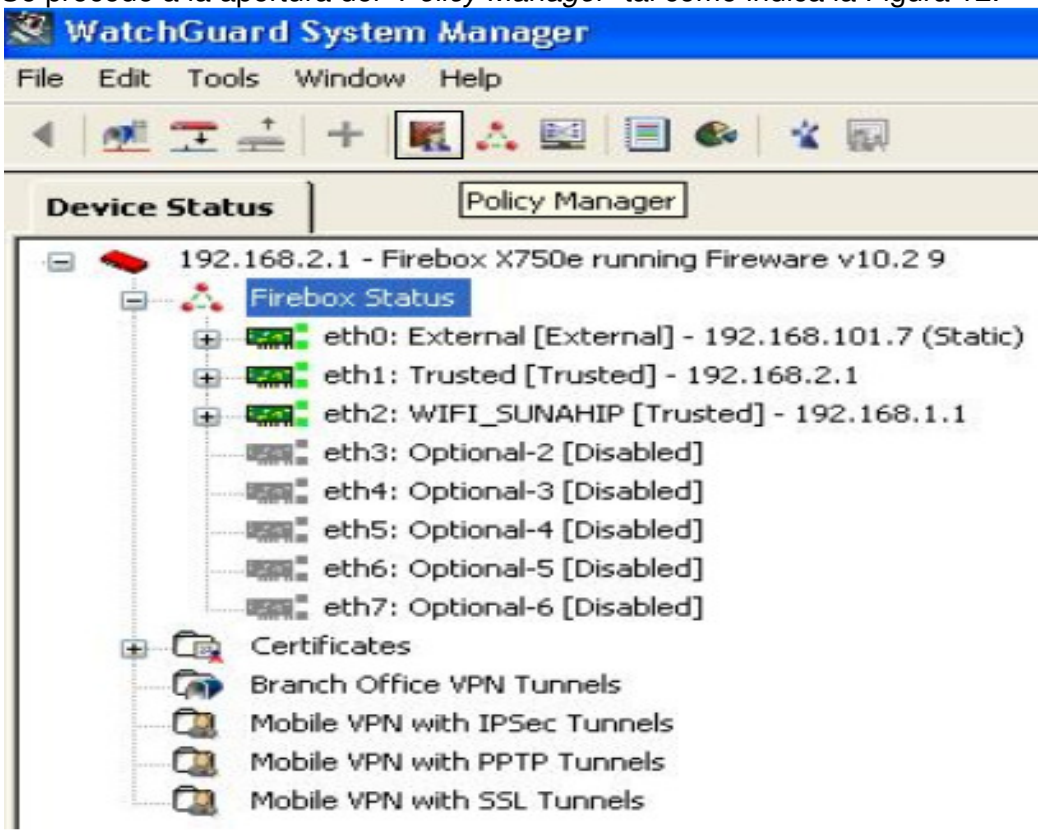


Figura 12. Selección del "Policy Manager" en el WSM

Realizando de esta forma la apertura de la interfaz gráfica del "*Policy Manager*" la cual se muestra en la Figura 13 – 14.

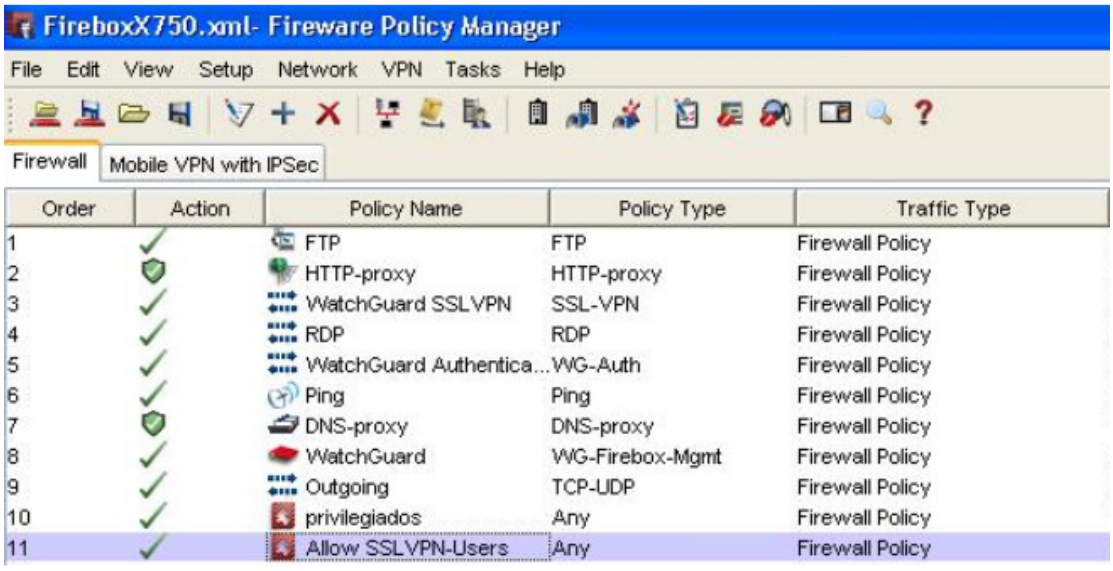


Figura 13. Interfaz del Policy Manager A

Log	Alarm	From	To	Port
No	No	Any-Trusted Any-Optional	Any-External	tcp:21
No	No	Todos	Any-External	tcp:80
No	No	Any-External Any-Trusted Any-O...	Firebox	tcp:443
No	No	192.168.1.4 192.168.1.6 192.168....	192.168.2.113	tcp:3389
No	No	Any-Trusted Any-Optional Any-Ex...	Firebox	tcp:4100
No	No	Any-Trusted Any-Optional	Any	ICMP (type: 8, code: 255)
Yes	No	Privilegiados Todos Firebox	10.1.4.3	tcp:53 udp:53
No	No	192.168.2.113	Firebox	tcp:4103 tcp:4105 tcp:4117
No	No	Any-Trusted Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)
Yes	No	Privilegiados	Any-External	Any
No	No	SSLVPN-Users (Firebox-DB)	Any	Any

Figura 14. Interfaz del Policy Manager B

Como se logra apreciar existen 11 políticas definidas, en esta interfaz se permite la creación, modificación y eliminación de políticas, así como las deshabilitación de las mismas. Al momento de la creación de políticas se puede elegir entre tres (3) tipos de políticas que son:

1. De Filtrado de paquetes.
2. *Proxies*.
3. Personalizados.

   En la Figura 15 se logra apreciar las políticas que tienen una previa configuración la cual puede ser usada como base y con pequeños cambios adaptarlas a las necesidades de la institución

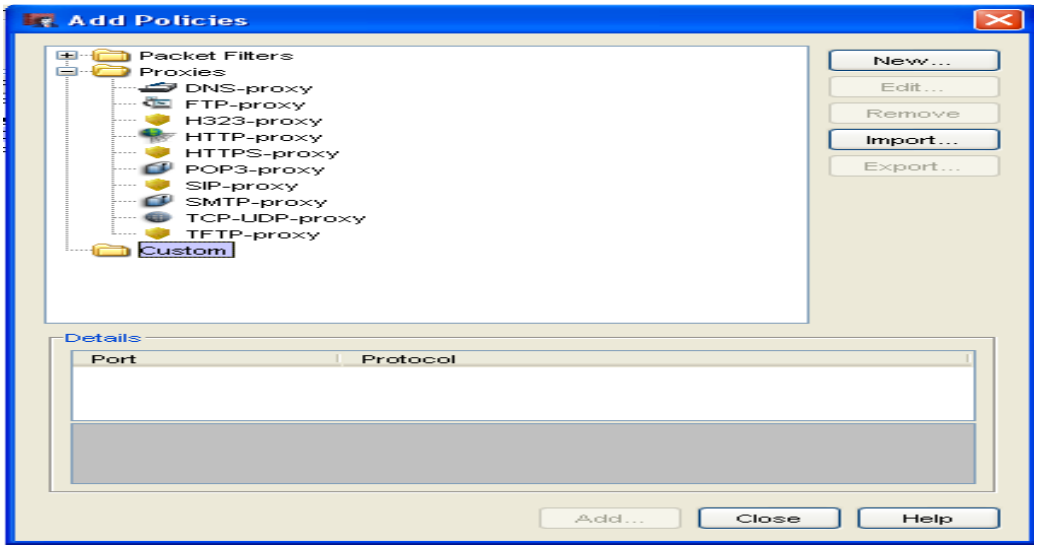


Figura 15. Interfaz de creacion de políticas

Para la eliminación, modificación o deshabilitacion de una política basta con un clic derecho sobre la política a la cual se le desea realizar la acción. Para el caso de la institución se realizaron las siguientes políticas:

1. **FTP**: Permite abiertamente tráfico tanto interna como externamente a través del puerto 21.

2. **HTTP – Proxy**: Permite al segmento de usuarios *Todos,* acceso libre hacia el exterior a través del puerto 80.

3. ***Watchguard* SSL VPN**: Permite una conexión segura al dispositivo desde cualquier punto de origen a través del puerto 443.

4. **RDP**: Permite el uso del protocolo RDP (*Remote Desktop Protocol*), el cual es utilizado para administración remota y está permitida solo por las IP privadas 192.168.1.4 – 192.168.1.6 – 192.168.1.7 hacia el servidor del dispositivo que es la dirección 192.168.2.113 a través del puerto 3389.

5. ***Watchguard* Autenthication**: Permite la comunicación desde cualquier punto sea interno o externo hacia el dispositivo, con la finalidad de permitir la autenticación de conexiones VPN a través del puerto 4100.

6. ***Ping***: Está definida de forma de que cualquier zona de confianza u opcional pueda hacer *ping* a cualquier dispositivo que se encuentre externo a la red. La intención de la creación de esta regla es evitar que entes externos logren hacer *ping* al dispositivo o a cualquier computador de la red interna.

7. **DNS Proxy**: El segmento de usuarios *Privilegiados, Todos* y el *Dispositivo* tienen acceso libre al servidor DNS con dirección IP 10.1.4.3 a través del puerto 53.

8. ***Watchguard***: Permite una conexión exclusiva entre el servidor y el dispositivo a través de los puertos 4103-4105-4117. La finalidad de esta política es asegurar que no exista interrupciones de ningún tipo entre el servidor y el dispositivo.

9. **Outgoing**: Es una política por defecto que permite desde cualquier zona de confianza u opcional tener acceso externo a través de cualquier puerto.

10. **Privilegiados**: Asegura que el segmento de usuarios *Privilegiados* pueda tener acceso externo libre.

11. **Allow SSL-VPN Users**: Permite a la red de usuarios VPN tener acceso libre.

Adicionalmente, se tiene un filtro de páginas web basadas en categorías, tal como se puede apreciar a continuación en la Figura 16.

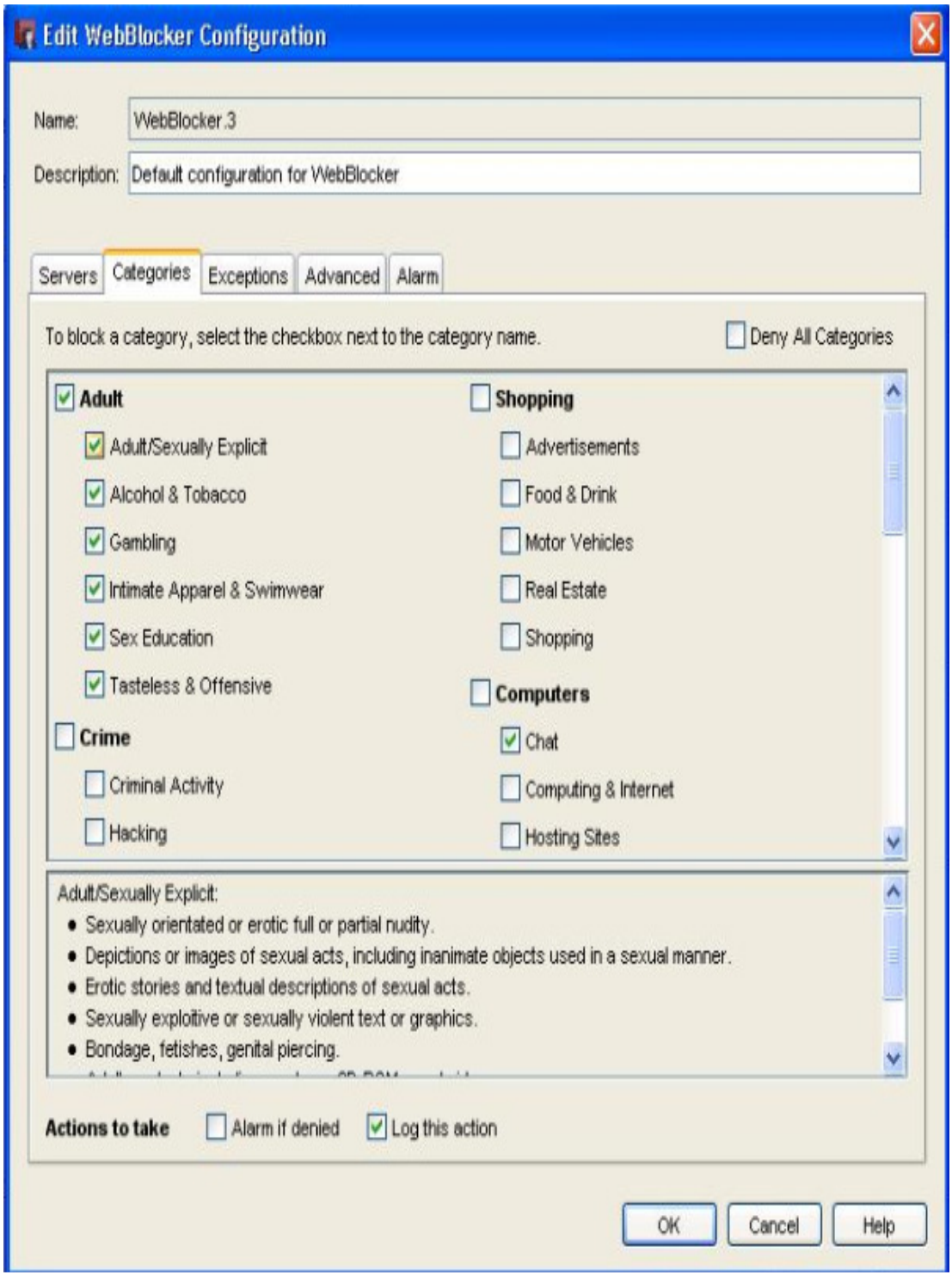


Figura 16. Interfaz de categorias del WebBlocker

Un punto clave para el administrador de red y el analista de seguridad es el uso del "*Firebox System Manager*" el cual puede ser accedido desde el WSM como muestra a continuación la Figura 17.

Figura 17. Selección del Firebox System Manager desde el WSM

Realizando así la apertura de la interfaz gráfica como lo muestra la Figura 18

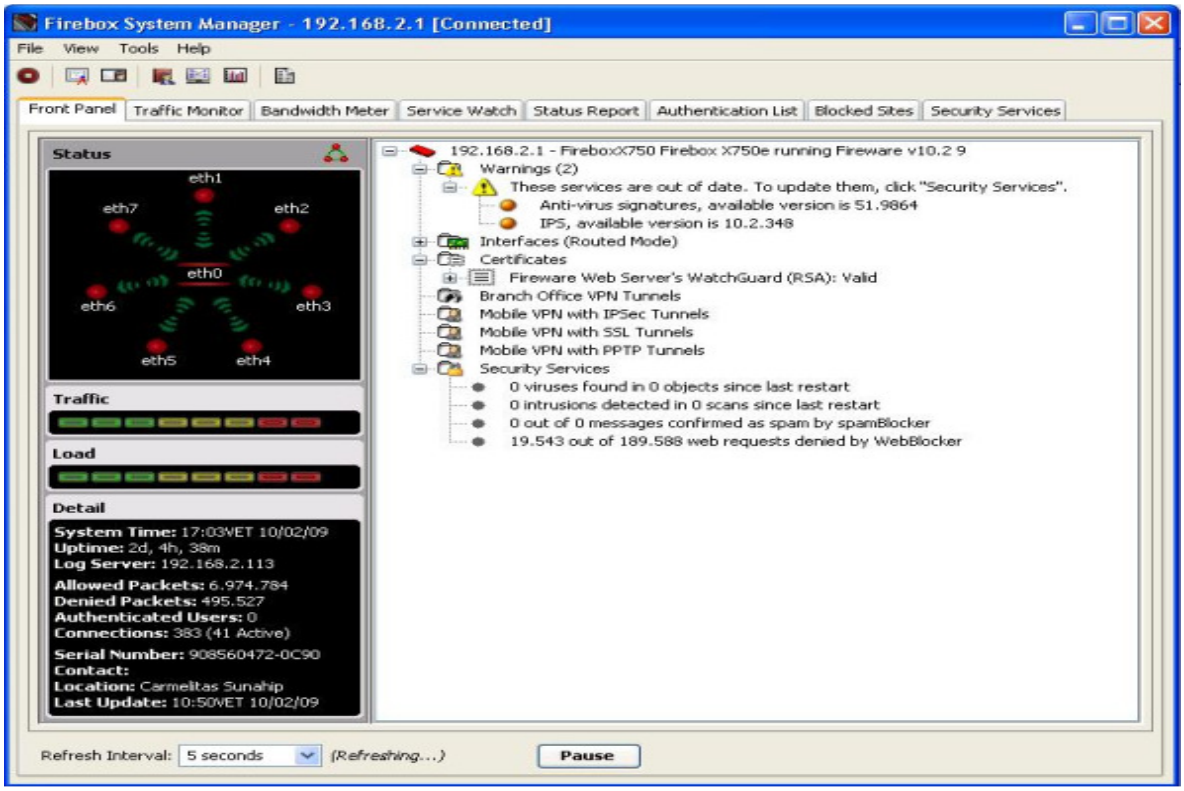


Figura 18. Interfaz del Firebox System Manager

A través de esta interfaz se obtiene conocimiento de cantidad de paquetes permitidos y denegados, verificar el tráfico que genera un computador en particular, medir el uso del ancho de banda así como verificar cuales son los servicios que lo están consumiendo, ver un reporte resumen sobre las actividades más recientes y quiénes se han conectado a la red, permite verificar si hay alguna dirección bloqueada de manera estática por el administrador y verificación del estado de los servicios de seguridad que proporciona el UTM.

Otra herramienta poderosa que debe ser tomada en cuenta por los administradores de red y analistas de seguridad es el "Host Watch" la cual se accede desde el WSM como lo muestra a continuación la Figura 19.

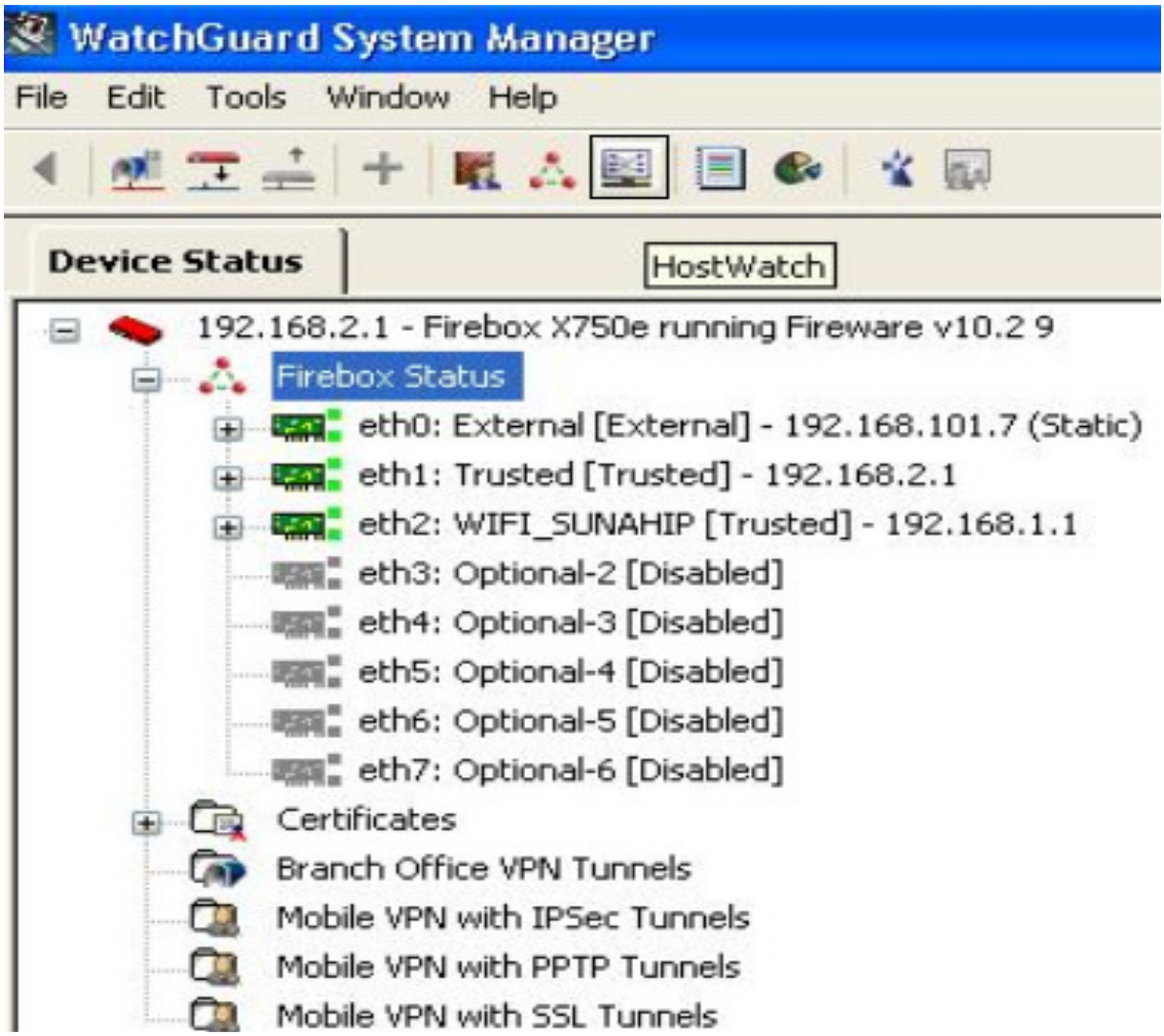


Figura 19. Selección del HostWatch desde el WSM

Realizando así la apertura de la interfaz gráfica como lo muestra la Figura 20

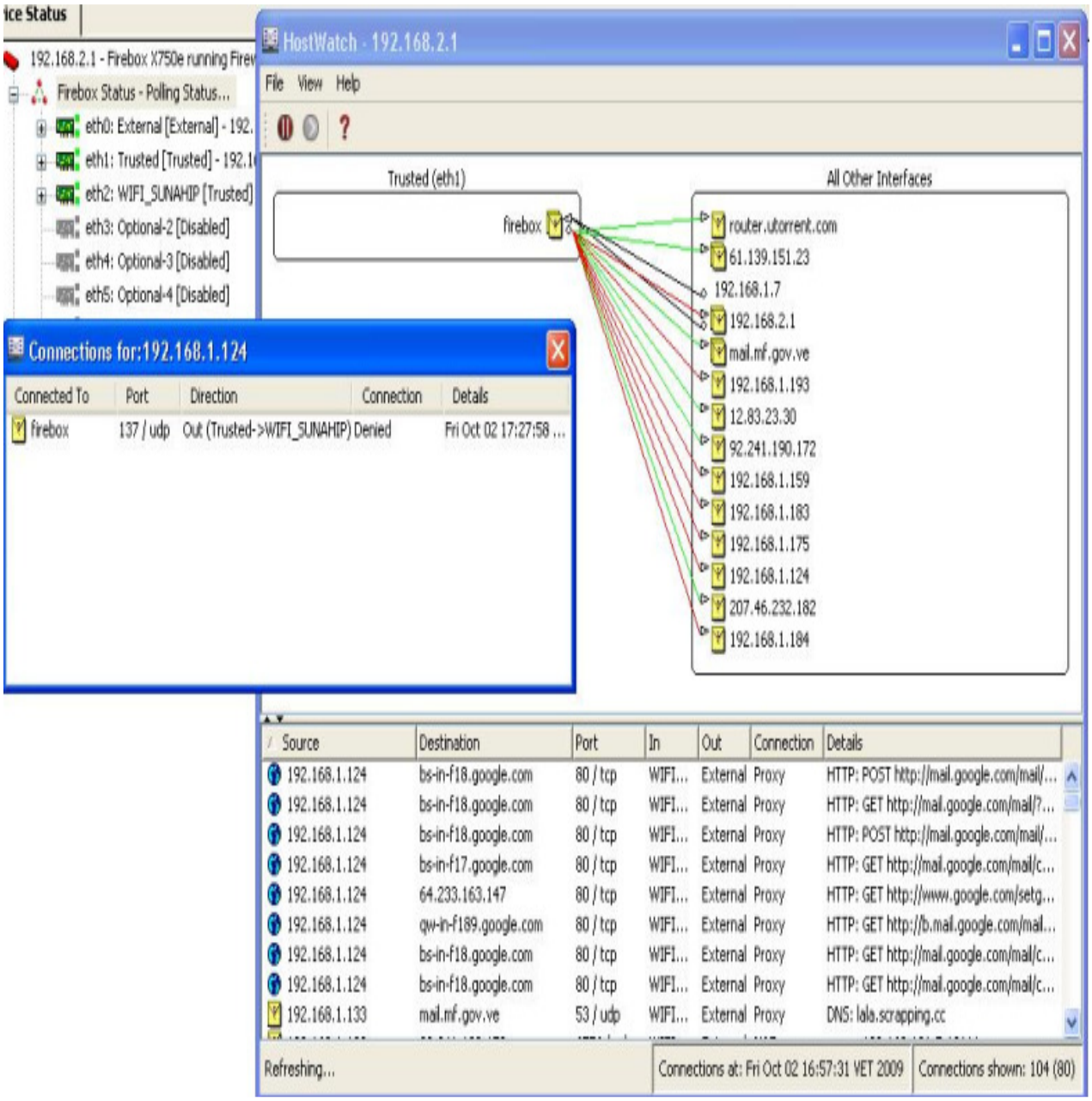


Figura 20. Interfaz del HostWatch

Esta interfaz permite de manera gráfica visualizar las diferentes conexiones existentes en el dispositivo, las líneas rojas indican un patrón dañino que al hacer doble clic muestra sus características, dando la opción de bloquear dicha máquina para evitar la propagación de la infección en la red por el tiempo que se desee como lo muestra a continuación la Figura 21.

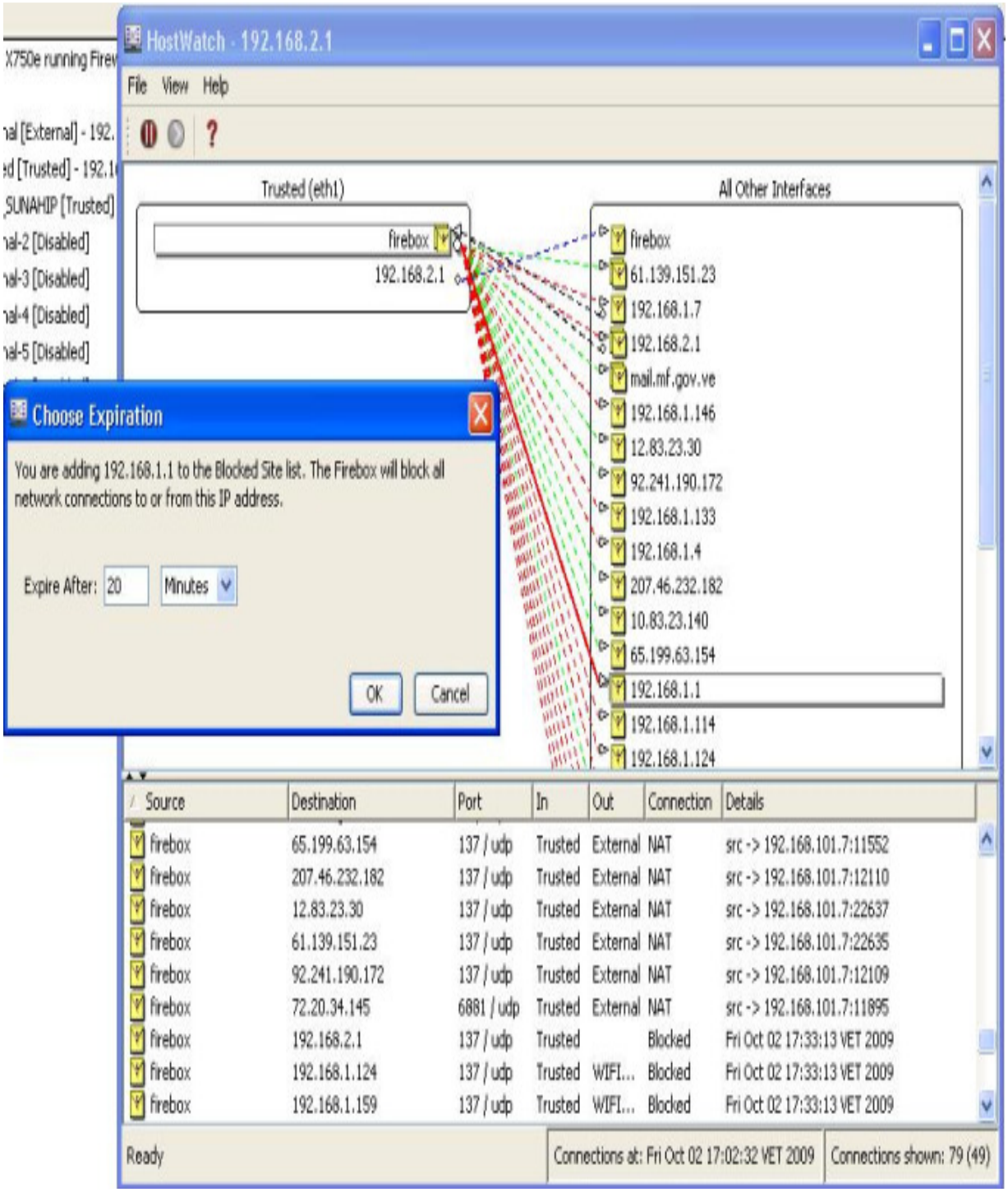


Figura 21. Interfaz del HostWatch para bloqueos

5. Pruebas y resultados

Firewall

Se localiza el *firewall* a través del uso de la herramienta "*HPing2*" con el siguiente comando **hping2 192.168.2.113 –c2 –S –p23 –n** obteniendo como respuesta **ICMP Unreachable type 13 from 192.168.2.113**. Adicionalmente se logro obtener la siguiente traza:

For your information, here is the traceroute from 192.168.10.5 to 200.74.233.142 :
192.168.10.5
?
192.168.0.1
192.168.17.130
161.196.251.69
200.109.126.217
?
200.44.43.21
200.44.43.77
64.215.187.69
67.16.132.10
213.200.84.37
213.200.73.6
200.74.216.60
?

Se ejecuta la herramienta "*NMAP*" con el comando nmap -n -vv -P0 -p256 <Host> obteniendo el resultado de la existencia de un puerto TCP 256 que se encuentra filtrado por el *firewall* como lo muestra a continuación la Figura 22.

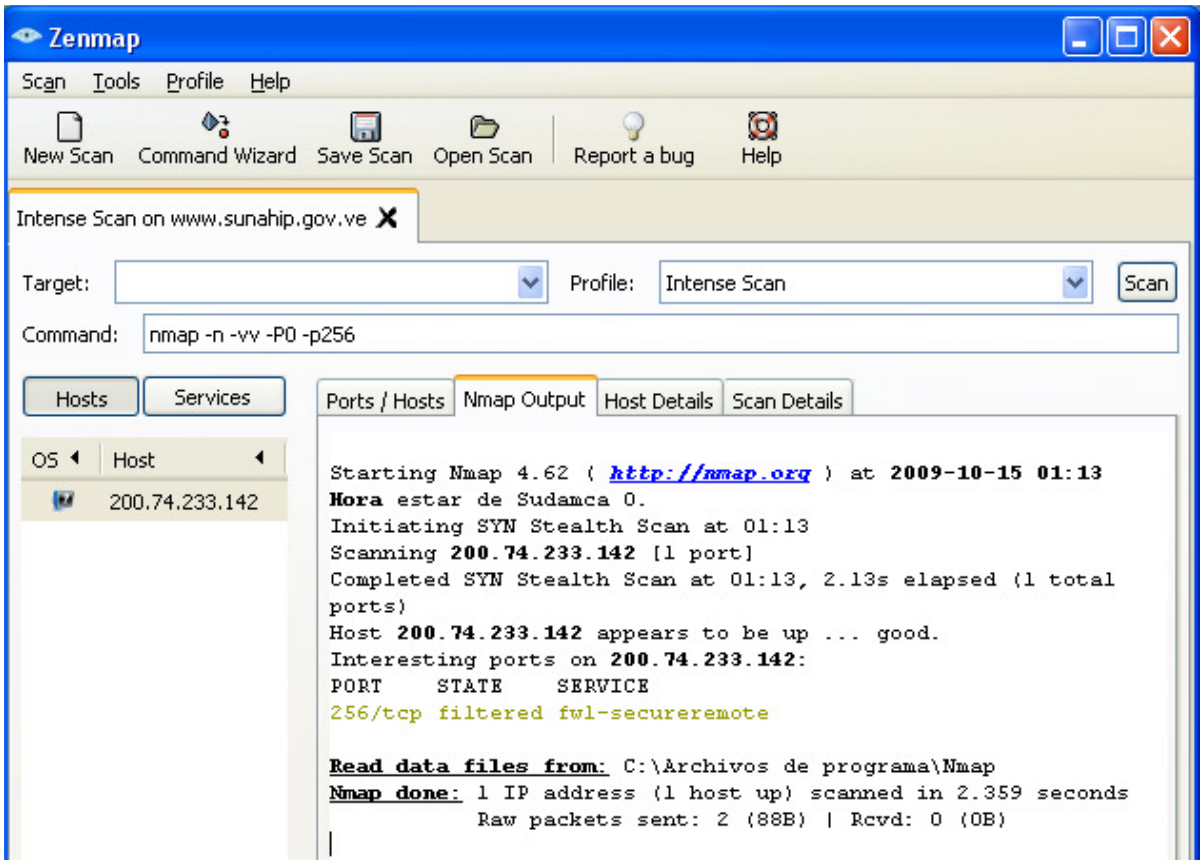


Figura 22. Puertos filtrados por el *firewall* - NMAP

No se logra obtener que se utiliza un servidor Windows 2003 con IIS 6.0 (*Internet Information Server*) con tecnología del lado del cliente ASP .NET, esto debido a que hay restricciones para realizar el *ping* de manera externa. A través de la creación de paquetes personalizados no se logra identificar el tipo de *firewall* debido a que igual que en la condición anterior existen reglas respecto al *ping* de manera externa, se logro constatar con el uso diario del dispositivo y en las pruebas de la realización de operaciones prohibidas que el dispositivo responde correctamente ante las políticas. Se prueba la utilización de canales cubiertos y redirección de puertos siendo estos detectados por el IPS bloqueando así la comunicación y no se encontraron vulnerabilidades especificas para el *Wathguard Firebox e750 con WSM 10.2.9.*

IDS/IPS

Se prueba el agotamiento de los recursos inundándolo con peticiones ARP utilizando la herramienta "*ARP Request Stress Tool*" como lo muestra a continuación la Figura 23.

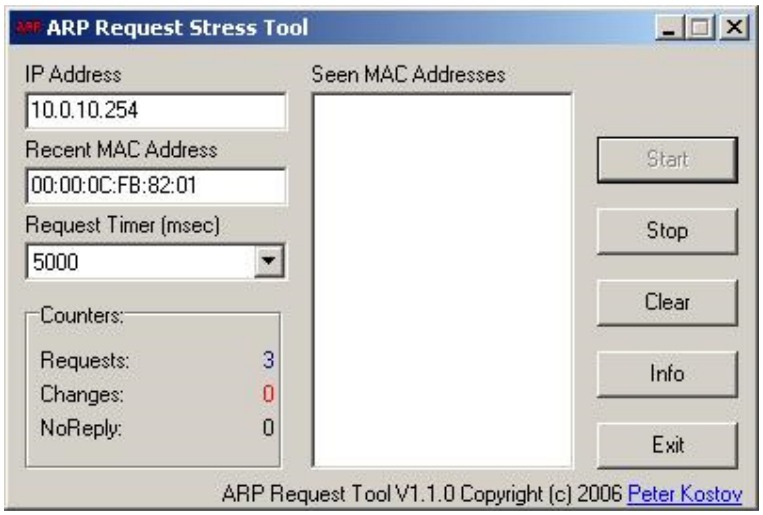


Figura 23. Interfaz de la herramienta ARP Request Stress Tool

detectándolo el IPS y bloqueándolo, seguidamente también a través del IPS se logra la detección de la suplantación de identidades de direcciones MAC e IP, un ejemplo de la herramienta "*MAC Spoofer*" se muestra a continuación en la Figura 24.

Figura 24. Interfaz de herramienta MAC Spoofer

Se emplea la herramienta "*HPing2*" para probar el envío de paquetes a la dirección de *broadcast* para causar una sobre carga en el dispositivo, lo que induce a un estado de inhibición causando la pérdida del servicio internet de la institución (hay que tomar en cuenta que este es un tipo de ataque interno), solventándolo con el reinicio del dispositivo. De esta manera se logra observar que todo el ataque queda registrado en los *logs*.

Posteriormente, ante la presencia de fragmentos duplicados el dispositivo solamente salva el primer fragmento y en el intento de causar una denegación de servicio a través del *ping de la muerte,* el IPS lo detecta de manera automática bloqueando el paquete.

Seguidamente, ante la presencia de paquetes impares, éstos son descartados automáticamente por el dispositivo y el puerto cero (0) se encuentra filtrado. Se prueba las manipulaciones de las banderas con la herramienta "*HPing2*" y "*NMAP*" siendo todas bloqueadas por el *firewall* en conjunto con el IPS. Se aplica la inundación de paquetes SYN con la herramienta "*ThunderFlood V1.1*" como se muestra a continuación en la Figura 25

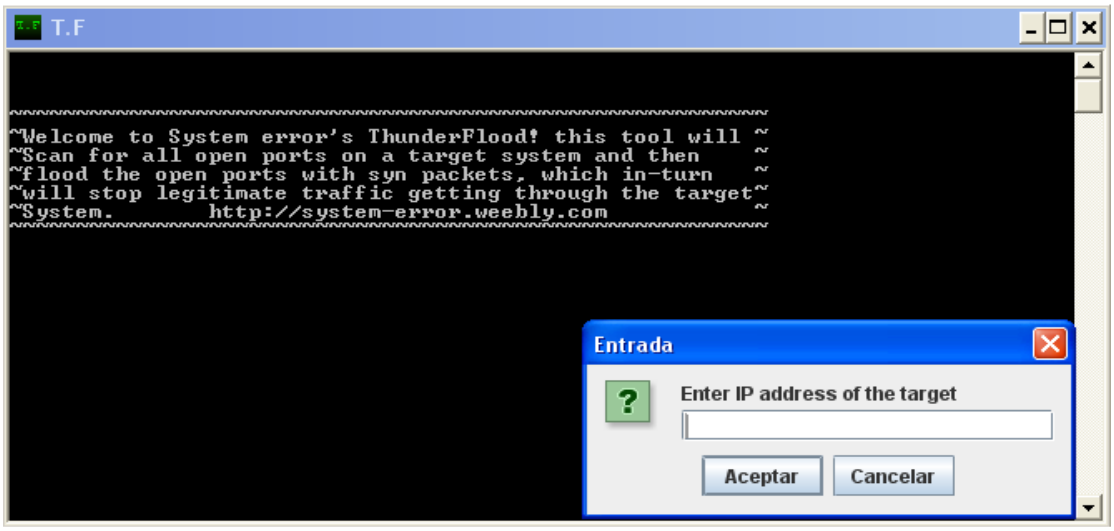


Figura 25. Interfaz de herramienta ThunderFlood

Estos son bloqueados, así como la codificación del URL y la solicitud de recorrido de directorio inverso, las culminaciones de peticiones son superadas por el dispositivo, por lo que se escanea todo completo y el empalme de sesión es tomada en cuenta por el dispositivo.

Redes inalámbricas

Se "*sniffea*" el tráfico con la herramienta "*AiroDump*" ejecutándose como muestra a continuación la Figura 26

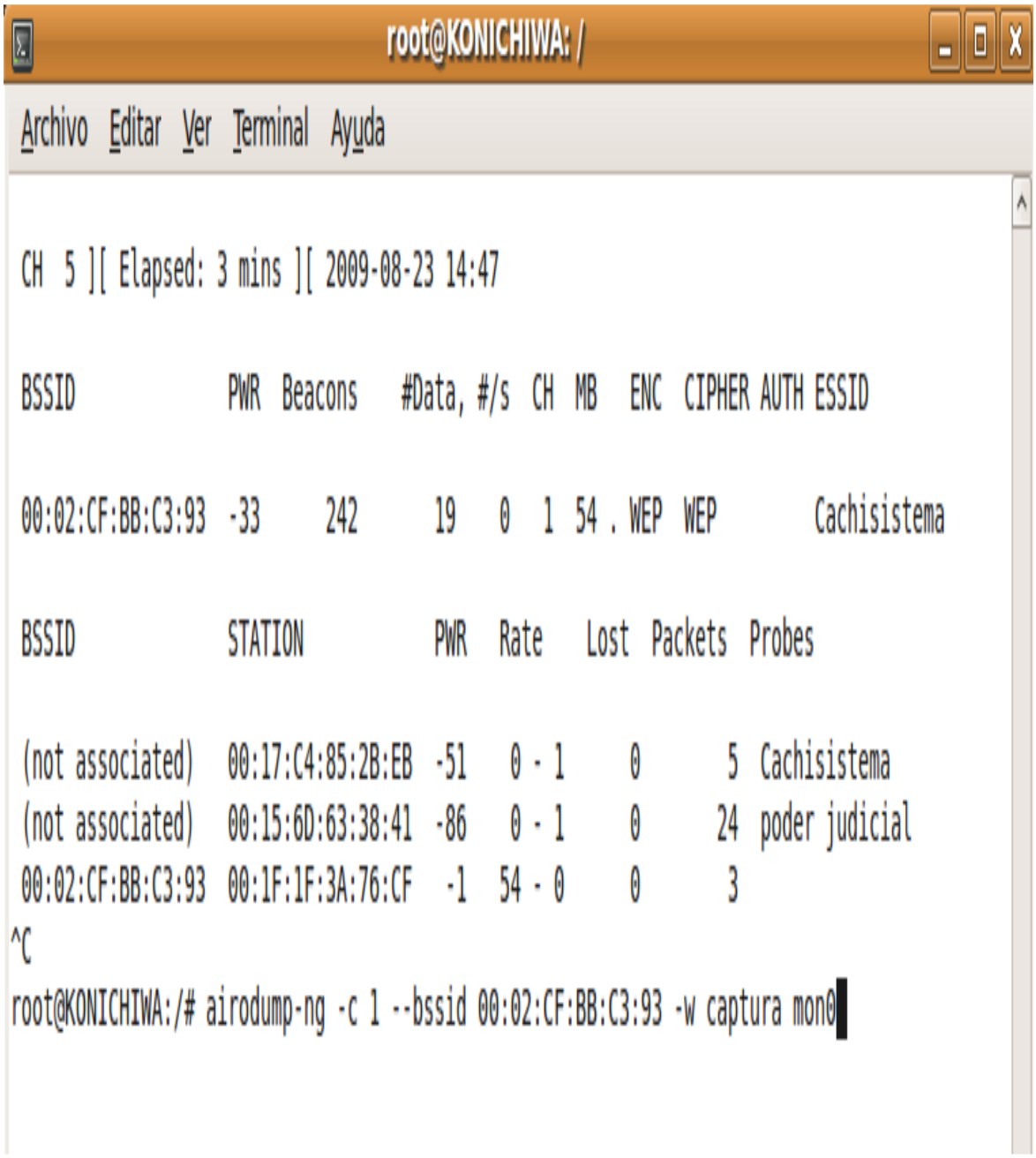


Figura 26. Ejecución de AiroDump

Igualmente se "*sniffea*" el tráfico con la herramienta "*AiroPeek*" para lograr verificar qué tráfico no encriptado atraviesa la red. Una muestra de la corrida del programa se muestra a continuación la Figura 27.

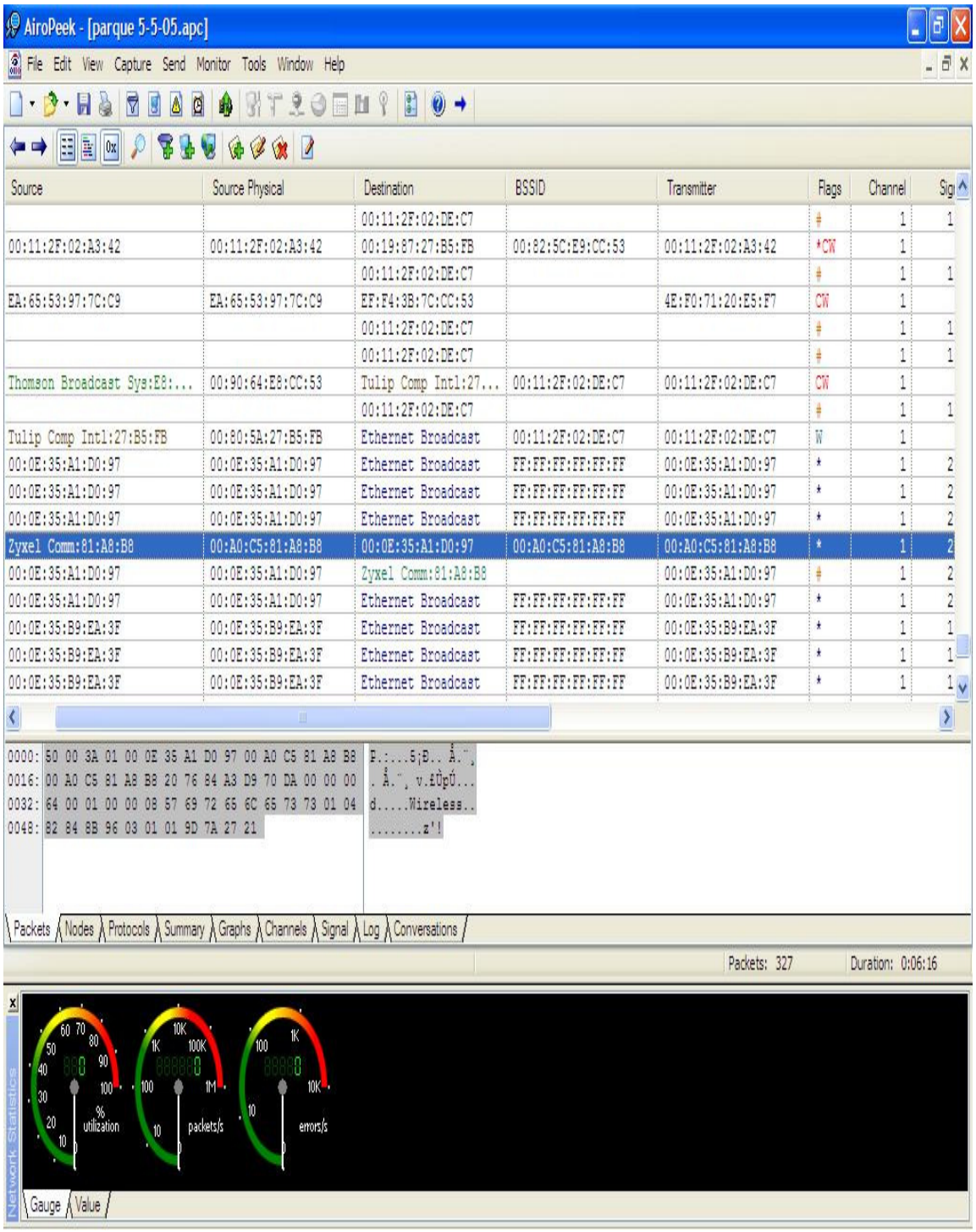


Figura 27. Captura de paquetes con AiroPeek

Posteriormente, se "*crackea*" la contraseña WEP previamente identificada con la herramienta "*AirCrack*" logrando *crackearla* y obteniendo la contraseña en pocos minutos, un ejemplo de su interfaz se representa a continuación en la Figura 28.

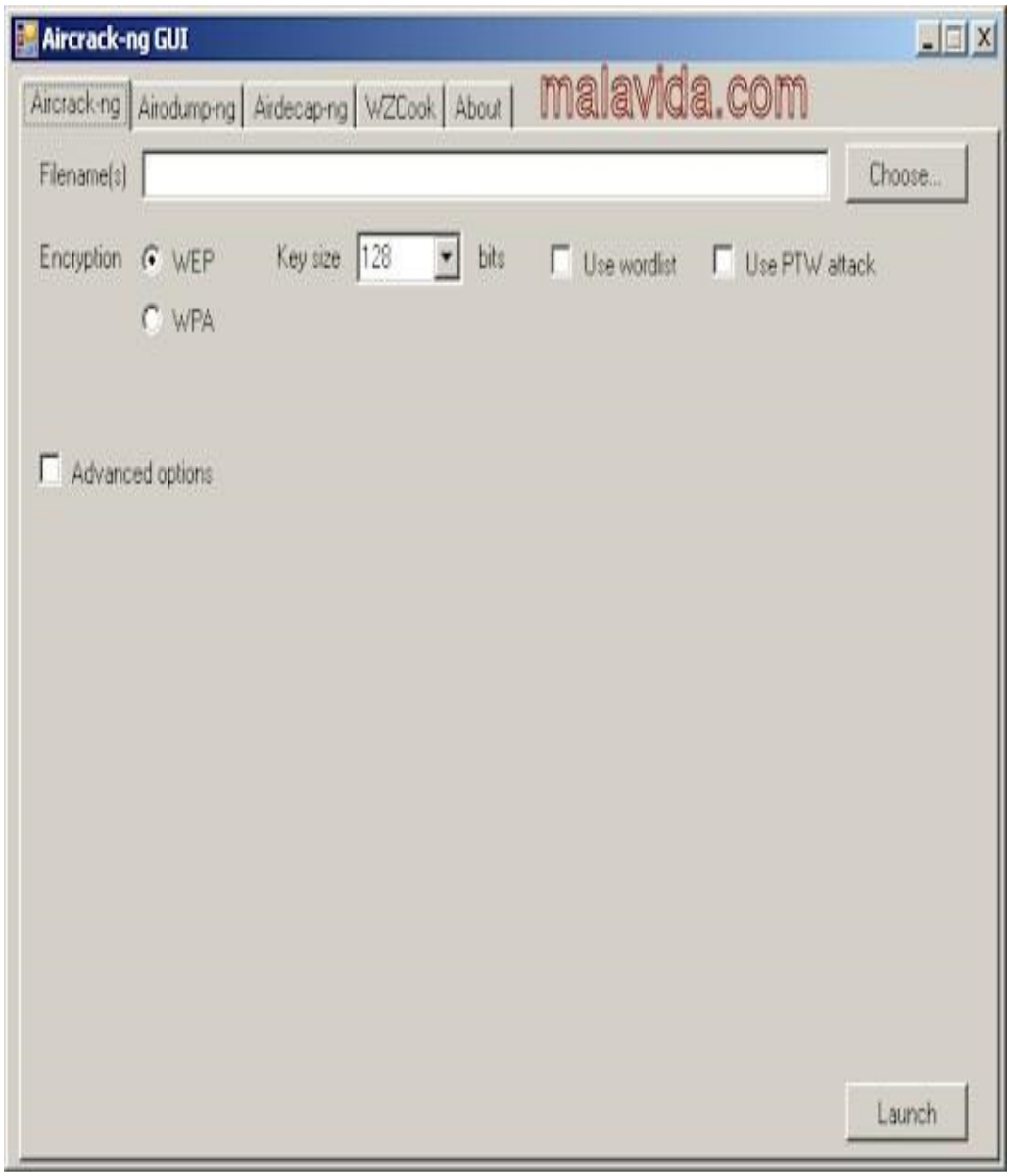


Figura 28. Interfaz gráfica de Aircrack

No se realiza la suplantación de direcciones MAC ya que no está implementada la lista de control de acceso basado en direcciones MAC, tampoco se realiza la interrupción de la señal o frecuencia, debido a que no se cuenta con ningún dispositivo que inserte ruido en las frecuencias deseadas. Se verifica el tráfico "*sniffeado*" y se logra dar con las contraseñas FTP que viajaron en texto claro.

Seguidamente, se prueba la generación rápida de tráfico empleando la herramienta "*AirPlay*" observando buena tolerancia por parte del *router*. Se inyectan paquetes encriptados con la herramienta "*WEPWedgie*" para generar más tráfico y facilitar el *crackeo* de la contraseña, un ejemplo de su ejecución se encuentra reflejada a continuación en la Figura 29.

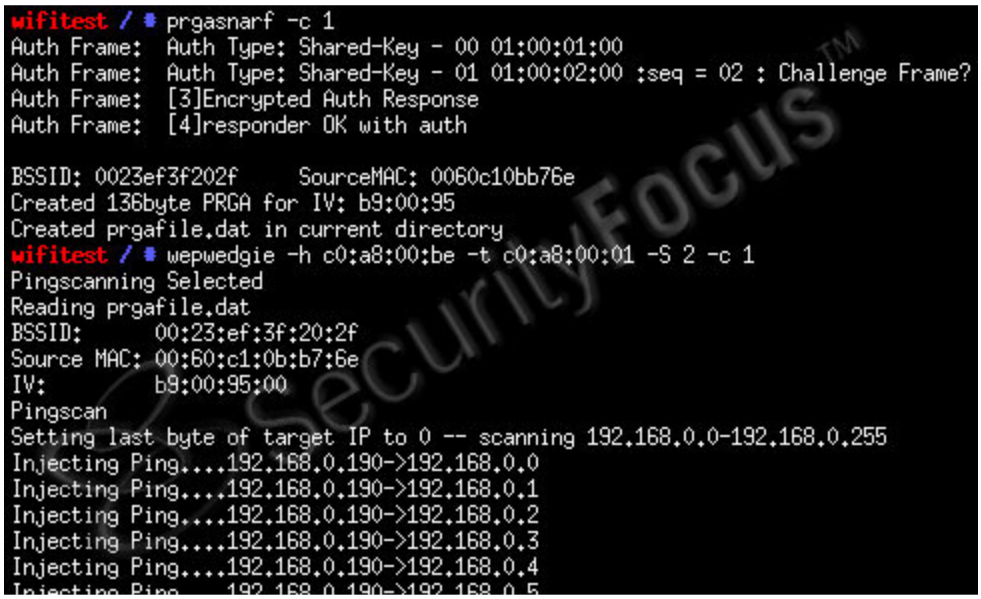


Figura 29. Ejecución de herramienta WEPWedgie

http://www.opennet.ru/base/sec/wep_sec5.jpg

Se logra de manera satisfactoria la desencriptacion de un solo paquete a través de la herramienta "*chopchop*", un ejemplo de su ejecución es representada a continuación por la Figura 30.

Figura 30. Ejecución de CHOPCHOP

http://www.securityfocus.com/pen-test/images/chopchop.jpg

Comparación antes/después de análisis de vulnerabilidades

Antes	Vulnerabilidades	Después
4025	Altas	1
181	Medias	1
0	Bajas	0
23	Advertencias de Seguridad	23

6. Trabajos a futuro

Gracias al desarrollo del Trabajo Especial de Grado, se sugieren recomendaciones para la implementación de proyectos en el área de redes y telecomunicaciones en la institución que escapan del alcance del presente trabajo y cuya aplicabilidad complementaría la seguridad informática, como la activación de la *alta disponibilidad* en conjunto con otro dispositivo UTM y aplicaciones de metodologías de intrusión de avanzada de manera periódica.

Igualmente se sugiere a la institución en el mediano plazo la implementación de *LDAP (Lightweight Directory Access Protocol) o Active Directory* para tener un mayor control de los usuarios respecto al uso del computado.

Por último, se recomienda que la institución emprenda una campaña de culturización en materia de seguridad informática que sea impartida por la máxima autoridad, creando conciencia del "*buen uso*" de los recursos informáticos.

7. Conclusiones

Se cumplió con el objetivo del trabajo el cual era implementar un dispositivo integrado de seguridad UTM evaluando la factibilidad de su configuración a través de la metodología LPT, dicha implementación permite la administración de la red de manera sencilla y segura.

La investigación realizada en el marco conceptual junto al desarrollo explicado en el marco aplicativo dio como resultado un dispositivo UTM funcional y verificado. Esta implementación fue realizada llevando a cabo la metodología de instalación de *Watchguard* y configurando el dispositivo en base a los requerimientos y políticas de uso de internet de la institución.

El dispositivo realiza la administración de la red de forma sencilla y segura, por lo que facilita la labor del administrador de la red y el analista de seguridad debido a que todos los eventos son configurables y pueden ser registrados en logs para su posterior análisis. Los diferentes servicios de seguridad del dispositivo poseen una baja cohesión, por lo cual la falla de alguno de los servicios no implica necesariamente la caída completa del sistema.

Los reportes del dispositivo pueden ser consultados y generados en cualquier momento, así como la posibilidad de obtener información de lo que pasa en la red en tiempo real. Esto permite un análisis de la condición de la red de manera sencilla y rápida.

Para llevar a cabo la evaluación de la factibilidad de la configuración del dispositivo se empleó la metodología de intrusión LPT. Esta metodología permitió llevar a cabo pruebas de intrusión en diferentes dispositivos y entornos de trabajo. Para nuestro caso se realizaron pruebas a *firewall*, IDS/IPS y redes inalámbricas, obteniendo resultados satisfactorios en lo que a seguridad informática se refiere dada las altas prestaciones del dispositivo.

A través del T.E.G. se pudo conocer más en cuanto a contra medidas efectivas para la prevención de ataques por parte de los hackers, lo que representa un aporte adicional a los conocimientos obtenidos a lo largo de la carrera y a las actividades extracurriculares desarrolladas en el área de seguridad informática.

Glosario de Términos

- **Acceso Remoto**: Es un método de comunicación que permite acceso a un sistema o red desde una ubicación remota.

- ***Active Directory:*** Termino utilizado por Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.

- **Anónimo**: Indica que no se tiene nombre, identidad o fuente.

- ***Antiphising:*** Servicio de seguridad encargado de verificar la legitimidad de páginas web.

- ***Antispam* (filtro de correo no deseado):** Servicio de seguridad encargado de bloquear o filtrar correo no deseado.

- **Anti-Troyano**: Software especialmente diseñado para ayudar a detectar y remover troyanos.

- **Antivirus**: Un programa que trata de reconocer, prevenir y eliminar virus informáticos y otro software malintencionado del equipo.

- **Buffer Overflow**: Es la situación en la que un programa escribe datos más allá del espacio del búfer asignado en memoria. Esto puede resultar en que memoria válida se sobrescriba.

- **Buffer**: Es una porción de memoria disponible para almacenamiento de datos.

- **Cache**: Es un buffer de almacenamiento rápido.

- ***Crackeo:*** Acción de desencriptar una llave o contraseña.

- **Cross-Site Scripting:** Una explotación de la seguridad informática que se utiliza para ejecutar un script malicioso.

- ***EC-Council:*** Casa de estudio que imparte y otorga certificaciones del area de IT con reconocimiento internacional.

- **Esteganografia**: Es la práctica de ocultar mensajes en una imagen, audio o video.

- ***Firewall*****:** Dispositivo que filtra el tráfico entre redes, puede ser hardware o software sobre un sistema operativo.

- ***FTP (File Transfer Protocol):*** Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.

- ***Hacker*****:** Individuo con amplios conocimientos teóricos-prácticos en seguridad informática que emplea técnicas de manera defensiva u ofensiva.

- ***Hacking:*** Empleo de herramientas o acciones llevadas por un hacker.

- **Ingeniería Social**: Es el arte de explotar debilidades comunes en la naturaleza humana, en lo cual personas inconscientemente revelan información como contraseñas o usuarios o cualquier otra información confidencial.

- **Interconexión de sistemas abiertos (OSI)**: Es un estándar creado por la Organización Internacional de Normas (ISO), que describe siete capas con distintas responsabilidades en el movimiento de datos y de cómo es intercambiado entre los dispositivos de red.

- ***IPS (Intrusion Prevention System):*** Servicio de seguridad encargado de prevenir intrusiones en una red o computador.

- ***Keylogger:*** Hardware o Software que registra pulsaciones del teclado.

- ***LDAP (Lightweight Directory Access Protocol):*** Es un protocolo a nivel de aplicación que permite el acceso de un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

- ***Logs:*** Archivos de almacenamiento de eventos también llamados bitácoras.

- **LPT (*Licensed Penetration Tester*):** Metodología para pruebas de intrusión de la casa EC-Council que define una serie de pasos para probar la seguridad de diferentes equipos, aplicaciones y entornos de trabajo.

- **Privacidad Equivalente a la cableada (WEP):** Es un protocolo de redes locales inalámbricas y fue diseñado para proveer un nivel de seguridad similar a una red local cableada.

- **Protocolo de Integridad de Llave Temporal (TKIP):** Es un estándar de encriptación diseñado para reemplazar WEP ya que proporciona mayor seguridad.

- **Protocolo de Mensajes de Control de Internet (ICMP):** Es un paquete IP encapsulados que se utiliza para enviar mensajes de error y de control.

- **Protocolo de Resolución de Dirección (ARP)**: Es un protocolo TCP/IP usado para resolver una dirección física a partir de una IP.

- **Protocolo de Transferencia de Hipertexto (HTTP)**: Es un protocolo de comunicación que facilita la navegación por el “World Wide Web”.

- **Protocolo**: Es una convención o estándar que controla o habilita comunicaciones, conexiones y transferencias de datos.

- **Puerta trasera**: Una brecha en la seguridad de un sistema informático que se dejó abierta a propósito para obtener acceso posteriormente.

- **Punto de Acceso (AP):** Es un hardware de comunicación que crea un punto central de conectividad inalámbrica.

- **rootkit**: Es una colección de herramientas utilizadas por los hackers después de ganar acceso a un computador mediante las cuales permiten ejecutar diversas acciones maliciosas sobre la víctima.

- ***Router:*** Dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (3) del modelo OSI.

- **Servidor Proxy**: Es un sistema que actúa en nombre de otros y es usado generalmente para dar anonimato.

- **Servidor**: Es una computadora de una red que proporciona servicios a aplicaciones de clientes o computadoras.

- **Sesión**: es una comunicación activa entre un usuario y un sistema o entre dos computadoras y se refiere a la capa 5 (capa de sesión) del modelo OSI.

- **Sistema de Detección de Intrusos (IDS):** Es un software o hardware que se encarga de monitorear paquetes que pasan a través de la red y es utilizado generalmente para verificar si el tráfico que pasa tiene alguna firma de un software dañino conocido.

- **Sistema de nombre de dominio (DNS):** Se encarga de la resolución de nombres de dominios en direcciones IP.

- ***Sniffear:*** Acción que involucra la captura de paquetes de una red.

- ***Sniffer:*** Software encargado de capturar paquetes en una red.

- **Spyware:** Software malicioso cuya finalidad es intervenir o monitorear el uso de una computadora sin la autorización del usuario.
- ***Spyware:*** Software que recopila información critica de un computador y las actividades realizadas en él.

- **Tiempo De Vida (TTL):** Es un campo en el protocolo IP el cual sirve para indicar por cuantos nodos puede pasar un paquete antes de ser descartado por la red (evitar bucles) o ser devuelto a su origen.

- **UTM (*Unified Threat Management*):** Dispositivo hardware que comprende integración de diferentes servicios de seguridad.

- ***VPN (Virtual Private Network):*** Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo internet.

- ***Watchguard:*** Compañía que vende productos de seguridad informáticos.

- **Zona Desmilitarizada (DMZ)**: Un área de red que se encuentra entre la red interna de una organización y una red externa, generalmente Internet. La mayoría de los servidores públicos, tales como Web y FTP residen en esta zona.

Referencias Bibliográficas

Bibliografia documental

[1] Graves, K. (2007). *Official Certified Ethical Hacker Review Guide.* Indianapolis, Indiana: Willey Publishing, Inc.

[2] Dhanjani, N. (2004). *claves hackers en Linux y Unix.* Aravaca Madrid: McGraw-Hill.

[3]Horton, M., & Mugge, C. (2004). *Claves Hackers.* Aravaca Madrid: McGraw-Hill.

[4] Tipton, H. F., & Henry, K. (2007). *Oficial Guide to the CISSP CBK (ISC)2.* boca Raton, Fl: Auerbach.

[5] EC-Council (2009). EC-Council Certified Security Analyst V4. Albuquerque, NM: EC-Council.

Consultas en internet

[6](http://www.netfilter.org/), Agosto 2009

[7](http://www.mcafee.com/mx/enterprise/products/network_security/utm_*firewa ll*.html), Agosto 2009

[8](http://www.sonicwall.com/mx/UTM_*Firewall*_VPN.html), Junio 2009

[9](http://www.*Watchguard*.com/products/utm.asp), Julio 2009

[10](http://www.audea.com/servicios/tecnologias-seguridad/ctutm/), Agosto 2009

[11] (http://www.miercom.com), Septiembre 2009

[12] (http://www.watchguard.com), Agosto 2009

[13](http://www.reuters.com/article/pressRelease/idUS153726+23-Feb-2009+PRN20090223), Junio 2009

[14] (http://www.nessus.org), Agosto 2009

Anexos

A. Política de Uso de Internet

1. Objetivo

Este documento describe las políticas bajo las cuales personal interno, podrán hacer uso del servicio de Internet.

2. Alcance

Esta política se aplica a todos los empleados y personas que trabajan dentro de la institución que utilicen el servicio de Internet.

3. Política

3.1. Del Uso Prohibido

El servicio de Internet no debe de ser usado para fines personales, y queda estrictamente prohibido utilizar cualquier aplicación Peer-to-Peer, descargadores de música, videos, juegos, software, escuchar música en línea, visitar paginas para adultos y/o sexo explicito, ya que este tipo de prácticas tienen el riesgo de contener virus, spyware y otro tipo de aplicaciones, mismas que reducen el rendimiento de los aplicativos y servicio de Internet.

3.2. Del Uso Personal

Usar el servicio de Internet en accesos permitidos de forma moderada.

3.3. Monitoreo

El personal de la institución, no tendrá ninguna expectativa de privacidad en el contenido de las páginas visitadas; La Gerencia de Tecnología es el área encargada de la administración de este servicio y tendrá la potestad para monitorear y controlar el tráfico de con el fin de evitar riesgos para los usuarios.

4. Aplicación

Opción 1. Cualquier empleado que viole estas políticas será sancionado de acuerdo a los criterios establecidos por el comité de seguridad.

Opción 2 Al personal de la institución que viole estas políticas se le hará una notificación y se hará acreedor a la suspensión del servicio por una semana.

Al personal de la institución que sea recurrente en este tipo de prácticas le será suspendido el servicio de forma permanente.

5. Definiciones

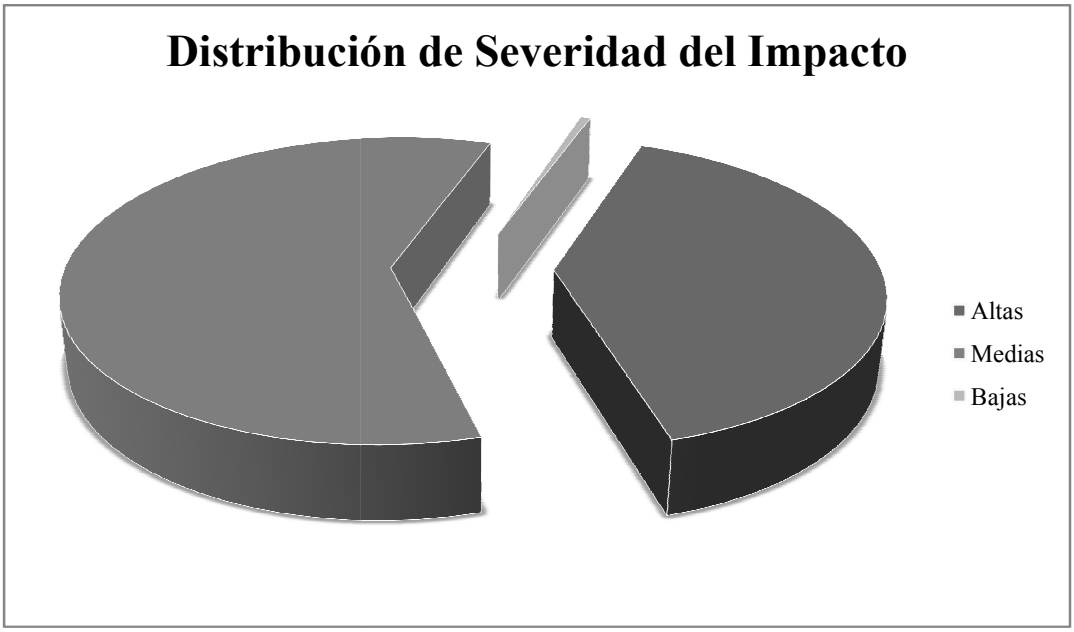
Término	Definición
Peer-to-Peer	Se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red
Virus	Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario
Spyware	Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento

6. Control de Cambios

Fecha	Revisión	Páginas Afectadas	Responsable de Cambio	Observaciones

B. Análisis de vulnerabilidades anterior a la implementación del UTM

Policy Name :	Complete Pen-test Assessment
Policy Type :	Audit & Pen-Test Assessment
Number of Vulnerabilities Found :	4229
High Level Vulnerabilities	4025
Medium Level Vulnerabilities	181
Low Level Vulnerabilities	0
Security Warnings	23



C. Análisis de vulnerabilidades actuales de la institución

Policy Name :	Complete Pen-test Assessment
Policy Type :	Audit & Pen-Test Assessment
Number of Vulnerabilities Found :	25
High Level Vulnerabilities	1
Medium Level Vulnerabilities	1
Low Level Vulnerabilities	0
Security Warnings	23