ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"SISTEMA DE PROTECCIÓN INTEGRAL APLICABLE A REDES DE ÁREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO"

REALIZADO POR:

GRACE KATHERINE ARTEAGA DELGADO
PABLO ALBERTO ATIAGA GALEAS

SANGOLQUÍ-ECUADOR
2013

Certificado de tutoría

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES

CERTIFICADO

Ing. Carlos Romero
Ing. Fabián Sáenz

CERTIFICAN

Que el trabajo titulado “SISTEMA DE PROTECCIÓN INTEGRAL APLICABLE A REDES DE ÁREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO”, realizado por Grace Katherine Arteaga Delgado y Pablo Alberto Atiaga Galeas, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Sangolquí, 10 de Septiembre de 2013

Ing. Carlos Romero	Ing. Fabián Sáenz
DIRECTOR	CODIRECTOR

Declaración de Responsabilidad

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

GRACE KATHERINE ARTEAGA DELGADO

DECLARO QUE:

El proyecto de grado denominado “SISTEMA DE PROTECCIÓN INTEGRAL APLICABLE A REDES DE ÁREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el documento, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 10 de Septiembre del 2013

_____

Grace Katherine Arteaga Delgado

Declaración de Responsabilidad

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

PABLO ALBERTO ATIAGA GALEAS

DECLARO QUE:

El proyecto de grado denominado “SISTEMA DE PROTECCIÓN INTEGRAL APLICABLE A REDES DE ÁREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el documento, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 10 de Septiembre del 2013

_____

Pablo Alberto Atiaga Galeas

Autorización de publicación

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Grace Katherine Arteaga Delgado

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo "SISTEMA DE PROTECCIÓN INTEGRAL APLICABLE A REDES DE ÁREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría

Sangolquí, 10 de Septiembre de 2013

_____

Grace Katherine Arteaga Delgado

Autorización de publicación

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Pablo Alberto Atiaga Galeas

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo “SISTEMA DE PROTECCIÓN INTEGRAL APLICABLE A REDES DE ÁREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría

Sangolquí, 10 de Septiembre de 2013

_____

Pablo Alberto Atiaga Galeas

DEDICATORIA

Dedico este proyecto de tesis a mis padres, por creer siempre en mí, y por hacer todo lo que estuvo en sus manos para hacer realidad este sueño, por guiarme para ser mejor cada día entregándome el mejor modelo a seguir.

A mis angelitos que son la inspiración que me impulsa a superarme día a día.

Y esa persona especial que ha estado a mi lado en todo momento, brindándome su amor y apoyándome para salir adelante aun cuando todo parecía perdido. Gracias por todo.

Grace Katherine Arteaga Delgado

DEDICATORIA

El presente trabajo lo quiero dedicar en primer lugar a mis padres y a mis hermanos, que siempre me han brindado su apoyo y enseñanzas para cumplir todas las metas propuestas personal y profesionalmente, protegiéndome y haciendo todos los sacrificios necesarios.

A mis amigos que siempre han mostrado la mejor voluntad, estando a mi lado en las diferentes etapas del camino para llegar a esta meta.

Pablo Alberto Atiaga Galeas

AGRADECIMIENTO

Agradezco a Dios por bendecirme e iluminar mi camino, gracias a Él he llegado hasta aquí.

A mis padres, por estar a mi lado en todo momento, y por apoyarme en cada etapa de mi vida brindándome su amor incondicional.

A mis hermanas por ser mis amigas, ayudándome y ofreciéndome una mano sin importar la circunstancia.

A mi familia que aunque se encuentre lejos siempre se preocupa por mí.

A mi compañero de tesis, gracias por ser un gran amigo y por su ayuda incondicional y desinteresada.

Y a la empresa e-Govsolutions por permitirnos desarrollar nuestro proyecto de Tesis en sus instalaciones, y a su propietario por ser una persona siempre abierta a transmitir sus conocimientos de manera desprendida.

Grace Katherine Arteaga Delgado

AGRADECIMIENTO

Quiero agradecer a todas las personas que han sido parte de mi vida en algún momento de ella, en especial a mi familia, a mis abuelos, padres, hermanos y sobrinos que siempre han estado a mi lado y me han enseñado el verdadero valor de vida.

A mis amigos que llegaron en diferentes momentos y se han quedado para compartir momentos imborrables.

A mis compañeros que han tenido la buena voluntad de ayudar independientemente de las circunstancias.

Y un agradecimiento especial a la empresa e-GovSolutions que nos apoyó y brindo todas las facilidades para la ejecución del proyecto

Pablo Alberto Atiaga Galeas

RESUMEN

El proyecto describe la implementación de un sistema de seguridad integral simulado dentro de la red de e-GovSolutions S.A. aplicable a una red de área metropolitana o red de área de campus. Se analizó las diferentes tendencias de seguridad de la información empresarial, atacantes y códigos maliciosos avanzados para posteriormente realizar un estudio de las posibles vulnerabilidades que podían existir en los diferentes componentes de la red como son enlaces, servidores, dispositivos finales y factor humano. Se combinaron recomendaciones, estándares, políticas y herramientas comerciales con herramientas de código abierto, que permitirán proveer seguridad en diferentes niveles de la red de manera que no existan huecos de seguridad y permita una protección en tiempo real para ataques conocidos que aprovechan vulnerabilidades del sistema, además de proteger contra ataques de malware sofisticados tales como ataques de día cero, malware polimórficos e ingeniería social. Para probar el sistema de seguridad integral se realizarán varias pruebas incluyendo pruebas de penetración y propagación de diferentes tipos de códigos maliciosos con diferentes vectores de ataques.

Palabras Claves:

- Malware
- Ataques Cibernéticos
- Red de Área Metropolitana, MAN
- Red de Área de Campus, CAN

INDICE DE CONTENIDOS

CAPÍTULO I

PRESENTACIÓN

CAPÍTULO II

SEGURIDAD PERIMETRAL, INTERNA Y EN APLICACIONES WEB

CAPÍTULO III

ANÁLISIS Y CORRECCIÓN DE VULNERABILIDADES

CAPÍTULO IV

SEGURIDAD EN ESTACIONES DE TRABAJO Y FACTOR HUMANO

CAPÍTULO V

EVALUACIÓN DEL SISTEMA INTEGRAL DE SEGURIDAD PROPUESTO

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

INDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

INDICE DE TABLAS

GLOSARIO

Malware.- software usado o creado por atacantes para interrumpir el funcionamiento de un equipo, obtener información sensible o ganar acceso a un sistema informático privado.

Seguridad de la información.- es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

Seguridad informática.- es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta

Tecnologías de Información (IT).- Es el conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizada de la información.

Red de área metropolitana (MAN).- Es una red informática que abarca una ciudad o un campus grande. Por lo general interconecta una seria de redes locales (LAN) utilizando tecnología “backbone” de alta capacidad

Red de área metropolitana privada.- Es una red de área metropolitana aplicable a organizaciones únicamente para uso interno, estas no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales.

Red de área de campus (CAN).- es una red informática que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar.

SISTEMA DE PROTECCIÓN INTEGRAL APLICABLE A REDES DE ÁREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO

El proyecto pretende estructurar un sistema de seguridad integral aplicable para redes de área metropolitana y redes de área de campus.

Se va a combinar herramientas comerciales con herramientas “open source” que permitirá proveer seguridad en diferentes niveles de la red de manera que no exista huecos de seguridad y permita una protección en tiempo real para ataques conocidos que aprovechan vulnerabilidades del sistema además de proteger contra ataques de malware sofisticados tales como ataques de día cero, malware polimórficos e ingeniería social.

El sistema integral se montará sobre diferentes servidores virtualizados y físicos, y se evaluará dentro de la red empresarial de EGOVERMENT SOLUTIONS S.A. Las pruebas de intrusiones y simulación de ataques se los realizará a nivel de un CEH (Certified Ethical Hacker)

Se ha dividido el estudio en cinco principales áreas, las cuales se van a citar a continuación:

- Seguridad perimetral.
- Seguridad en aplicaciones web
- Análisis de amenazas basado en comportamiento
- Análisis y corrección de vulnerabilidades.
- Seguridad en el usuario final y factor humano

En el área de seguridad perimetral se analizará la importancia, configuración, modo de operación, funcionamiento interno, ventajas, desventajas y alcance de tres herramientas; un analizador de malware perimetral (FireEye), un firewall de siguiente generación (Palo Alto Networks) y un sistema de prevención de intrusos (Snort).

En el área de seguridad en aplicaciones web se analizará la importancia y los huecos de seguridad existentes en las aplicaciones web además de explicar la configuración, modo de operación, funcionamiento interno, ventajas, desventajas y alcance de un firewall de aplicaciones web (ModSecurity).

En el área de análisis de amenazas basado en comportamiento se analizará la importancia, configuración, modo de operación, funcionamiento interno, ventajas, desventajas y alcance de dos herramientas; un analizador de botnets, virus y spyware basado en comportamiento (BotHunter) y un honeypot (KFsensor).

En el área de análisis y corrección de vulnerabilidades se explicará la importancia de tener un sistema poco vulnerable y la realización de hardening de servidores para diferentes sistemas operativos existentes, se explicará cómo realizar un análisis de vulnerabilidades en tres puntos esenciales: general (Qualys), aplicaciones web (Qualys WAS) y usuarios finales (Secunia PSI) para posteriormente realizar las correcciones necesarias, además se analizará de forma teórica y práctica el modo de explotación de vulnerabilidades utilizando las siguientes herramientas backtrack, metasploit y nmap. Finalmente se explicará los fundamentos del hackeo ético.

En el área de seguridad en el usuario final se analizará la importancia, configuración, modo de operación, funcionamiento interno, ventajas, desventajas y alcance de Internet Security personal, además de la realización de hardening en sistemas operativos comerciales personales y explicación de fundamentos de la ingeniería social. Por otro lado se explicará la importancia del factor humano dentro de la prevención contra amenazas, la capacitación básica que debe tener y las políticas de seguridad de la información dentro de una empresa.

Finalmente se establecerá un procedimiento para el análisis de malware utilizando todas las herramientas antes mencionadas y sitios de actualidad de seguridad informática, además de crear un plan de contingencia en caso de detectar un equipo infectado dentro de la red.

CAPÍTULO I

PRESENTACIÓN

1.1. ANTECEDENTES

Malware es un software o código malicioso que por lo general daña, deshabilita, toma control o roba información de un sistema computarizado. ([1] Wikipedia, 2013)

Hoy en día los threats son más desarrollados que nunca y todos los tipos de empresas han sido atacadas exitosamente, obteniendo cualquier tipo de información ([1] Wikipedia, 2013)

Los hackers en la actualidad son más peligrosos y sofisticados. La orientación de los mismos ha cambiado en los últimos años. En sus inicios el objetivo de un malware consistía en molestar o dañar cualquier dispositivo de una estación de trabajo, y posteriormente se volvió una herramienta perfecta para obtener cualquier tipo de información valiosa y cada vez existen más tipos de datos que pueden ser aprovechados para la inserción en la red. ([2] Miller, 2012)

Actualmente en el mercado no existe una solución holística que provea seguridad y garantía contra ataques sofisticados sobretodo hablando de ataques de día cero, ingeniería social o ataques polimórficos. Los equipos utilizados actualmente en temas de seguridad tales como firewalls, IPS, antivirus han demostrado no ser suficientes para los diferentes tipos de ataques y ser obsoletos en ataques sofisticados y especialmente dirigidos.

En el ámbito de redes de área metropolitana o redes de área de campus resulta necesario encontrar un equilibrio entre seguridad y rendimiento, estableciendo una infraestructura sólida y políticas que reduzcan el riesgo al mínimo. Es de conocimiento público que este tipo de redes contienen activos de información muy valiosos además de permitir accesos a diferentes enlaces a través de la nube, esto genera más vulnerabilidades ante cualquier individuo que tenga acceso a internet por lo que es extremadamente necesario tener seguridades avanzadas que permitan bloquear accesos no permitidos, robo de información o inclusión de malware.

1.2. JUSTIFICACIÓN E IMPORTANCIA

Los ataques cibernéticos han mostrado un gran crecimiento en la actualidad, además de ser dirigidos y mucho más avanzados que nunca. Al ser dirigidos, todo tipo de empresas se han visto afectadas en busca de información o intentando causar daño económico o moral.

Es fundamental entender que en el siglo actual, la información es el activo más valioso dentro de una empresa, de esta manera se debe proteger accesos no autorizados a información personal (usuarios, contraseñas, números de tarjetas de crédito, identificaciones) e información confidencial corporativa (correos, conversaciones, archivos confidenciales).

En la gran cantidad de empresas, existen ya políticas de seguridad de la información que deben ser complementadas con sistemas avanzados para la protección de la red.

En la actualidad el software inseguro debilita cada vez más la infraestructura de las redes. Día a día las instalaciones son cada vez más complejas, y con esto se dificulta la seguridad de las aplicaciones de manera alarmante. La cantidad de información transmitida por la red no permite darse el lujo de tolerar problemas de seguridad que podrían ser controlados.

Hoy en día existen organizaciones políticas y sociales que han encontrado dentro del hackeo una herramienta magnífica para vulnerar seguridades y demostrar el potencial dentro de la sociedad actual por lo que todos los años se han realizado diversos congresos para encontrar soluciones óptimas para una protección real.

“Los ataques cibernéticos son el cuarto riesgo global en términos de probabilidad, superando a una crisis por abastecimiento de agua” ([3] Forum, 2012)

Es la primera vez en la historia que los ataques cibernéticos son tema principal no solo de congresos tecnológicos sino también de congresos económicos, políticos y sociales.

El entorno empresarial comprende varios huecos de seguridad que deben ser protegidos y la única forma de conseguirlo es realizando un estudio completo del funcionamiento de malware enfocándose en los puntos críticos pero no en tipos específicos de ataques, ya que el mundo del malware va a seguir innovando y hay que lograr estar un paso delante de los atacantes.

1.3. OBJETIVOS

1.3.1. General

- Diseñar un sistema integral de seguridad aplicable para una red de área Metropolitana y una red de Campus que comprenda seguridad interna, perimetral y en aplicaciones WEB de manera que sea demostrable mediante la generación de ataques.

1.3.2. Específicos

- Realizar una explicación de los conceptos más importantes para entender la situación actual de la seguridad en tecnologías de la información estableciendo la topología de red simulada a ser utilizada.

- Establecer el correcto funcionamiento de herramientas basadas en comportamiento y firmas orientado a seguridad perimetral, interna y en aplicaciones web.
- Analizar la explotación y corrección de vulnerabilidades.
- Establecer políticas y procedimientos que permitan asegurar un correcto comportamiento del factor humano dentro de la seguridad en tecnologías de la información.
- Evaluar el sistema integral de seguridad propuesto dentro de la red empresarial de EGOVERMENT SOLUTIONS S.A. y el procedimiento en caso de hallar una estación de trabajo o servidor infectado.
- Determinar las posibles soluciones, ventajas y desventajas a partir de los resultados obtenidos mediante las pruebas y simulaciones realizadas para futuros trabajos de investigación.

1.4. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

Dentro de la época actual, la información se ha convertido en el activo más importante tanto en el ámbito personal como empresarial y esta información cada vez se sigue almacenando en dispositivos informáticos.

Prueba de esto es el cambio de mentalidad que ha transcendido en un cambio de enfoque por parte de los atacantes informáticos

En la década de los ochenta se empieza a dar a conocer el término virus informático, que por lo general utilizaban los discos flexibles (floppy disks) para su propagación. A mediados de la década de los noventa los atacantes se enfocaron en el correo electrónico ya que el internet empezaba a demostrar todo su potencial.

Los correos electrónicos eran ideales para la propagación de virus, debido a las siguientes características:

- Una gran cantidad de personas tiene una cuenta
- Enviar un correo electrónico es gratuito
- Es fácil adjuntar scripts o archivos maliciosos

- Ideal para ataques de ingeniería social
- Muy pocas seguridades

A partir del año 2000 el virus informático toma una importante popularidad, las características comunes de este tipo de malware eran las siguientes: ([4] FireEye, Inc., 2013)

- Propagación rápida
- Infectar cientos de miles de sistemas
- Hacerse notar
- Dañar y colisionar sistemas informáticos

Con estas características el atacante buscaba fama y demostrar sus capacidades. Finalmente a partir del 2005, cuando el internet y los dispositivos informáticos de almacenamiento masivo entraron en un crecimiento exponencial, los atacantes empiezan a redireccionar su enfoque hacia la sustracción de información y con esto llegar a obtener inimaginables cifras de dinero. ([4] FireEye, Inc., 2013)

De esta forma la cantidad de amenazas en los medios informáticos empezó a crecer alarmantemente y con esto la complejidad y riesgo de los mismos. En la actualidad nos encontramos con millones de casos de cybercrimen, cyberbullying y cyberespionaje (Figura 1.1.)

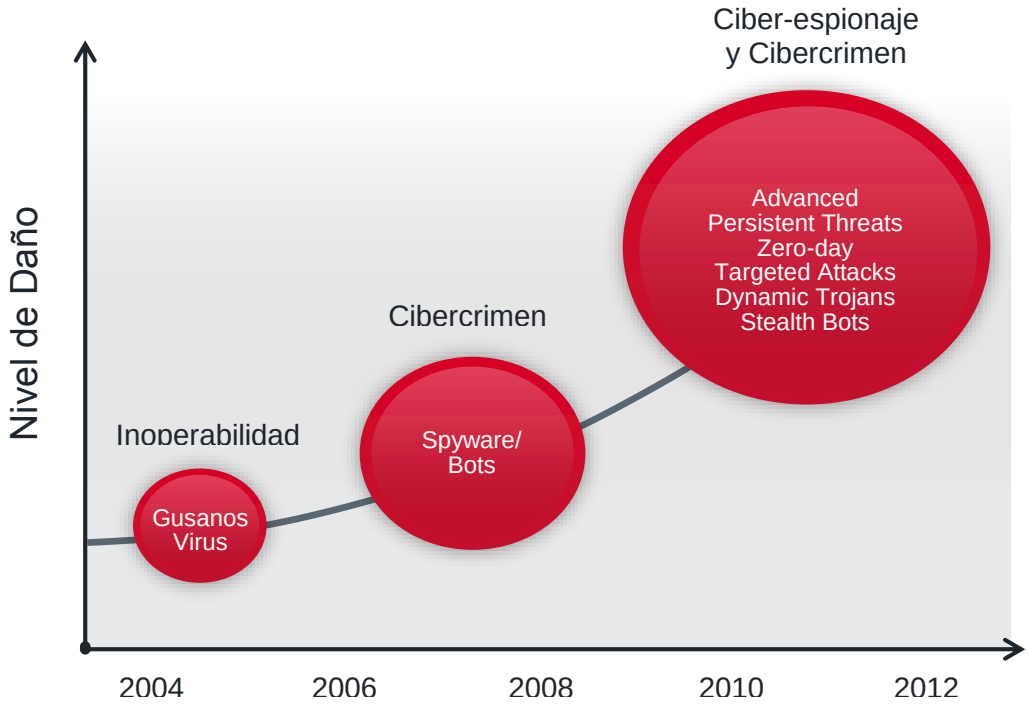


Figura. 1.1. Evolución del malware ([4] FireEye, Inc., 2013)

Personas de todas las clases sociales, de todos los países han sido atacadas por la distribución de diferente información personal, de esta misma manera empresas de todos los tamaños y sectores económicos han sido vulneradas y afectadas en cifras que superan los miles de millones de dólares.

Evidentemente, la necesidad de proteger la información ha atraído la atención de organizaciones gubernamentales, sociales, monetarias y obviamente informáticas. Prueba de ello es el reporte de Riesgos Globales 2012 realizado por el Foro Económico Mundial (WEF). Este reporte es basado en un análisis de 469 expertos de la industria, gobierno, educación y sociedad civil que examinan 50 riesgos globales a través de cinco categorías: ([3] Forum, 2012)

- Económico
- Ambiental
- Geopolítico
- Social
- Tecnológico

En dicho reporte, los ataques cibernéticos son considerados como el cuarto riesgo global en términos de probabilidad (ver Figura. 1.2. y 1.3.) y como el mayor riesgo tecnológico en términos de probabilidad y el segundo en términos de impacto (ver Figura. 1.4.) ([3] Forum, 2012)

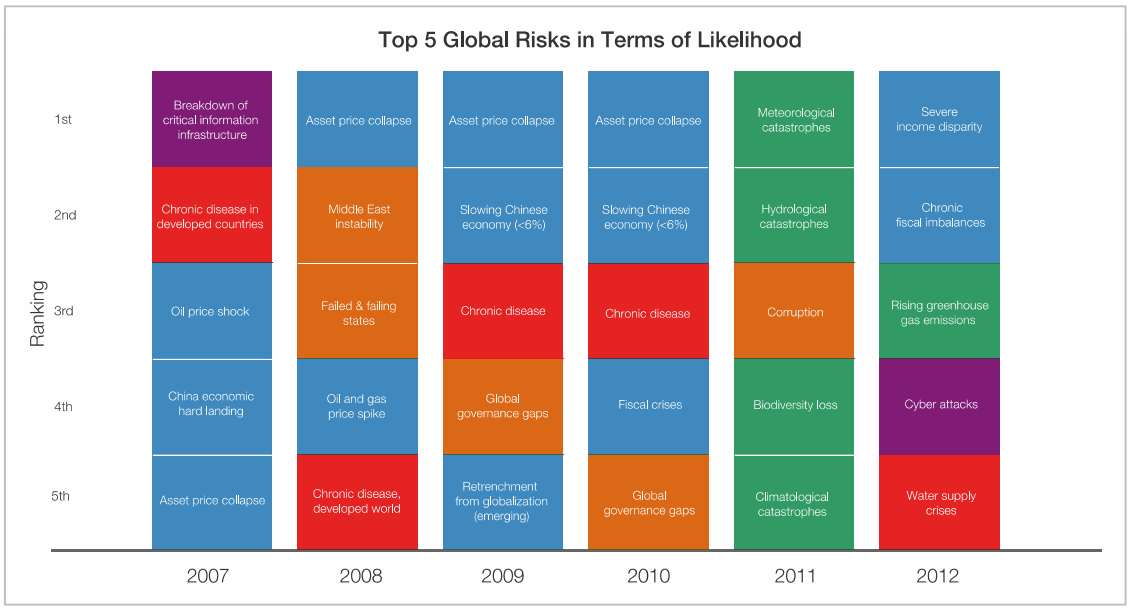


Figura. 1.2. Top 5 de riesgos globales en términos de calidad de vida en el 2012 ([3] Forum, 2012)

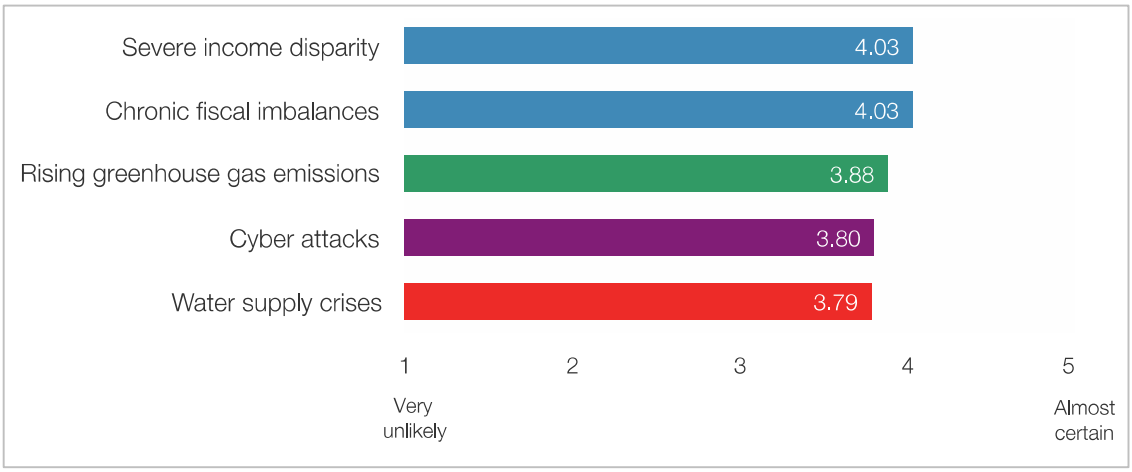


Figura. 1.3. Top 5 de riesgos globales en términos de calidad de vida en el 2012 ([3] Forum, 2012)

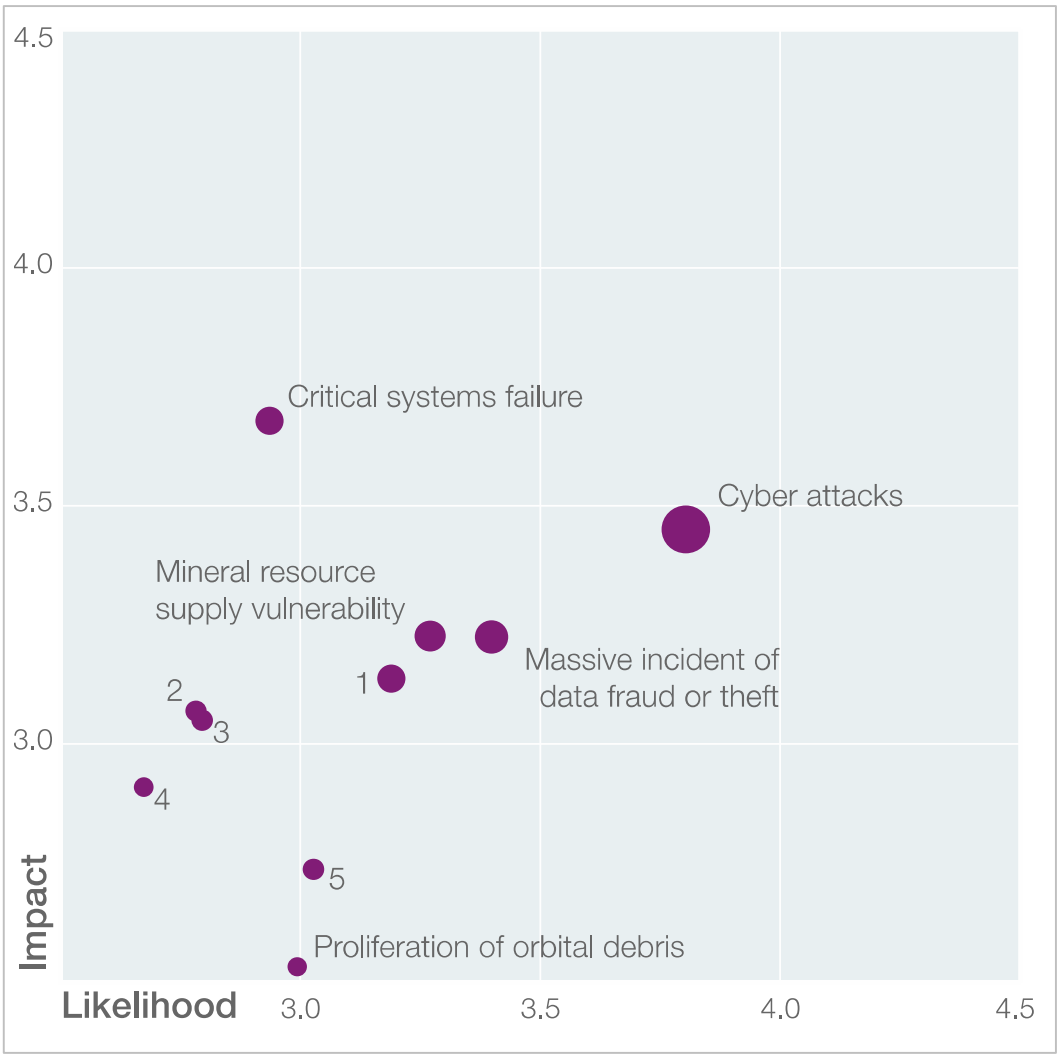


Figura. 1.4. Riesgos globales diagramados en términos de impacto y calidad de vida ([3] Forum, 2012)

1.5. FUNCIONAMIENTO DE UN MALWARE

Cada tipo de malware tiene su forma específica de funcionamiento, la cual se explicará en el capítulo siguiente. Sin embargo si es posible explicar el

funcionamiento del malware de forma general dependiendo en la etapa del ataque se lo utilice. Es posible dividir los ataques en tres etapas principales:

- Reconocimiento
- Intrusión
- Explotación

En la primera fase, de reconocimiento, no es necesario utilizar ningún de código malicioso. En esta etapa se utilizan técnicas de footprinting cuyo objetivo es estudiar el objetivo y conocer cuáles pueden ser las vulnerabilidades dentro del entorno, esto puede comprender software, hardware o incluso factor humano y así encontrar por lo menos una ventana que nos permita llegar al objetivo.

La segunda fase, de intrusión, consiste en la explotación de vulnerabilidades de sistemas o humanas con el objetivo de lograr ingresar a la red. En el caso de sistemas se pueden encontrar vulnerabilidades a nivel de sistema operativo, servicios o elementos de seguridad.

La tercera fase, de explotación, consiste básicamente en cumplir el objetivo, este puede ser la sustracción de información, comprometimiento del sistema para un ataque futuro o corrupción de equipos/servidores (como son los ataques de denegación de servicio). En el caso de sustracción de información se lo puede realizar con códigos previamente programados que son capaces de buscar y transmitir la información automáticamente o con códigos maliciosos que están diseñados para permitir al atacante tomar el control del dispositivo del usuario, llamado código de comando y control (C & C). El código de C & C realiza llamados denominados callbacks a uno o varios servidores de comando y control. Este código también puede comprometer otros activos en la red de la empresa para extender el alcance del ataque.

Un claro ejemplo de este tipo de ataque de da cuando se tiene un sitio web legítimo pero vulnerable, esto proporciona a los atacantes la oportunidad de publicar un anuncio o link falso, el cual podría contener un exploit de día cero de manera que no sea detectado por ningún sistema de prevención de intrusos.

Mediante este exploit es posible provocar que el navegador descargue un binario de malware en un segundo plano. Una vez que el binario malicioso es ejecutado, un proceso se carga en la máquina de la víctima, y el atacante empieza a realizar callbacks lo cual indica que está listo para ser controlado remotamente por el servidor de C&C para finalmente buscar más víctimas y así incrementar la rentabilidad del ataque (Figura 1.5.). ([4] FireEye, Inc., 2013)

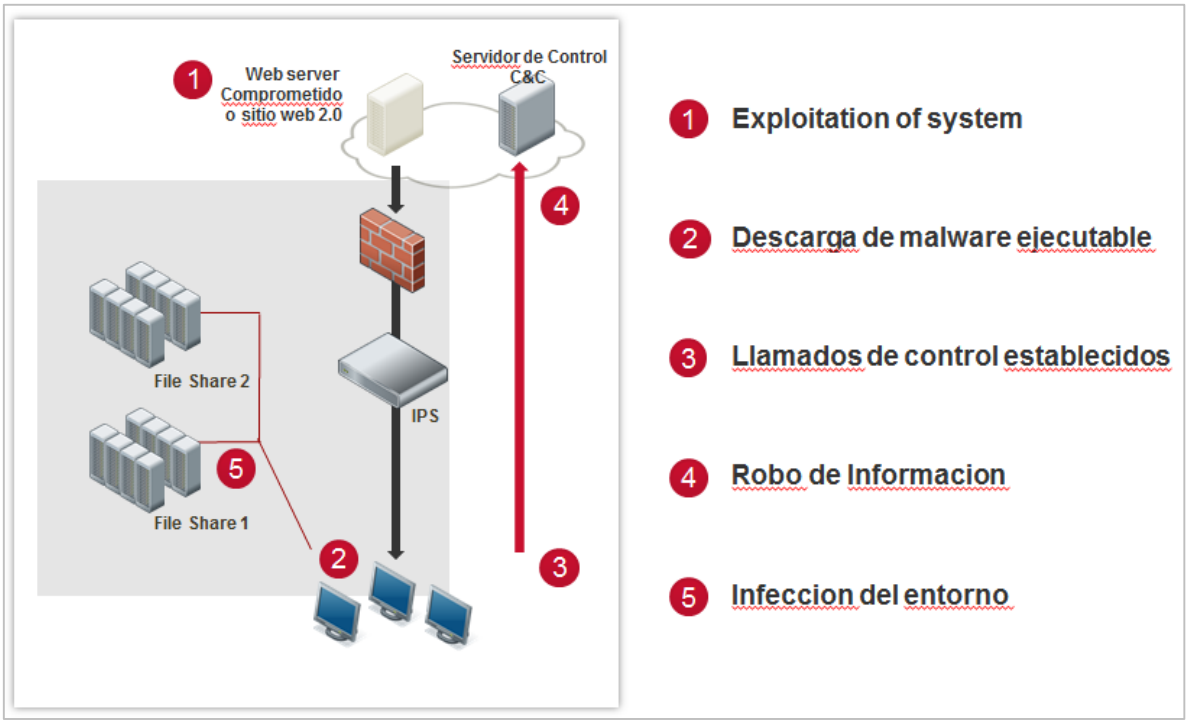


Figura. 1.5. Ataque mediante código de comando y control ([4] FireEye, Inc., 2013)

1.6. TIPOS DE MALWARE

Adware

Es un programa malicioso que se instala en la máquina víctima sin que esta lo note, su función es mostrar o descargar anuncios publicitarios en la pantalla del usuario.

Cuando un adware ingresa en el sistema, la víctima empieza a visualizar anuncios publicitarios de manera inesperada, los cuales suelen ser mostrados como ventanas emergentes del explorador.

El adware en si no produce daños en el sistema, pero este afecta al usuario ya que se convierte en una molestia al abrir automáticamente ventanas emergentes, además el adware disminuye el rendimiento del equipo, ya que consume recursos como procesador, memoria y ancho de banda.

Muchas empresas utilizan el adware como una manera de ofrecer sus productos, incluyendo ventanas emergentes no deseadas en sus versiones gratuitas y ofreciendo la versión pagada del mismo producto sin el fastidioso adware.

Generalmente trabaja en conjunto con algún spyware el cual recolecta información para saber que publicidad mostrar a cada usuario.

Hoax

Son correos electrónicos los cuales se distribuyen a través de cadenas, cuyo objetivo es confundir a los usuarios, haciéndoles creer que algo falso es real, esta amenaza no tiene como fin conseguir dinero.

Los contenidos de este tipo de correos pueden ser muy variados, entre los cuales encontramos, alertas falsas de virus, historias solidarias sobre gente enferma, secretos para hacerse millonario entre otras.

Entre las principales características de los hoax tenemos:

- Tienen una redacción poco profesional.
- Invitan al usuario a reenviar el correo a sus contactos.
- El remitente normalmente es un contacto conocido, que ha creído en el contenido de la cadena.
- Algunas veces indican un beneficio o donación por cada vez que se reenvíe el mensaje.

Como su objetivo no es lucrativo, las principales motivaciones de este tipo de correos son:

- Generar miedo, inseguridad y duda en las víctimas.
- Armar bases de datos con las direcciones de correo electrónico de quienes reciben la cadena.
- Aumentar el ego de la persona que creo el hoax al ver que su correo está siendo difundido por la red.

Aunque sus fines no sean extremadamente dañinos, no se debe subestimar este tipo de amenazas, ya que se han presentado casos en que el correo pide al receptor eliminar ciertos archivos del sistema. Por lo cual vale la pena asegurarse que los correos no se traten de hoax ingresando a bases de datos confiable que identifican este tipo de amenazas.

Ransomware

Es un código malicioso que se encarga de cifrar la información de la víctima, la cual deberá pagar al atacante la cantidad de dinero que éste disponga para que le entregue un conjunto de instrucciones y de esta manera el usuario pueda recuperar sus archivos.

En sus inicios los métodos de cifrado eran básicos lo cual permitía a la víctima recuperar su información sin necesidad de pagar el dinero solicitado por el atacante, sin embargo hoy en día se han desarrollado métodos de cifrado más sofisticados aumentando la complejidad de esta amenaza.

Normalmente se ataca a ciertos archivos como son procesadores de texto, hojas de cálculo o diapositivas. También son afectados correos electrónicos o imágenes que pueden ser considerados como importantes.

Scam

Se llama así a las estafas realizadas por medios tecnológicos, los medios que utiliza son similares al phishing con la diferencia de que no busca obtener datos sino obtener dinero a través del engaño.

Las principales técnicas utilizadas para realizar scam son a partir de anuncios de ganancias millonarias o por peticiones de caridad. En donde se pide a la víctima una pequeña suma de dinero ya sea como donación o para efectivizar su premio.

Aunque los scam son amenazas constantes, estos se presentan más después de desastres naturales, o cuestiones sociales que afecten de manera considerable, en estas situaciones aumenta notablemente la cantidad de correos scam en la red.

Troyanos

Son archivos que engañan al usuario fingiendo ser indefensos, pueden venir inmersos en programas o juegos, de manera que la víctima los ejecuta sin saber que el troyano en ese momento se instala en el ordenador, aparentemente realizan tareas habituales pero paralelamente están ejecutando otras tareas ocultas en el ordenador.

Los troyanos pueden ser transmitidos por medio de mensajes de correo electrónico, mensajes instantáneos o bajándolos directamente desde la Web, no necesariamente son dañinos, y estos no pueden replicarse por sí mismos, estos pueden ser utilizados para diferentes propósitos por lo que se clasifican en:

- Backdors

  También llamados de acceso remoto o puertas traseras, los cuales permiten al atacante conectarse de manera remota al equipo infectado utilizándolo para diversas actividades como envío masivo de correos, ejecución de archivos o aplicaciones maliciosas.

- Keyloggers

  Son utilizados para obtener información sensible de la víctima, instalando una herramienta en el ordenador, la cual captura las pulsaciones del teclado, robando así información como contraseñas, cuentas bancarias entre otras. Esta información es enviada al atacante el cual la puede utilizar a su conveniencia para realizar todo tipo de ataques.

- Banker

Roban información de las cuentas bancarias de los usuarios realizando un reemplazo total o parcial de la página web de la entidad bancaria o grabando el comportamiento del usuario al ingresar a la banca electrónica. Los datos recolectados son enviados al atacante mediante correo electrónico o alojándolos en sitios ftp.

- Downloader

Su principal función es descargar archivos maliciosos en el ordenador de la víctima, estos archivos se ejecutan automáticamente al reiniciar el sistema.

- Botnets

Crean redes de equipos zombis. El atacante utiliza el troyano generalmente junto con backdoors para controlar gran cantidad de ordenadores y utilizarlos como lo desee, normalmente con objetivos malignos.

- Proxy

Instala herramientas en el ordenador para que este pueda funcionar como un servidor proxy. El atacante esconde su identidad en el ordenador infectado para poder acceder a la web a través de él y así realizar ataques por internet.

- Password Stealer

Roban la información que es introducida en los formularios de las páginas web, son bastante similares a los keyloggers ya que roban información de todo tipo para utilizarla según su conveniencia.

- Dialer

Crean conexiones telefónicas en el ordenador infectado, la víctima puede ver de manera trasparente como se realizan llamadas de alto costo a sitios principalmente relacionados con contenido para adultos, en este caso el ordenador no sufre ningún daño únicamente el usuario se ve afectado económicamente.

Botnet

Los malware de tipo bot son aquellos que están diseñados para armar redes de botnets, es una de las principales amenazas que se dan en la actualidad.

Un botnet es una red de equipos que se encuentran infectados, los cuales son controlados por un atacante el cual manipula cada uno de los equipos para que trabajen de forma conjunta, convirtiéndose en robots o también llamados zombis.

Cuando un ordenador ha sido infectado con malware de este tipo, primeramente se realiza una comunicación con el servidor de Comando & Control que es quien controla toda la red de los botnets administrando a todos los equipos infectados y ordenándoles las tareas maliciosas que decida como pueden ser envío de spam, ataques de denegación de servicio distribuido (DoS), alojamiento de archivos para sitios web maliciosos, instalación de otro malware o publicidad online.

Cuando un equipo ha sido convertido en un zombi, esto es transparente para el usuario por lo cual se observa un excesivo consumo de ancho de banda, haciendo que el sistema trabaje lentamente e incluso impidiendo su total funcionamiento.

Las redes botnet ofrecen al atacante anonimato, lo q ocasiona que sea uno de los métodos más utilizados para realizar ataques a gran escala desde todos los sistemas infectados.

Payload

Son acciones adicionales que están incluidas en virus, troyanos o gusanos, estas acciones pueden ser eliminación de datos, reemplazo del BIOS, robo de datos, etc.

El payload no necesariamente es maligno, pero puede implicar efectos dañinos para el computador infectado.

Rogue

Es un tipo de software que simula ser una aplicación anti malware, pero que en realidad hace lo contrario; instalar malware en el ordenador. Este tipo de malware se caracteriza por dar alertas llamativas al usuario, donde indica que el computador se encuentra infectado y le invita a descargar un software que indica ser la solución para la supuesta amenaza encontrada, puede trabajar de dos maneras: la primera es descargando un software que va a instalarse en el ordenador y va a realizar acciones maliciosas como son el robo de información, la segunda opción es que solicita cierta cantidad de dinero por la obtención de este software fraudulento.

En este tipo de ataque se utiliza la ingeniería social, se lo reconoce por utilizar un lenguaje informal, además de exagerar los detalles sobre las consecuencias de la supuesta amenaza e invitar al usuario a adquirir un producto.

Entre sus variantes encontramos tipos de rogue que realizan un escaneo del sistema y muestran supuestas amenazas encontradas con detalles que atemorizan al usuario y lo obligan a tratar de solucionar el problema con rapidez.

Spam

Es correo electrónico no deseado el cual es enviado de manera masiva por parte de una tercera persona. También es llamado correo basura.

Normalmente es utilizado para propagar publicidad, aunque existen casos en los que se lo utiliza para enviar códigos maliciosos. Además causan molestias al usuario al recibir mensajes no deseados en la bandeja de entrada, y consumo de gran cantidad de recursos como el ancho de banda.

La cantidad de spam que es enviado ha ido aumentando con el pasar del tiempo, anteriormente eran enviados únicamente en formato de texto, lo cual permitía crear filtros contra éstos, pero en la actualidad se comenzó a enviar correos con gráficos incluidos y contenido HTML lo que complica el filtrado de spam.

El principal método de protección son las herramientas antispam, aunque es importante que los usuarios también colaboren y no reenvíen cadenas de correo,

además en caso de enviar información a sitios desconocidos utilizar la opción copia oculta (CCO) de manera que las direcciones de correo no sean públicas y no puedan ser utilizadas por terceros.

Virus

Un virus es un programa el cual ha sido creado para producir daños en el ordenador, se caracteriza porque pretende trabajar de manera transparente para el usuario, además de que pueden reproducirse a sí mismos.

Se puede alojar en diferentes sitios como archivos ejecutables, el disco de arranque o en la memoria del ordenador que trabaja como huésped del virus.

Los daños que podría causar también son variables, pueden ir desde un molestoso mensaje en la pantalla, hasta inhabilitar completamente el sistema operativo. El virus convive con el código de un archivo existente, en el cual se inyecta el código malicioso, cuando el usuario ejecuta el archivo aparentemente normal, también se ejecuta el código del virus infectando el sistema. Otro modo de funcionamiento es que el virus renombra el archivo original reemplazando completamente el código de manera que el usuario ejecuta únicamente el código malicioso.

Una vez ejecutado se producen dos daños paralelamente, la infección en sí y la propagación para seguir infectado otros equipos. Los virus pueden ser transmitidos mediante un medio de almacenamiento como un pen drive o compartiendo archivos dentro de una red local.

Hoy en día los virus no se encuentran únicamente en archivos ejecutables, sino que han ido aumentando su capacidad al alojarse en archivos como .mp3 o .pdf, además utilizan las conexiones de alta velocidad para infectar la mayor cantidad de ordenadores en el menor tiempo posible.

Gusanos

Son un subconjunto de malware, se diferencian de los virus en que no necesitan un anfitrión para seguir vivos. Pueden reproducirse utilizando la red local o por medio de correos electrónicos.

Los gusanos no causan necesariamente un daño en el sistema, su objetivo principal es que pueda ser copiado en la mayor cantidad de equipos que le sea posible. En algunos casos transportan otros tipos de malware como troyanos o rootkits, o simplemente buscan agotar los recursos del sistema mientras se distribuyen e infectan a más ordenadores, aprovechando las vulnerabilidades que encuentran en el sistema operativo o en las aplicaciones del equipo.

Cuando intentan infectar por primera vez, utilizan la ingeniería social donde muestran mensajes atractivos al usuario, puede ser a partir de correos electrónicos con archivos adjuntos, una vez que el gusano fue descargado la propagación continúa por cuenta propia.

Tipos de gusanos

- De correo electrónico

  Los mensajes de correo electrónico son atractivos e invitan al usuario a abrirlos, en ese momento se realiza un envío automático a toda la libreta de direcciones del usuario que ha sido infectado. En este tipo de ataque se busca suplantar la identidad de la víctima con fines maliciosos, esto se conoce como spoofing.

- P2P

  Utilizan redes P2P para transmitirse e infectar ordenadores, utilizando nombres atractivos que son comúnmente utilizados, pueden ser programas crackeados, fotos o videos.

- Web

Es bastante similar a los otros tipos de gusanos en la forma de descargarse, se crean páginas web atractivas que son falsas, normalmente se combinas con técnicas de phishing que obligan a la víctima a descargarse archivos maliciosos.

Otra manera de propagarse es a través de las vulnerabilidades encontradas en las aplicaciones web, por medio de la ejecución de un script se puede descargar y ejecutar archivos maliciosos sin necesidad de que intervenga el usuario, esta técnica se conoce como Drive-By-Download en donde lo único que hace el usuario es ingresar a una URL contaminada.

- Por mensajería instantánea

Utilizan el cliente de mensajería instantánea, afectan a los más populares como son MSN y Windows Messenger. Se utilizan métodos de ingeniería social, donde se ofrece transferir un archivo con nombres llamativos para que más usuarios lo transfieran y descarguen. Cuando un usuario se encuentra infectado por este tipo de gusano, al abrir el cliente de mensajería instantánea automáticamente se envía una invitación con el archivo infectado a todos los contactos de la víctima, normalmente estos archivos son ejecutables a pesar de que en el texto de envío figuran como fotos o videos.

Phishing

Consiste en el robo de información personal de la víctima a partir de falsificación de un sitio web de confianza. Normalmente es utilizado para obtener información financiera del usuario, el cual cuando ingresa sus datos en un sitio que es supuestamente de confianza lo que hace es enviar todos sus datos directamente al atacante.

En estos ataques se recolectan contraseñas de los usuarios conocidos como Password Harvesting. Normalmente se envían mensajes de correo electrónico que simulan ser de la organización bancaria del usuario, entre las principales características encontramos:

- Utilizan nombres de organizaciones reconocidas.
- El nombre del remitente simula ser de la organización bancaria.
- El mail contiene el logo de la compañía.
- Solicita a la víctima que reingrese datos con el fin de actualizarlos aunque en realidad en este paso es donde roba toda la información.
- El mensaje incluye un enlace en donde re direcciona al usuario a otra ventana.

Una vez que el usuario ha sido redireccionado a otra página web, donde ingresará los datos anteriormente solicitados. Aunque el texto que se indica en el link sea el del sitio verdadero al momento de dar clic el usuario es dirigido a un sitio falso.

El phishing utiliza el factor miedo, para lograr que el usuario ingrese al sitio web del atacante, normalmente pone un tiempo límite ocasionando que el usuario se vea obligado a ingresar al sitio de manera precipitada.

El atacante intenta utilizar todos los componentes de la página original de manera que intenta que la página falsa sea lo más parecido posible a la página oficial para aumentar la eficacia del engaño.

Rootkit

Es una herramienta que mantiene de forma encubierta el control de una computadora, pueden ser programas o archivos que permiten que el atacante pueda tener acceso y controlar el sistema.

El rootkit no es en sí maligno, sino que permite ocultar acciones malignas, tratando de deshabilitar cualquier software de seguridad utilizado en el ordenador. Son utilizados principalmente para ocultar procesos al usuario, como inicios de sesión o uso de otros programas.

Un rootkit ataca directamente al funcionamiento de base del sistema operativo, otros rootkits atacan directamente a las aplicaciones insertando códigos maliciosos cambiando el comportamiento habitual de la aplicación.

Spyware

Son programas espías que recolectan información del usuario sin su conocimiento, principalmente se lo utiliza para conocer cuáles son los hábitos de la víctima al acceder a internet para posteriormente enviar esta información a un ente externo que controlará y manipulará esta información para beneficios propios.

Esta amenaza afecta a la privacidad de la víctima, y produciendo pequeñas alteraciones en las configuraciones del sistema, principalmente en la página de inicio o internet.

Algunos spyware poseen características que los permiten interactuar con el usuario, donde simulan ser buscadores, haciendo que los datos obtenidos por este spyware sean más confiables que los de otro spyware.

1.7. MALWARE SOFISTICADO

La seguridad de redes hoy en día está siendo forzada a avanzar a niveles superiores; las técnicas tradicionales de protección como los antivirus y los IPS son métodos que ya no son suficientes para proteger a las empresas, ya que éstas solo han encontrado la manera de mantener inmunes a los ataques conocidos, de esta manera la industria de malware está creciendo a un ritmo alarmante superando de manera significativa a las defensas tradicionales.

Los códigos maliciosos en la actualidad tienen una gran complejidad y los cybercriminales logran resultados al realizar múltiples ataques de gran complejidad. El uso de exploits de día cero son muy populares entre los hackers que intentan buscar vulnerabilidades dentro de los diferentes tipos de sistemas.

Los hackers han desarrollado de manera sigilosa, dinámica y persistente tipos de malware que pueden aprovechar vectores desconocidos. Además los ataques en la actualidad son personalizados y varían en función de los objetivos de los atacantes.

A pesar de que resulta complicado definir el malware sofisticado, ya que este tiene miles de variaciones, si podemos fijar características específicas que todos las comparten como las siguientes:

- No está limitado por el tiempo, puede durar meses o incluso años hasta ser exitoso
- Es dirigido y tiene un objetivo previo específico
- Por lo general lo realiza un grupo de expertos de por lo menos 5 años de experiencia
- Realiza un extenso estudio de la víctima
- Utiliza múltiples tipos de malware
- Es polimórfico para lograr burlar mecanismos de defensa
- En por lo menos alguna etapa utiliza un ataque de día cero o métodos avanzados de encriptación
- Busca conocer las personas que se desarrollan en el entorno de la víctima para poder hacer ataques de ingeniería social exitosos
- Protege la identidad de los atacantes

Un ejemplo de un ataque sofisticado fue el realizado a la empresa Sony en abril del 2011 con el objetivo de robar millones de cuentas relacionadas con datos personales como tarjetas de crédito que se encuentran dentro de las bases de datos relacionadas con la consola de juego PlayStation (ver Figura. 1.7.). Sin embargo después se demostró que esto solo fue una artimaña del atacante para desviar la atención, ante esto Anonymous envió una carta que entre otras cosas anunciaba que ellos nunca han estado asociados con un evento criminal. ([5] Wikipedia - PlayStation Network outage, 2013)

El 20 de abril del 2011 se publicó un artículo dentro del blog oficial de Play Station anunciando que algunas características estaban fuera de servicio donde los

clientes recibían un mensaje donde indicaba que el sistema se encontraba bajo mantenimiento. Al día siguiente la empresa seguía pidiendo paciencia a sus clientes mientras internamente continuaba investigando el ataque externo. Ese día más tarde Sony admitió que había sido víctima de un ataque cibernético ejecutado entre el 17 y el 20 de abril anunciando también que temporalmente iban a suspender la conexión a la red y empezaron a ejecutarse planes de remediación.

Tuvo que pasar más de una semana para que la red de PlayStation vuelva a funcionar, no sin antes admitir que la información personal de sus clientes estaba comprometida gracias a la intrusión externa. Posteriormente y de manera oficial publicaron que resultado del ataque se habían sustraído 12 mil números de tarjetas de crédito y 24.7 millones de cuentas y el 23 de mayo anunciaron que el ataque les había costado aproximadamente 171 millones de dólares. ([5] Wikipedia - PlayStation Network outage, 2013)

El principal sospechoso de esta acción era “Anonymous” ya que en previas ocasiones Sony había sido una de las víctimas de sus conocidos ataques de denegación de servicio y además en los servidores afectados se veía el mensaje “We are legion” asociado totalmente con esta organización (ver Figura. 1.6.) ([6] Albanesius, 2011)

Anonymous Hacked Sony's PlayStation Network! No They Didn't!

By Chloe Albanesius | May 6, 2011 06:03pm EST | 44 Comments

The debate over whether online activist group Anonymous was behind the Sony PlayStation hack continued Friday, with a group spokesman taking to the op-ed pages of *The Guardian* to deny any wrongdoing, while sources told the *Financial Times* that Anonymous members are probably behind the attack.

Sony's PlayStation Network has been offline since April 20 thanks to a sophisticated cyber attack. Earlier this week, Sony told members of Congress that one of its Sony Online Entertainment (SOE) servers contained a file called "Anonymous" with the words "We Are Legion," the group's tagline. In response, Anonymous said it has never engaged in credit card theft, and said that many of its corporate adversaries engage in activities far more ethically suspect than Anonymous.

Barrett Brown, a sometimes spokesman for Anonymous, reiterated those thoughts in his Friday op-ed. "The circumstances of this incident are highly suspicious," he wrote.

Figura. 1.6. Captura de pantalla de artículo relacionado con ataque a Sony PlayStation ([6] Albanesius, 2011)

Otro ejemplo muy divulgado fue el de "Operación Aurora", este se basó en una serie de ataques persistentes generados entre finales de 2009 e inicios del 2010 que afectó a decenas de empresas, entre las más importantes están: Yahoo, Symantec, Adobe Systems, Juniper Networks y Google. ([7] Wikipedia - Operation Aurora, 2013)

Los atacantes utilizaron principalmente un exploit de día cero para Internet Explorer y correos electrónicos dirigidos a instalar un software malicioso programado para robo de datos en las máquinas de la víctima. Estos ataques fueron muy eficaces atacando a los usuarios al hacer clic en vínculos comprometidos a través de sus cuentas de correo. ([7] Wikipedia - Operation Aurora, 2013)

1.8. TENDENCIAS EN EL ÁMBITO DE SEGURIDAD

De acuerdo al reporte comprendiendo la seguridad y los riesgos para el 2013 por Forrester, el año pasado se dieron gran cantidad de ataques cibernéticos los cuales afectaban de manera potencial a la seguridad de la organización, este era un tema realmente preocupante para los encargados del área de TI, ya que entre el año 2011 y 2012 el capital destinado para la seguridad no incrementaba en la cifra esperada. ([8] Andrew, 2012)

Para el 2013 los Especialistas en TI han visto incrementar el presupuesto que ha sido destinado para asegurar todo lo referente a tecnologías de la información, y esto se da básicamente por el creciente número de ataques y de incidentes de seguridad que las empresas están recibiendo por este medio.

Los especialistas en seguridad conocen el ritmo alarmante con el cual la tecnología va creciendo, lo cual significa que el personal ha optado por utilizar dispositivos móviles tales como tablets, teléfonos inteligentes, además se incrementó el uso de tecnología en la nube y redes sociales. Con esto las personas encargadas de la seguridad se encuentran presionadas para mejorar sus medidas de seguridad debido a la aparición de nuevas amenazas las cuales son cada vez más complejas.

Si se compara las inversiones que realizan en temas de seguridad tanto en Europa como en Norte América, los datos son bastante similares, la mayor diferencia se da en seguridad de los datos que absorbe más capital en Europa debido a la estrecha relación existente entre las leyes de privacidad y la seguridad de los datos existente en este continente, mientras que Norte América se enfocan más en las operaciones de seguridad, debido a la cantidad de ataques cibernéticos organizados. (ver Figura. 1.7.)

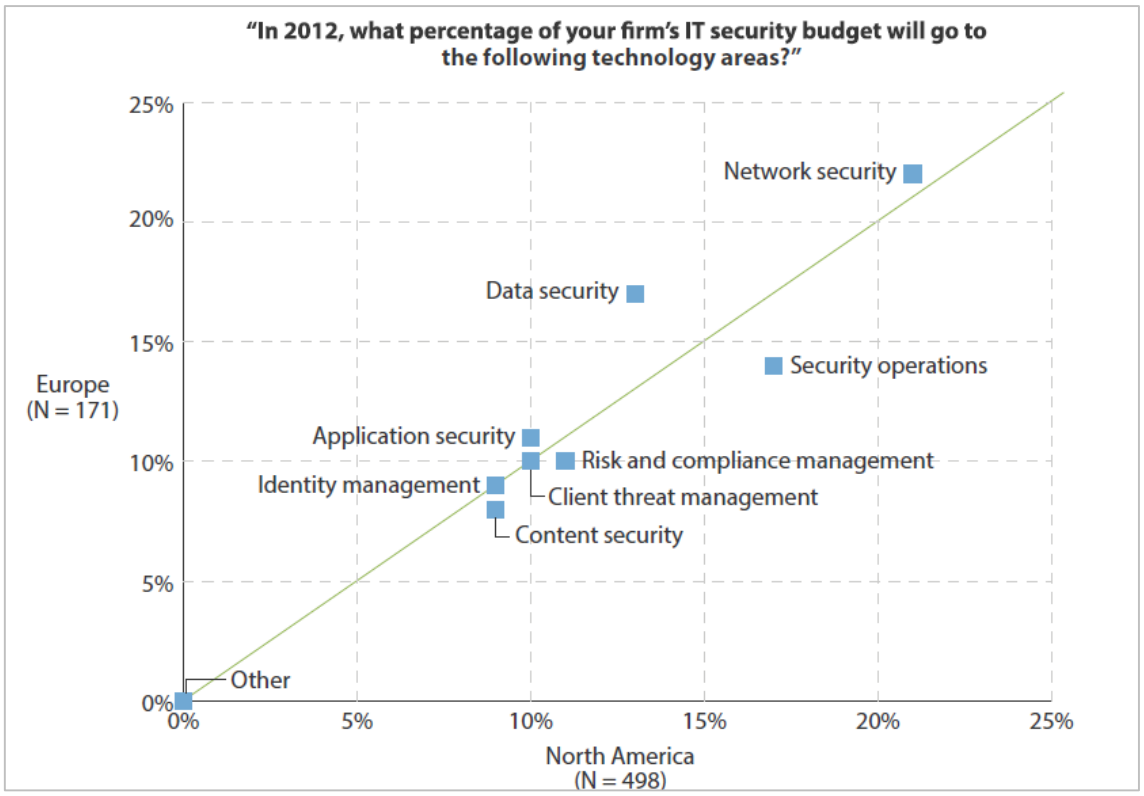


Figura. 1.7. Porcentajes del capital de seguridad IT ([8] Andrew, 2012)

Como se observa la seguridad de la red es el punto primordial de protección, las organizaciones se concentran en proteger la red ocupando aquí el mayor presupuesto destinado para tecnologías de la información.

Los entornos empresariales son cada día más hostiles, por lo que la protección contra amenazas y vulnerabilidades se convierte en una prioridad para las organizaciones quienes buscan proteger sus datos. Frente a las amenazas cada vez más avanzadas, el usuario sigue siendo uno de los mecanismos de control más valiosos, buscando que a partir de la capacitación del factor humano, se pueda tener una respuesta adecuada en momentos críticos.

Por otro lado, Gartner presenta una lista de las predicciones desde el 2013 hasta el 2017, sobre las tendencias que se seguirán en cuanto al tema de tecnologías de la información (Figura 1.8.). ([9] Rose Andrew, 2013)

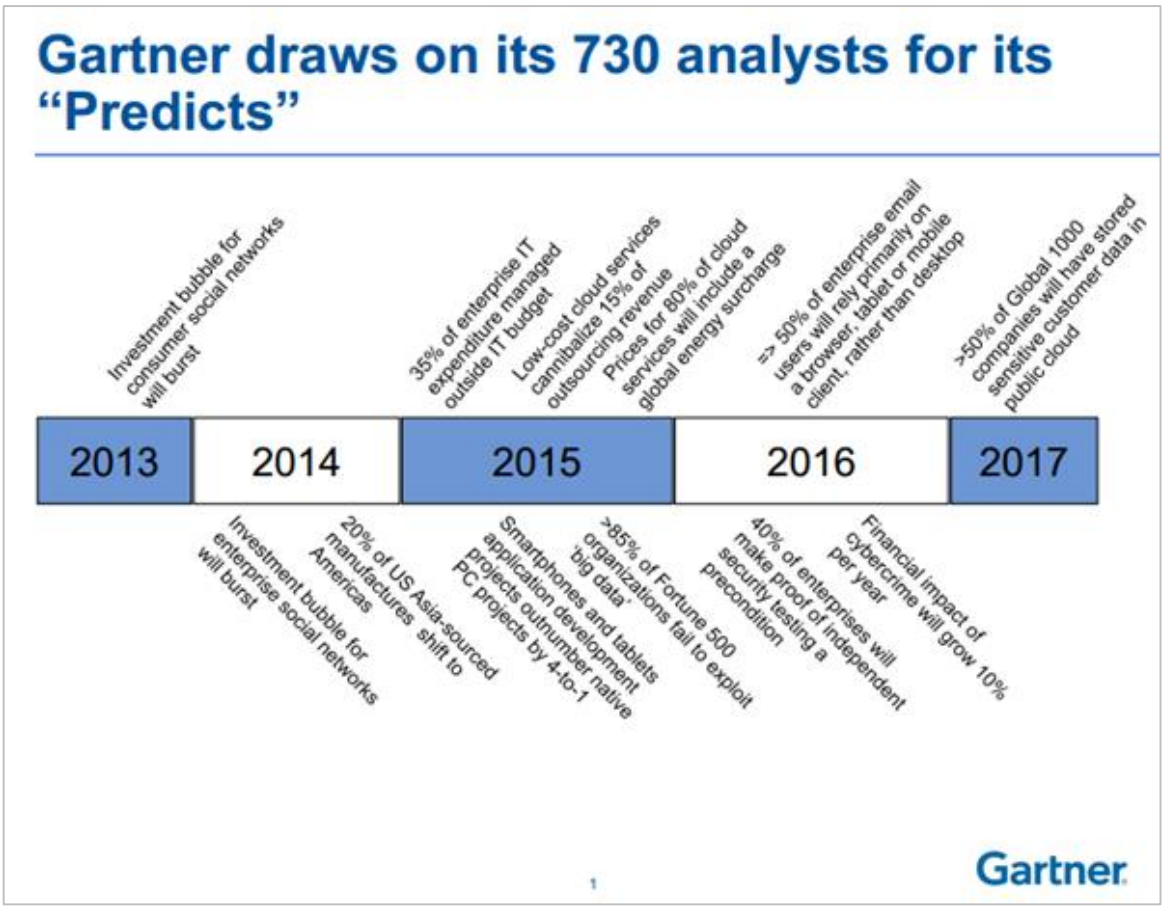


Figura. 1.8. Predicciones de Gartner ([9] Rose Andrew, 2013)

En el 2013 la inversión para redes sociales destinadas a usuarios finales está aumentando enormemente, se espera que para el año 2014 las redes sociales ya no van a estar destinadas solo para usuarios finales sino también estarán inclinadas a software para redes sociales empresariales.

Para el año 2015 se espera que el gasto general de las empresas se separe completamente de la parte de seguridad de la información, de manera que aunque la atención no se centre totalmente en la seguridad de TI, se reconozca que el crecimiento de la empresa en la parte digital es de suma importancia debido a la información que se almacena. El 80% de los servicios en la nube incluirán un recargo para los gastos de energía mundial por lo que las organizaciones se verán obligadas a migrar hacia servicios en la nube de origen externo. Crecerá el desarrollo de aplicaciones para Tablets y teléfonos inteligentes, superando al desarrollo de aplicaciones para PC en una relación de 4 a 1.

Las predicciones para el 2016 el impacto financiero del cybercrimen crecerá un 10% por año y esto es debido a la cantidad de vulnerabilidades que se descubren constantemente. Toda empresa deberá realizar pruebas independientes de seguridad antes de poder probar cualquier servicio en la nube, al realizar estas pruebas se podrán indicar que la empresa es competente para utilizar estos servicios.

Por lo menos el 50% de los usuarios de correo electrónico empresarial utilizarán los servicios de mail de tablets, teléfonos inteligentes en lugar de usar el computador de escritorio.

Para el 2017 más del 50% de las compañías a nivel mundial migrarán datos sensibles de clientes a la nube pública dejando expuesta dicha información. Se deberá elaborar un balance entre los riesgos y la agilidad de tener información en la nube, además las empresas empezarán enviando información menos sensible a la nube. ([10] Greg, 2013)

Según Gartner, analizando las tendencias empresariales para el 2013, las empresas que comúnmente no usaban IPS han optado por adquirir Firewalls de nueva generación, aunque usen únicamente las características básicas de éste.

Las empresas que utilizan Firewall e IPSs por separado los cuales trabajan principalmente en modo de detección, utilizando los requerimientos mínimos de cada equipo migran a Firewalls de siguiente Generación para integrar en este las características del IPS.

Mientras que las empresas que usan firewall junto con un IPS en modo de prevención, con un conjunto de firmas existentes y otro grupo de firmas personalizadas, migrarán a NGFW pero continuarán usando las características de IPS en modo de prevención.

La gran variedad de equipos para el control de la seguridad en las organizaciones puede confundir a los usuarios sobre la utilidad de cada herramienta. Mientras que los Firewall se dedican a controlar las aplicaciones

externas los WAFs se ubican principalmente delante de los servidores, con el fin de proteger las aplicaciones Web.

Con esto se puede concluir que la adquisición de un Firewall de Siguiente Generación, no reemplaza a un WAF, pues entre estas herramientas se complementan al realizar distintas tareas y proteger distintas secciones de la red trabajando en distintos niveles de la capa OSI.

En la cumbre anual de seguridad y riesgos, Gartner destacó que las organizaciones han gastado millones de dólares en seguridad para tecnologías de la información, entre estas herramientas encontramos Firewalls, IPS, aseguración de salida a la Web, y protección para usuarios finales, estas soluciones son cada vez más obsoletas y por lo tanto menos eficaces ante la cantidad de amenazas y la sofisticación de las mismas. ([11] Gartner, 2013)

Razón por la cual Gartner recomienda que las organizaciones deben adoptar una nueva estrategia en la cual adquieran soluciones de seguridad de próxima generación, dentro de estos equipos estarán detección y análisis de malware, firewalls de nueva generación, análisis forense, y la tecnología de SandBoxing.

En general, Gartner cree que las organizaciones deben utilizar soluciones que abarquen la mayoría de los ataques dirigidos a través de malware, además los ataques que implican Web deberán utilizar soluciones específicas como WAFs (Web Application Firewall) para reforzar el desarrollo de las aplicaciones Web.

1.9. TOPOLOGÍA DE LA RED

A continuación se presenta la topología de red de área de campus a ser simulada dentro de la red de EGOVERMENT SOLUTIONS S.A. (ver Figura. 1.9.).

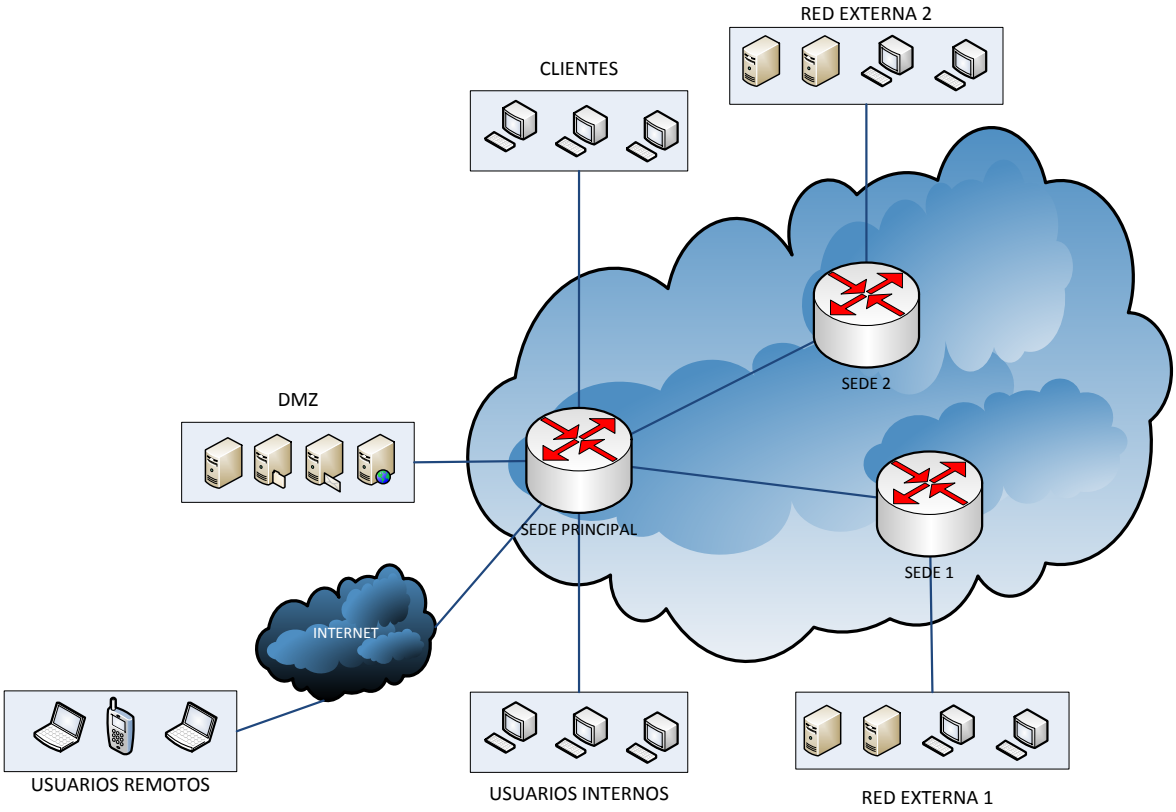


Figura. 1.9. Topología de red a ser simulada en la red de e-GovSolutions

Es necesario proteger todos los enlaces existentes con diferentes sistemas de seguridad, colocando protecciones adicionales en los enlaces que van hacia internet. Los dispositivos más importantes son el firewall y el sistema de prevención de intrusos y además en necesario investigar nuevas herramientas existentes que puedan complementar a los sistemas antes mencionados. (ver Figura. 1.10.).

Absolutamente todos los enlaces deben estar protegidos por un firewall y un sistema de prevención de intrusos. Para esto se utilizará un firewall de siguiente generación (Palo Alto Networks), el cuál funciona perfectamente como los dos elementos y como tiene una gran versatilidad de ruteo, este reemplazará a los ruteadores que se encuentran dentro de la red de área de campus y de esta forma pueden estar protegidos todos los enlaces internos existentes.

Para el acceso a internet se proveerán soluciones complementarias ya que es el principal vector de donde provienen las amenazas hoy en día, primero hay que tomar en cuenta que el sistema de prevención de intrusos es basado en firmas, por

lo que hay que proveer sistemas que sean capaces de bloquear ataques nuevos o desconocidos (FireEye y BotHunter).

Con el objetivo de no tomar ninguna acción, pero proveer mayor información en caso de una alerta se utilizará un sistema de detección de intrusos (Snort), además para tener un elemento con diferente arquitectura de forma que se pueda tener otro filtro de información.

Otro elemento que requiere protección adicional son los servidores WEB que suelen ser el punto de entrada de un atacante a la red interna, para esto se usará un firewall de aplicaciones WEB (ModSecurity).

Para proteger a los servidores de ataques internos, se va a colocar un honeypot (KFSensor) dentro de la DMZ a fin de detectar comportamiento anómalo en esa zona.

Finalmente para la protección de los dispositivos finales se debe tener protección antivirus (Kaspersky), un software que permita tener todos los programas actualizados (Secunia PSI) y elementos para realizar escaneos de vulnerabilidades continuos para poder realizar la corrección de los mismo (Qualys) (Tabla. 1.1.).

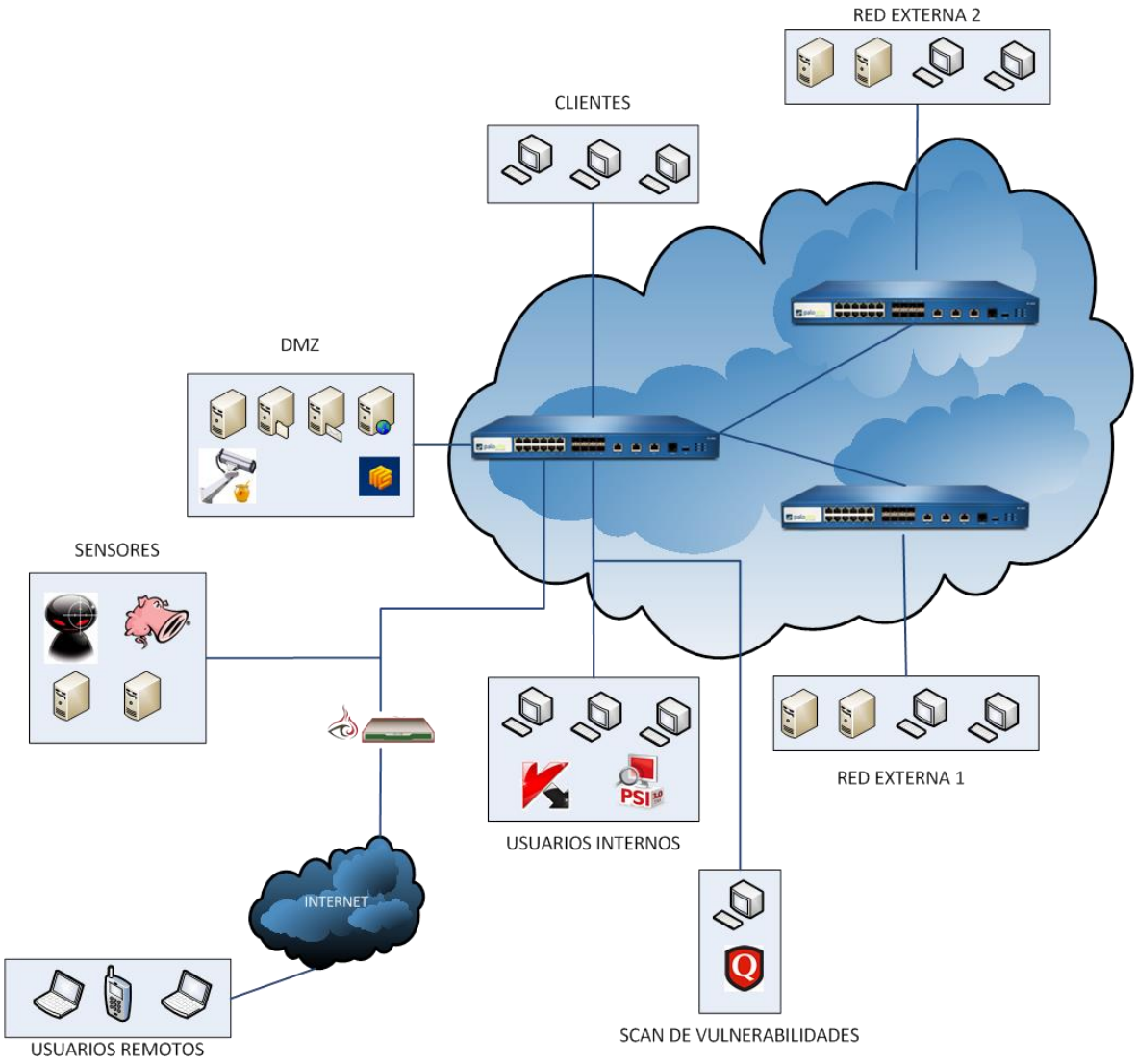


Figura. 1.10. Topología de la red

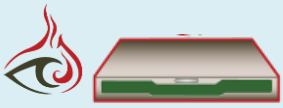
Símbolo	Significado
	FireEye Web MPS 4310 Protección contra amenazas de siguiente generación
	Palo Alto Networks PA – 3020 Firewall de siguiente generación
	BotHunter Sistema de diagnóstico de botnets
	Snort Sistema de detección de intrusos
	KFSensor HoneyPot
	ModSecurity Firewall de aplicaciones web
	Qualys Escáner de vulnerabilidades
	Karsperky Internet security
	Secunia PSI Gestor de actualizaciones

Tabla. 1.1. Simbología de la topología de la red

CAPÍTULO II

SEGURIDAD PERIMETRAL, INTERNA Y EN APLICACIONES WEB

2.1. SEGURIDAD PERIMETRAL

2.1.1. Importancia de la seguridad perimetral

Se entiende por seguridad perimetral a todas las herramientas de hardware o software que se pueden implementar para proteger todas las conexiones que se realicen entre la nube y la red local, esto protegerá a la red de todos los ataques que se generen por entes externos.

Por lo general esto comprende la primera etapa de una infección, la cual consiste en que el atacante mediante diferentes tipos de ataques logra ingresar a cualquier dispositivo interno de la red.

La mayoría de empresas concentran su esfuerzo en esta área ya que es evidente que al tener una puerta en la nube para la conexión a su red, además del acceso libre al internet, se genera una vulnerabilidad inmensa para la seguridad de la información de la empresa.

El atacante va a hacer una evaluación de todo el entorno de red, de manera que pueda conocerlo, comprenderlo para ser más asertivo al realizar su ataque (ver Figura. 2.1.).

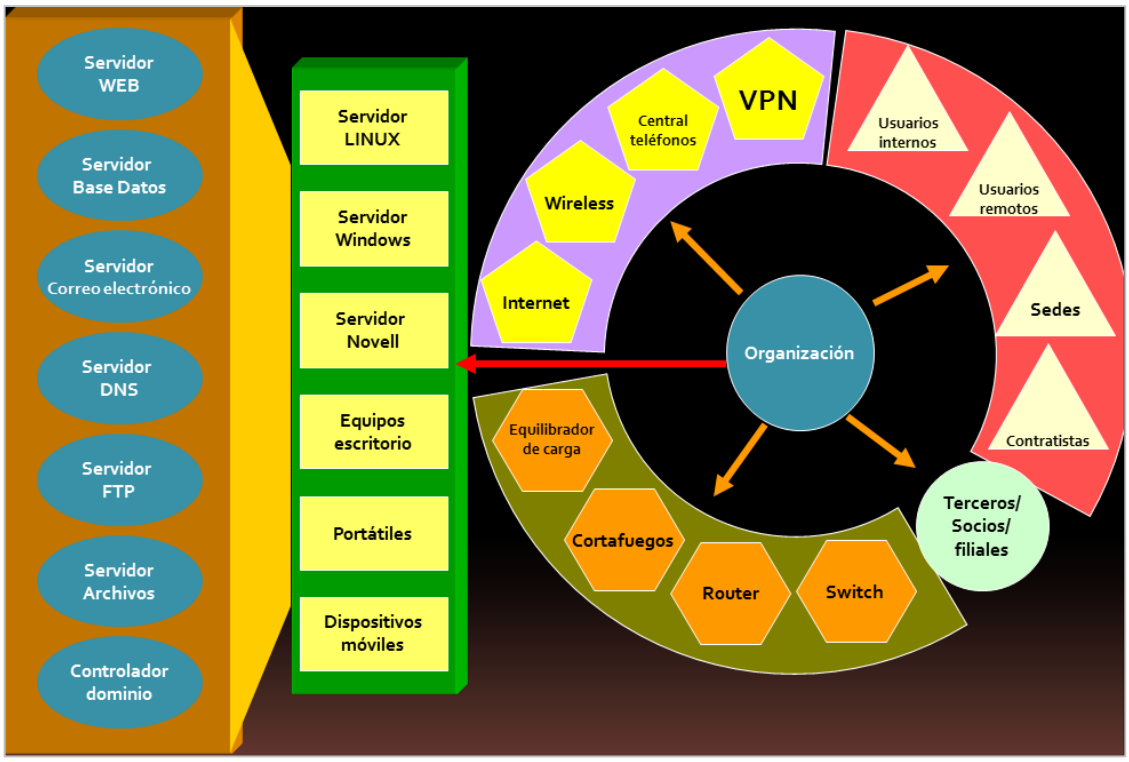


Figura. 2.1. El punto de vista del atacante ([12] Pazmiño, 2012)

Es por esto que si no se logra una protección óptima a nivel del perímetro, el atacante tendrá mayor visibilidad y potencial de llegar al objetivo mediante equipos privilegiados haciendo más complicado el trabajo de detección.

Siempre la puerta de entrada tiene que ser la que mayor protección tenga, de esta manera además de estar protegiendo la entrada de elementos no deseados, se protege la salida de información confidencial y privada.

2.1.2. Herramientas para seguridad perimetral

Existen varios elementos que pueden ayudar a la protección perimetral del entorno empresarial.

El principal elemento de seguridad perimetral es el cortafuegos (firewall), este dispositivo es el encargado de permitir el tráfico que es necesario para nuestro ambiente empresarial y sobretodo negar el acceso a entes no autorizados.

En este punto es necesario clasificar el firewall en dos tipos principales:

- Firewall tradicional
- Firewall de siguiente generación

El primero permite o limita el tráfico realizándolo mediante el bloqueo de puertos, el segundo lo realiza mediante el bloqueo de aplicaciones esto debido a la versatilidad y el crecimiento de aplicaciones evasivas que ya son lo suficientemente hábiles para funcionar en puertos que la mayoría de veces se encuentran abiertos (80, 442, 23, 21, etc.).

Otros dispositivos son los antivirus de red, estos funcionan a través de firmas y son capaces de detectar binarios de ataques conocidos.

Por otro lado existe también el sistema de prevención o detección de intrusos que va a tener la función de detectar los diferentes tipos de ataques conocidos de manera que pueda proteger o alertar. Estos dispositivos tienen la capacidad de detectar además comportamiento anómalo o sospechoso y aplica sus reglas de acuerdo al protocolo que detecta en la transmisión del paquete.

Otro dispositivo muy utilizado es el filtrado de URL que principalmente se basa en la reputación de direcciones web para categorizarlas y de esta manera poder crear políticas.

El elemento utilizado para prevenir la fuga de información es denominado DLP (Data Loss Prevention), estos equipos suelen buscar dentro de documentos o correos electrónicos expresiones regulares que permiten detectar palabras o patrones claves para la empresa.

Los servidores proxy son herramientas todavía muy utilizadas cuya principal función es interceptar las conexiones de red entre el cliente y el destino. Esto para realizar un monitoreo de la actividad y poder tomar acciones de bloqueo.

En necesario recalcar que ninguna de estas herramientas funciona para ataques no conocidos o no solucionados, es por esto que algunas empresas están

haciendo varios esfuerzos de manera que puedan detectar amenazas por patrones de comportamiento.

2.1.3. Analizador de malware perimetral (FireEye)

2.1.3.1. Introducción.

Existe un hueco de seguridad en donde las defensas tradicionales son vulnerables (ver Figura. 2.2.).

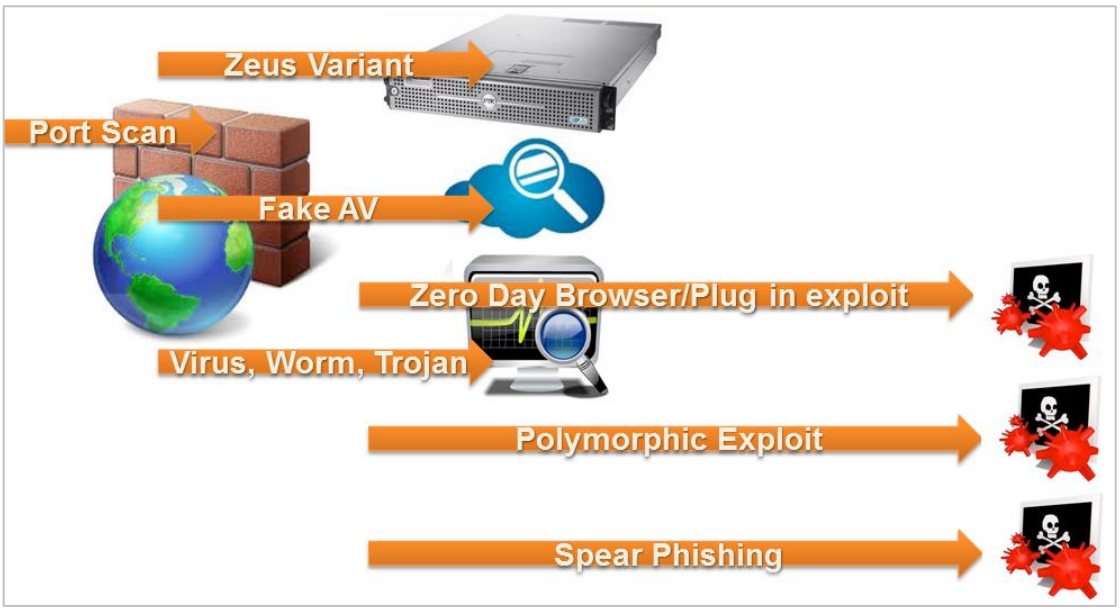


Figura. 2.2. Defensas tradicionales vulneradas ([4] FireEye, Inc., 2013)

Tres de los principales ataques para vulnerar las defensas tradicionales son los ataques de día cero, los exploits polimórficos y spear phishing. Los ataques de día cero lo van a hacer simplemente porque no tienen una firma o solución, los exploits polimórficos se encargan de burlar las firmas mediante modificaciones en su carga útil (payload), es decir, entienden el funcionamiento del sistema de prevención/detección de intrusos y se disfrazan para no encajar en los parámetros de sus reglas y finalmente el spear phishing es un phishing direccionado que conoce, entiende y analiza a su víctima de manera que mediante el engaño logre tener la “aprobación” para el ataque y así empezar a realizar cambios y solicitudes de usuario privilegiado.

Ante estos ataques sofisticados solo hay una forma posible de detectarlos y es analizando su comportamiento. Justamente lo que hace FireEye es correlacionar los eventos de los host detectando patrones sospechosos y además analiza y ejecuta los archivos que son transmitidos en ambientes virtualizados que simulan ambientes reales (servidores, distintos sistemas operativos, parches, usuarios finales, etc.). FireEye enfoca su análisis en tres sectores específicos (ver Figura. 2.3.): ([4] FireEye, Inc., 2013)

- Tráfico WEB (Web MPS)
- Servidores de correo (Email MPS)
- Servidores de archivos (File MPS)

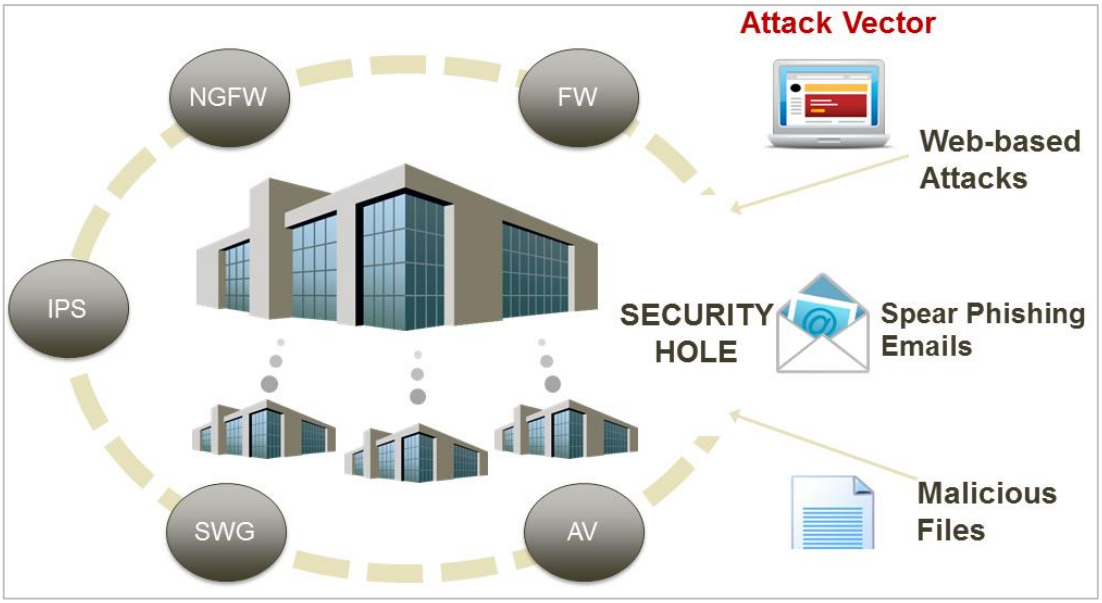


Figura. 2.3. FireEye cubre el hueco de seguridad ([4] FireEye, Inc., 2013)

Para cada uno de estos sectores, FireEye tiene un equipo independiente (hardware) por lo que para el sistema integral de prueba de EGOVERMENT SOLUTIONS únicamente se utilizará el Web MPS ya que la administración de servidores de correo se encuentra en la nube y no se poseen servidores de archivos.

El sistema de protección de malware de FireEye no pretende reemplazar ningún sistema de seguridad tradicional perimetral, simplemente se vuelve el complemento perfecto.

2.1.3.2. Identificación de malware basado en comportamiento

Existen patrones de comportamiento a nivel de sistema operativo, registros o programas específicos que pueden hacer notar la participación de un proceso en segundo plano ya sea para robo de información o comportamiento malicioso (ver Figura. 2.4.).

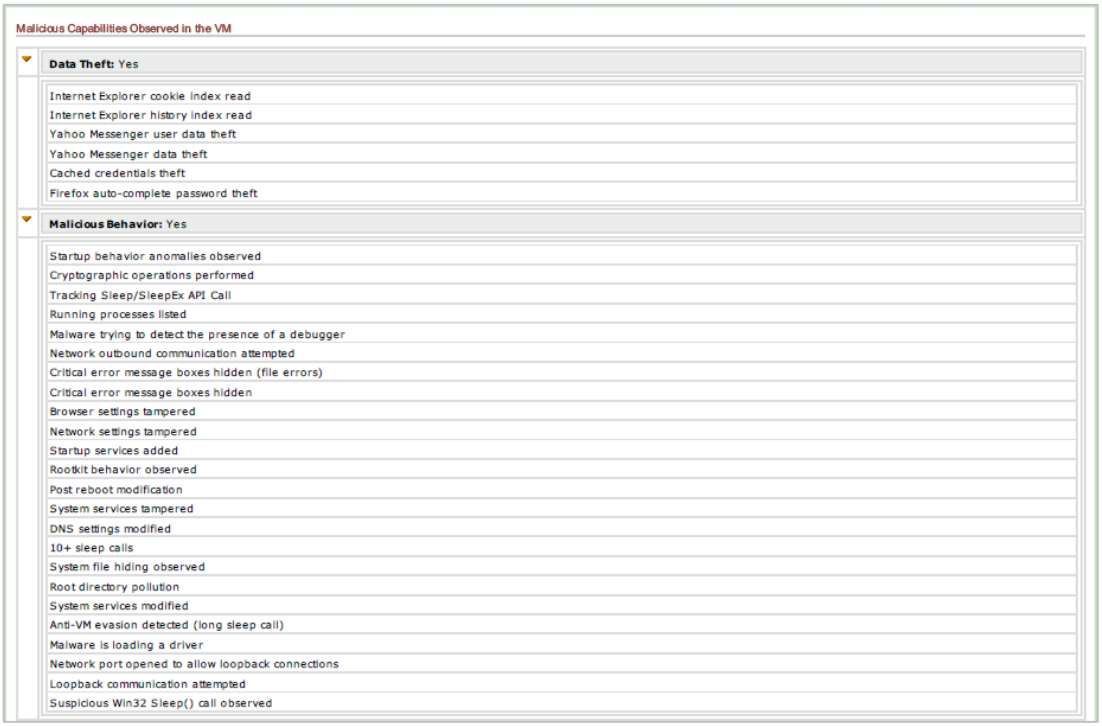


Figura. 2.4. Ejemplo de patrones de comportamiento maliciosos

Si bien es cierto que todos los malware tienen características diferentes de funcionamiento, se puede investigar acciones sospechosas como escalamiento de privilegios, modificación de registros o archivos de configuración.

La única forma de detectar este comportamiento es dejándole actuar al malware y permitiéndole que se ejecute sobre diversos ambientes de manera que sea posible analizar su legitimidad. Precisamente esto es lo que hace FireEye, además de analizar en ambientes virtualizados todos los archivos que pasan por la red también visualiza el comportamiento de los clientes reales, correlaciona los eventos y crea un perfil de infección.

Además de estos patrones de comportamientos también FireEye se encarga de correlacionar eventos con listas negras de servidores de comando y control y detecta binarios de malware, de manera que podamos realizar la descarga del archivo y analizarlo con diferentes herramientas de software y hardware para investigación forense. Por otro lado con este archivo se puede realizar un análisis en páginas como www.virustotal.com (ver Figura. 2.5.) de manera que se pueda identificar a los diferentes sistemas de antivirus que reconocen este binario como amenaza.

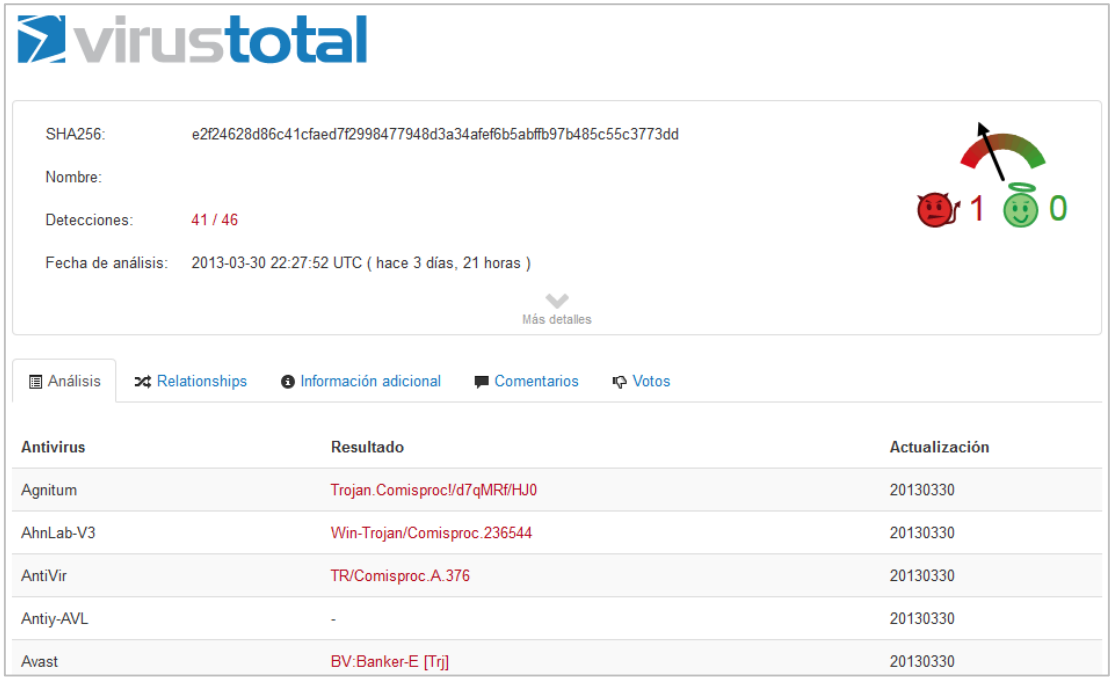


Figura. 2.5. Ejemplo de análisis de archivo en el sitio www.virustotal.com

Dejando de lado el análisis con FireEye, existen varias herramientas de uso libre que permitirán investigar una amenaza. Aquí el objetivo es montar un laboratorio en determinados sistemas operativos y ejecutar los archivos para analizar su comportamiento. Principalmente existen tres tipos de herramientas que colaborarán con este análisis:

- Herramientas basadas en hooks
- Herramientas basadas en diferencias
- Herramientas basadas en notificaciones

Las herramientas basadas en hooks, interceptan las llamadas a las API del sistema en modo kernel y en modo usuario de manera que se pueda detectar cuáles son los cambios realizados en un sistema. Estas proveerán una gran cantidad de información, sin embargo puede requerir un mayor tiempo para el análisis. ([13] EC-Council, 2013)

Las herramientas basadas en diferencias o también conocidas como herramientas basadas en snapshots guardan el estado del sistema en dos momentos diferentes de manera que se los puedan comparar y encontrar diferencias. ([13] EC-Council, 2013)

Las herramientas basadas en notificaciones pueden registran rutinas del sistema de manera automática cuando sucede un evento específico. Esta información es vital para un analista ya que puede determinar eventos importantes como la creación o modificación de archivos. ([13] EC-Council, 2013)

2.1.3.3. Funcionamiento interno

El sistema de protección de malware para tráfico web (Web MPS) se encarga de controlar el vector de amenazas web. Es un sistema cerrado capaz de controlar exploits web en tráfico de entrada y de salida y callbacks (llamados a servidores externos de comando y control) en diferentes protocolos.

El equipo se encarga de hacer una captura agresiva y analizarla con la ingeniería más sofisticada de virtualización de sistemas (ver Figura. 2.6.) para detección de ataques de día cero llamada MVX (Multi-Vector Virtual Execution), la cual permite protección en tiempo real y la captura de callbacks dinámicos. ([14] FireEye Inc., 2012)

Esta ingeniería permite un análisis multiflujo para entender todo el contexto de un ataque dirigido avanzado, entiende todo el ciclo de vida de un ataque, desde la explotación inicial hasta el robo de datos.

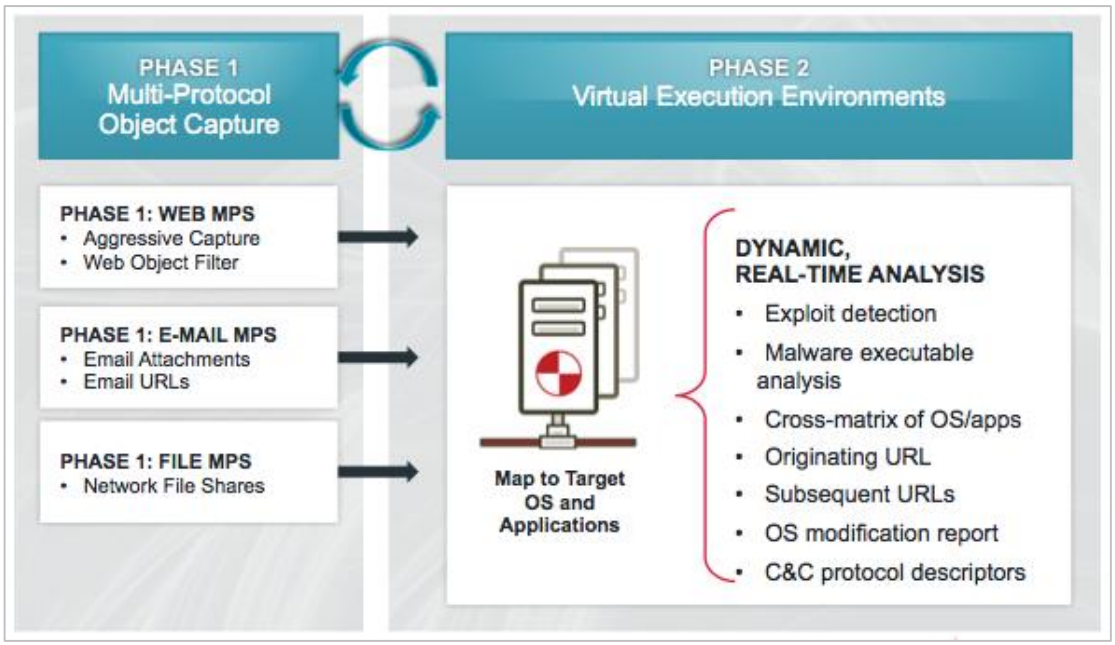


Figura. 2.6. Captura y análisis de paquetes ([4] FireEye, Inc., 2013)

El ciclo de acción del equipo de FireEye se resume en tres fases principales (ver Figura. 2.7.):

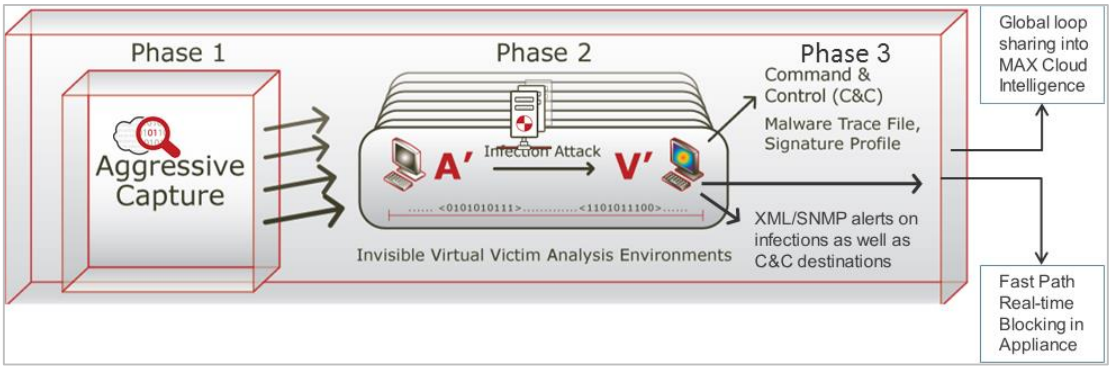


Figura. 2.7. Ciclo de acción de FireEye ([4] FireEye, Inc., 2013)

Fase 1: Agresiva captura heurística

- Se usa out-of-band/pasivo o en línea
- Captura multi-protocolo de HTML, archivos (por ejemplo: PDF) y ejecutables
- Maximiza la captura de ataques potenciales día-cero

Fase 2: Análisis máquina virtual

- Confirmación de ataques maliciosos
- Remoción de falsos positivos

Fase 3: Bloquea callbacks

- Detiene robo de data/bienes

Finalmente una vez que se ha detectado un ataque diferente, todos los equipos FireEye alrededor del mundo son notificados mediante el Malware Protection Cloud (MPC) el cuál es el servicio para descarga de actualizaciones, firmas, parches, versiones de máquinas virtuales y versiones de sistemas operativos.

2.1.3.4. Ventajas y desventajas

Ventajas:

- Es capaz de detectar cualquier tipo de malware sofisticado.
- Es capaz de detener callbacks en caso de que ingrese un host infectado.
- Fácil instalación y configuración.
- Es capaz de enviar notificaciones vía correo electrónico o vía syslog hacia un sistema de correlación de eventos.
- No genera latencia.
- Recibe colaboraciones de todas las partes del mundo (MPC Network).

Desventajas:

- Es una herramienta costosa.
- No es capaz de descifrar tráfico.
- Debido a la cantidad de interfaces tiene limitaciones para colocar el equipo en sectores internos.
- El equipo más grande soporta 1Gbps de thoughput, lo que limita su funcionamiento en ambientes muy grandes.

2.1.4. Firewall de siguiente generación (Palo Alto Networks)

2.1.4.1. Introducción

En la última década la necesidad de la evolución de las amenazas y las aplicaciones ha generado un avance sumamente importante en el tema de seguridad perimetral, específicamente en el tema de los cortafuegos.

Como se vio anteriormente este debe ser el dispositivo que se encargue de permitir solo el tráfico que se desea dentro de la red tanto de entrada como de salida. Anteriormente parecía suficiente con controlar direcciones IP's y puertos pero ahora, debido a que las aplicaciones son evasivas, vulnerables y usadas para malware, los cortafuegos han tenido que seguir evolucionando y empezar a detectar las mismas independientemente de la dirección y puerto. También se ha visto la necesidad de inspeccionar dentro de estas aplicaciones para ver realmente si son legítimas o están llevando algún código no deseado dentro de ellas y finalmente se ha llegado a la conclusión que los computadores ya no necesariamente se encuentran asociadas a una persona por lo que la mayoría de empresas utilizan servidores de dominio que permiten al usuario autenticarse con su contraseña y es importante que el cortafuegos tome una decisión también con esta información.

En resumen los siguientes son los requerimientos que debe tener un cortafuegos para que sea considerado de nueva generación:

- Identificar aplicaciones independientemente del puerto, protocolo, cifrado o táctica evasiva.
- Identificar usuarios en lugar de direcciones IP's.
- Proteger en tiempo real contra amenazas embebidas dentro de las aplicaciones.
- Visibilidad granular y control de acceso y funcionalidad de las aplicaciones.
- Implementación en modo de bloqueo con capacidad de multi-gigabit sin degradación de rendimiento.

Ahora para elegir la herramienta a ser utilizada se va a analizar inicialmente el cuadrante de Gartner en el tema de Firewalls.

El cuadrante de Gartner es una serie de reportes publicada por Gartner Inc. que se encargan de posicionar a las empresas tecnológicas dentro de un mercado

específico. Este se ha convertido en un análisis sumamente reconocido alrededor del mundo y por lo general es el primer paso de cualquier empresa para investigar a los proveedores de tecnología antes de decidir hacer una inversión.

Con esta serie de reportes se puede ver de manera gráfica donde se encuentras los competidores divididos principalmente en 4 grupos (ver Figura. 2.8.): ([15] Gartner Inc., 2013)

- Líderes.- ejecutan correctamente de acuerdo a su visión del mercado y se aseguran una buena posición en el futuro
- Visionarios.- entienden el camino correcto del mercado, pero no lo ejecutan bien
- Jugadores en posición aceptable.- suelen ser exitosos en un mercado pequeño, no innovan y se enfocan en ser más eficaces que sus competidores
- Desafiantes.- ejecutan bien y son capaces de enfocarse en una gran parte del mercado, sin embargo no llegan a entender cuál es la dirección del mismo.

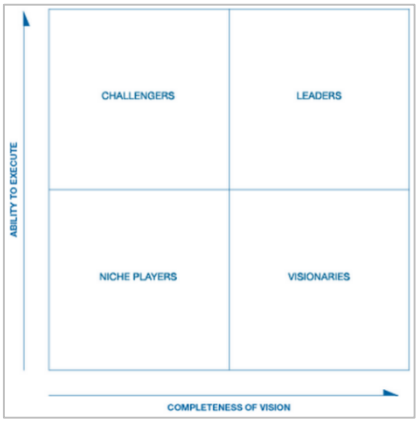


Figura. 2.8. Formato del cuadrante de Gartner ([15] Gartner Inc., 2013)

No siempre la mejor opción va a ser buscar dentro de los líderes principalmente porque por lo general son los más costosos, por esto es necesario realizar un análisis de las necesidades. En el tema de cortafuegos nos vamos a concentrar este cuadrante ya que debido a la evolución de las aplicaciones debemos contar con un equipo que entienda perfectamente cuál es el camino correcto y obviamente que lo sepa ejecutar.

Para escoger el equipo correcto se va a analizar los cuadrantes de los últimos 2 años, 2012 (ver Figura. 2.9.) y 2013 (ver Figura. 2.10.).

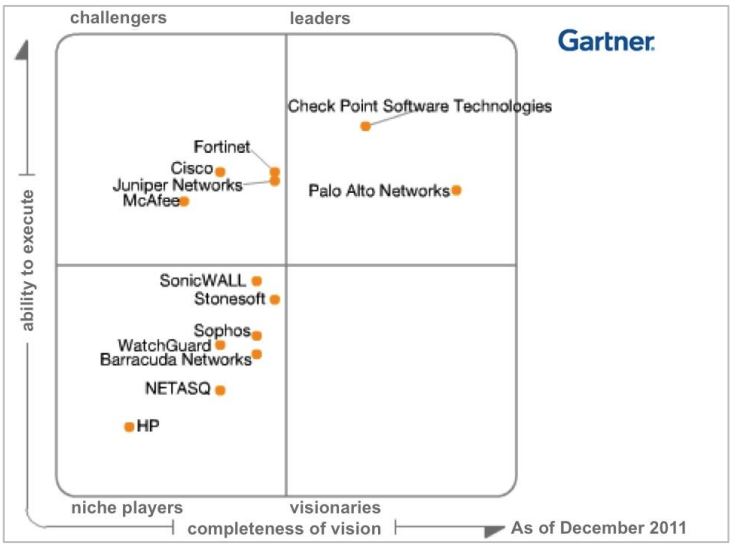


Figura. 2.9. Cuadrante de Gartner de firewalls empresariales de diciembre del 2011 ([16] Gartner Inc., 2011)

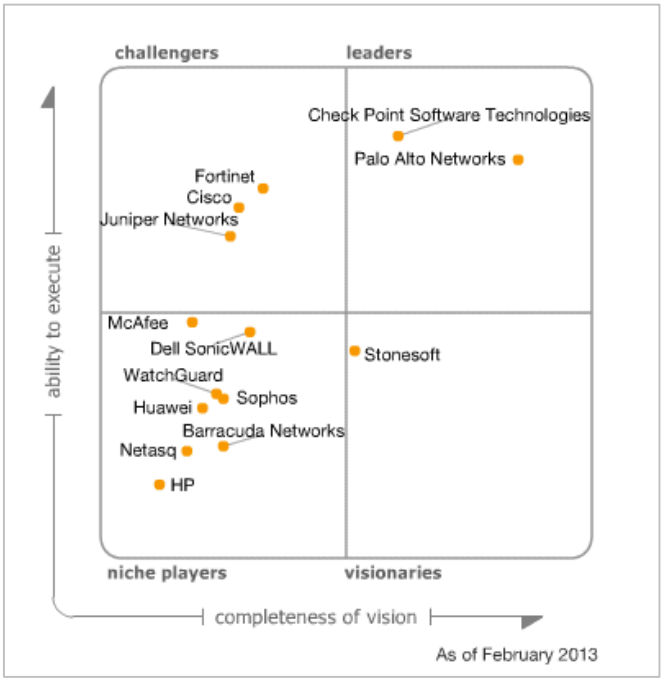


Figura. 2.10. Cuadrante de Gartner de firewalls empresariales de febrero del 2013 ([17] Gartner Inc., 2013)

En el cuadrante de líderes solo tenemos a dos competidores que coinciden en los dos últimos años: Check Point y Palo Alto Networks. En los últimos dos años

podemos ver que el más visionario ha sido Palo Alto Networks con una distancia considerable y que en apenas 8 años ya casi ha alcanzo la habilidad de ejecución de una empresa que ya lleva 20 años en el mercado, por lo que solo por el análisis del cuadrante le da una ventaja a Palo Alto Networks

Dentro del análisis, se va a proceder a analizar los siguientes puntos:

- Tecnología
- Rendimiento
- Administración
- Generación de Reportes
- Confiabilidad

La tecnología usada por Check Point y de muchos otros competidores es conocida como Statefull Inspection y la de Palo Alto Networks es conocida como App-ID.

La primera consiste en realizar un seguimiento de los estados de las conexiones de red que atraviesan el firewall por lo que principalmente toman decisiones con la información que proviene de la cabecera del paquete. Por otro lado la tecnología de Palo Alto Networks se basa en la identificación de aplicaciones mediante firmas y además es capaz de descifrar, decodificar y utilizar heurística. La gran desventaja de Statefull Inspection es que es muy poco capaz de detectar aplicaciones dentro de la misma url, por ejemplo, Facebook tiene dentro de la misma página varias aplicaciones (chat, posting, mail, apps, etc.). Esto se vuelve una gran ventaja para Palo Alto Networks ya que toma la decisión principalmente basado en la capa 7 del modelo OSI. Por lo tanto en este punto se puede decir que Palo Alto Networks es la mejor opción.

A nivel de rendimiento, debido a su tecnología Check Point puede disminuir su rendimiento hasta un 90% si todas las características del mismo están activas (IPS, filtrado de URL, DLP, etc). Palo Alto Networks tiene una disminución máxima de su ancho de banda del 30%. Esta diferencia principalmente se da puesto que

Check Point (al igual que todos los statefull inspection) realiza el procesamiento del mismo paquete varias veces, una por cada módulo activado (ver Figura. 2.11.).

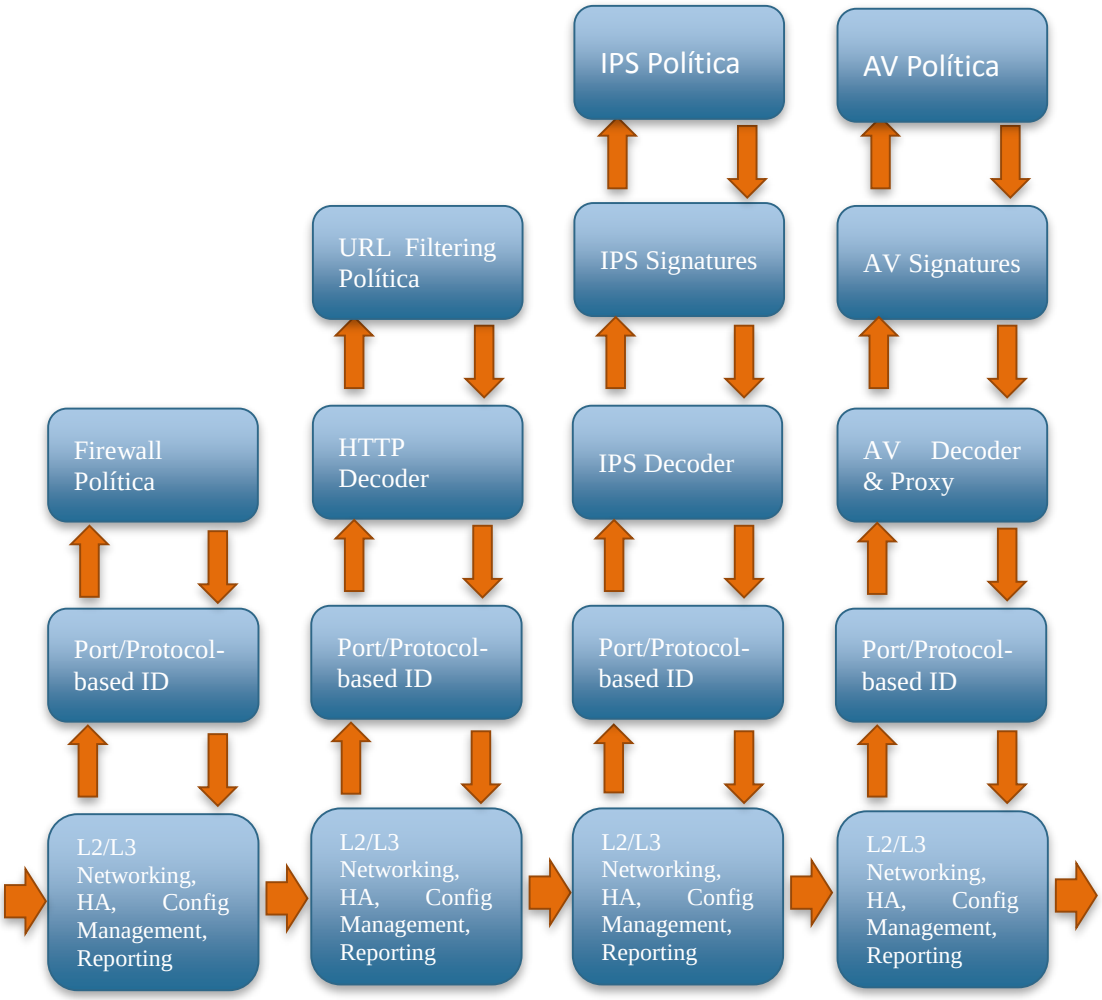


Figura. 2.11. Flujo de tráfico Stateful Inspection ([18] Monarque, 2012)

Por lo tanto debido a que Palo Alto Networks puede hacer todo el procesamiento en un solo flujo de tráfico (ver Figura. 2.12.), este punto también se vuelve positivo para Palo Alto Networks.

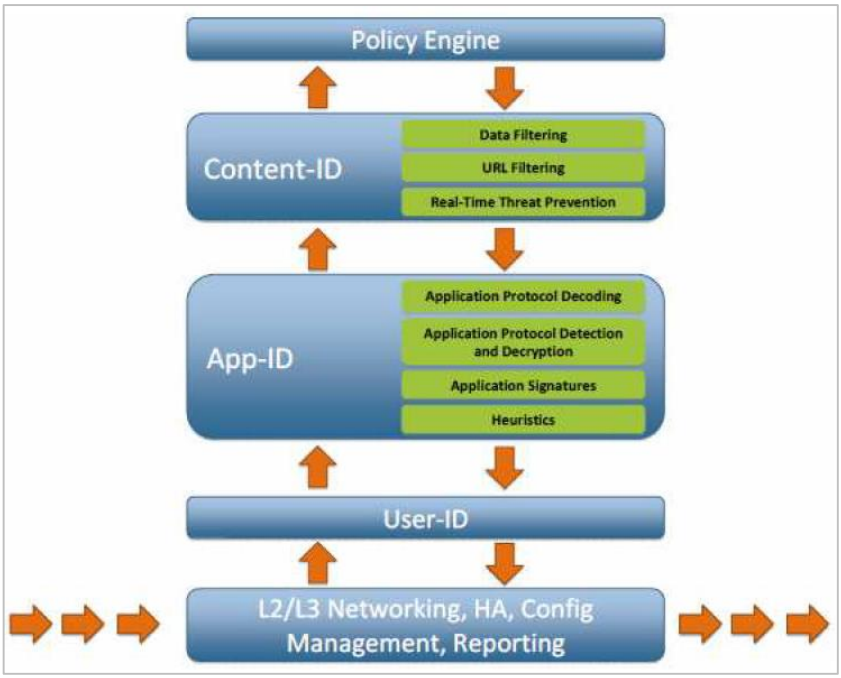


Figura. 2.12. Flujo de tráfico Palo Alto Networks ([19] Palo Alto Networks, 2012)

En el lado de administración es una decisión muy simple. En Check Point se debe crear series de políticas por cada módulo incorporado, mientras que Palo Alto Networks tiene políticas unificadas, es decir, dentro de una misma política se define perfiles de aplicación, IPS, filtrado de URL, DLP, etc. Por lo tanto se considera que es otra característica favorable para Palo Alto Networks.

El tema de reportes de las dos marcas es muy similar, realmente los dos son muy buenos ya que mediante el manejo de filtros se pueden obtener reportes personalizados con únicamente la información que se desea. Sin embargo Check Point tiene un módulo exclusivo de generación de reportes por lo que esto genera un costo adicional, lo que genera una inclinación nuevamente hacia Palo Alto Networks.

Finalmente en el punto de confianza hay que dárselo a Check Point ya que es una empresa que a lo largo de los años se ha sabido ganar la seguridad de sus clientes y su experiencia es mayor a la de Palo Ato Networks. Es por eso que en el cuadrante de Gartner se lo ubica con una mayor habilidad de ejecución.

Por lo tanto la elección para firewall de siguiente generación es Palo Alto Networks.

2.1.4.2. Firewall vs Firewall de nueva generación.

Como se lo ha mencionado anteriormente, el firewall es el dispositivo encargado de permitir el ingreso a la red únicamente a los usuarios permitidos y que puedan navegar las aplicaciones permitidas. Anteriormente este requerimiento se traducía a controlar direcciones IP's y puertos, por ejemplo se entendía que todo el tráfico que circula por el puerto 80 es HTTP. Actualmente las aplicaciones han cambiado, están son evasivas y se comunican a una gran cantidad de servidores que son renovados o cambiados a diario. Por ejemplo, en el tema de proxys anónimos (servidor proxy que sirve como intermediario con el objetivo de que el usuario pueda navegar a las páginas que desee sin dejar rastro alguno) existen miles de servidores de este tipo que salen a diario y que es muy fácil de encontrarlos (ver Figura. 2.13.), por lo tanto intentar colocar estas direcciones IP's en listas negras es un trabajo imposible de realizar.

Last update	IP address	Port	Country	Speed	Connection time	Type	Anonymity
18 secs	93.123.45.23	8008	Bulgaria			HTTPS	High +KA
18 secs	190.14.226.74	8080	Colombia			HTTPS	High +KA
1 minute	110.138.216.102	8080	Indonesia			HTTPS	High +KA
2 minutes	190.214.41.90	3128	Ecuador			HTTPS	High +KA
2 minutes	193.179.3.20	8080	Czech Republic			HTTPS	High +KA
2 minutes	64.185.107.238	3128	United States			HTTP	Low
3 minutes	211.108.62.230	8888	Korea, Republic of			socks4/5	High +KA
3 minutes	200.146.46.218	3128	Brazil			HTTPS	High +KA
3 minutes	202.159.95.220	8080	Indonesia			HTTPS	High +KA
4 minutes	195.251.250.243	3128	Greece			HTTPS	High +KA
4 minutes	212.113.47.87	3128	Ukraine			HTTPS	High +KA
4 minutes	1.63.199.162	6675	China			socks4/5	High +KA
5 minutes	124.67.101.134	6675	China			socks4/5	High +KA
6 minutes	203.77.250.170	8080	Indonesia			HTTPS	High +KA
6 minutes	125.214.169.67	8080	Sri Lanka			HTTPS	High +KA
6 minutes	77.94.48.5	80	Turkmenistan			HTTP	Low
6 minutes	217.12.113.67	443	Moldova, Republic of			HTTPS	High +KA

Figura. 2.13. Resultado de la búsqueda de proxys anónimos en la página www.hidemyass.com

Bajo estas premisas, los cortafuegos tuvieron que innovar e ir más allá, esto quiere decir que en lugar de tomar una decisión por medio de la dirección IP, se la debe tomar por la aplicación. Por ejemplo en el caso de los proxys anónimos, independientemente de al servidor al que se conecten, estos corresponden a la misma aplicación (identificada usualmente como “php proxy”) y así se pueden ejecutar políticas prohibiendo el uso de los mismos.

Otro de los cambios necesarios en los cortafuegos fue la identificación de usuarios en lugar de direcciones IP’s. Con el enorme crecimiento del uso de dispositivos móviles (laptops, teléfonos inteligentes y tablets) que requieren conectarse al internet a través de redes inalámbricas se volvió indispensable el uso de servidores de dominio y portales cautivos (software o hardware que vigila el tráfico y fuerza a los usuarios a pasar por una página especial para autenticarse) para conocer el usuario conectado, es por esto que las políticas tienen que establecerse mediante el usuario.

La última diferencia principal entre los dos tipos de cortafuegos es la inspección dentro del contenido del tráfico. En la actualidad existen amenazas y datos dentro de aplicaciones legítimas. Si un usuario está autorizado a utilizar una aplicación determinada es necesario que esta aplicación sea segura para la empresa, para esto es necesario la búsqueda de amenazas (virus, spyware, exploits, etc), tipo de contenido de la navegación (filtrado de URL) y datos sensibles para la organización (Data Loss Prevention).

Analizando estos puntos se concluirá que un cortafuegos tradicional no es capaz de tomar una decisión de lógica positiva (permitir únicamente lo que se desea, en lugar de bloquear lo que no se desea), esto genera el problema de que aplicaciones que son capaces de utilizar puertos comúnmente abiertos, como el 80 (HTTP) o 443 (HTTPS), van a poder generar tráfico sin ser detectados (ver Figura. 2.14.).

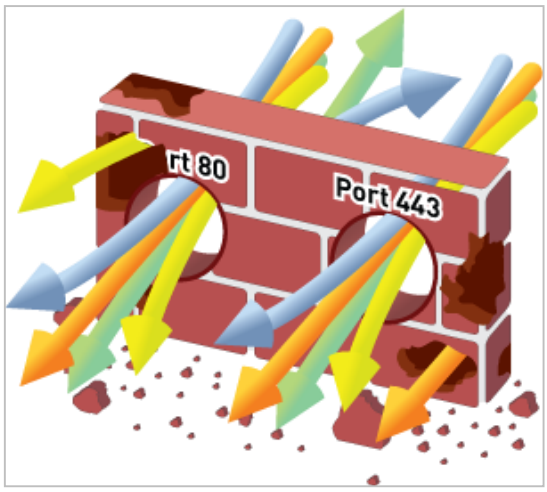


Figura. 2.14. Firewall tradicional vulnerado ([20] Palo Alto Networks, 2012)

2.1.4.3. Funcionamiento interno.

Internamente el cortafuegos de Palo Alto Networks realiza un procesamiento paralelo entre todo lo que comprende el flujo de tráfico y la parte de procesamiento del tráfico (ver Figura. 2.15.), en la cual contiene CPU's independientes para realizar la parte de administración del equipo y la otra para el procesamiento de los paquetes. Esto permite que el flujo de tráfico no se vea afectado si existe alguna sobrecarga de administración o procesamiento.

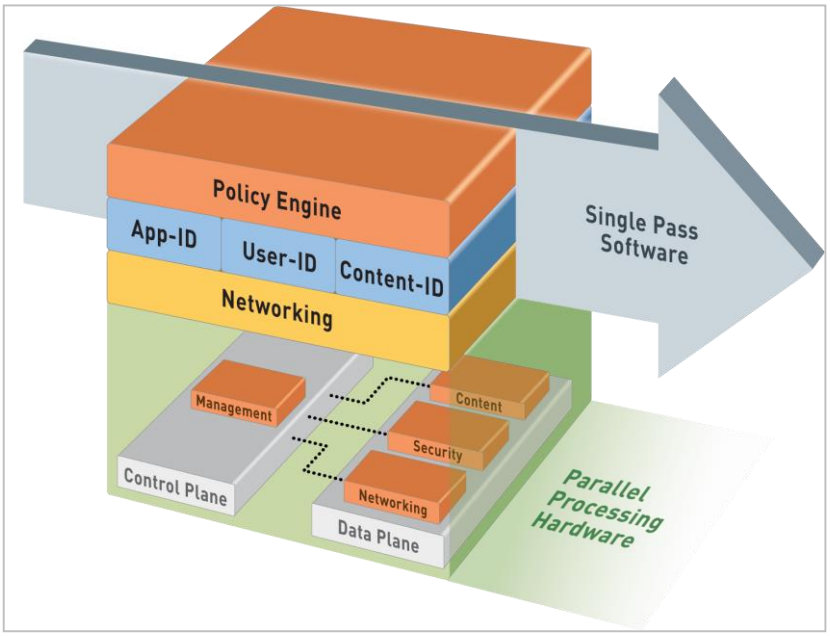


Figura. 2.15. Arquitectura Palo Alto Networks ([20] Palo Alto Networks, 2012)

2.1.4.4. Identificación de aplicación, usuario y contenido

Los cortafuegos de Palo Alto Networks se caracterizan principalmente por funcionar con tres tecnologías principales:

- App-ID
- User-ID
- Content-ID

App-ID es el encargado de identificar las aplicaciones y lo hace mediante cuatro características principales (Figura 2.16.):

- Firmas de aplicaciones
- Decodificación
- Descifrar
- Heurística

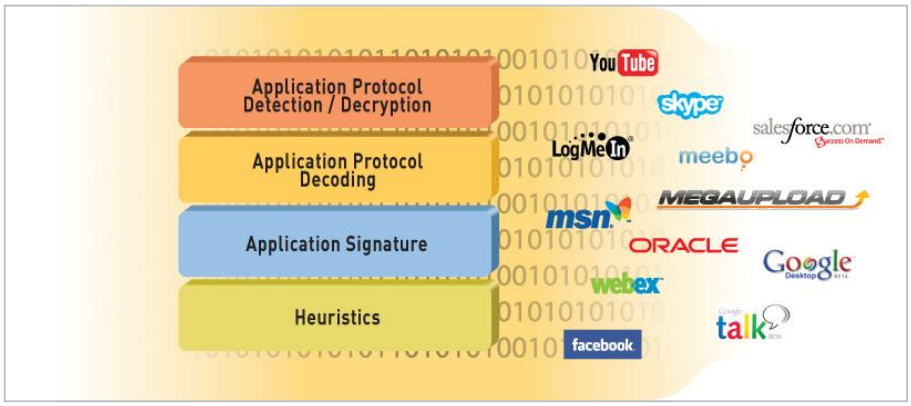


Figura. 2.16. Características principales App-ID ([20] Palo Alto Networks, 2012)

El flujo del análisis del tráfico (ver Figura. 2.17.) realiza el siguiente procedimiento:

- Identifica la dirección IP y el puerto de comunicación.
- Compara el tráfico con las firmas de aplicaciones disponibles en la base de datos de Palo Alto Networks.
- Aplica las políticas de descifrado (SSL o SSH) y vuelve a realizar la comparación con las firmas de aplicaciones.
- Busca protocolos de codificación conocidos, intenta decodificarlo y vuelve a realizar la comparación con las firmas de aplicaciones.

- Aplica heurística buscando patrones de comunicación y comportamiento para de esta manera intentar identificar la aplicación.
- En caso de que no logré identificar la aplicación, esta aparecerá como aplicación desconocida para futura investigación de la organización (es muy probable que sean aplicaciones desarrolladas internamente) o directamente de la gente de soporte de Palo Alto Networks, esto a fin de crear una firma de aplicación para uso interno o mundial dependiendo del caso.
- Posterior a cada uno de los pasos anteriores revisa la existencia de políticas y aplica las acciones respectivas.

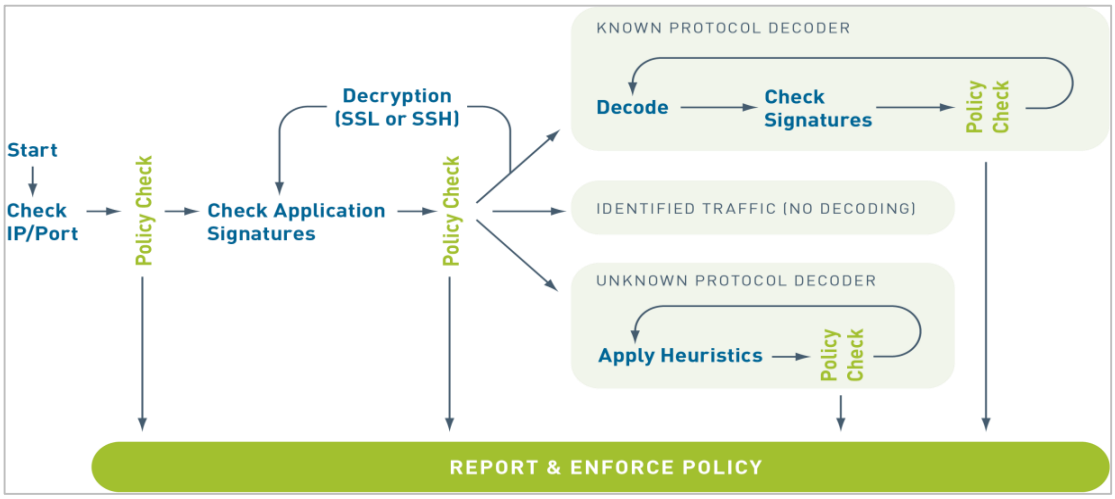


Figura. 2.17. Procedimiento App-ID ([19] Palo Alto Networks, 2012)

User-ID es el encargado de identificar los usuarios y lo hace mediante cuatro características principales (ver Figura. 2.18.):

- Monitoreo de logs
- Descubrimiento de roles
- Polling de estación final
- Portal cautivo

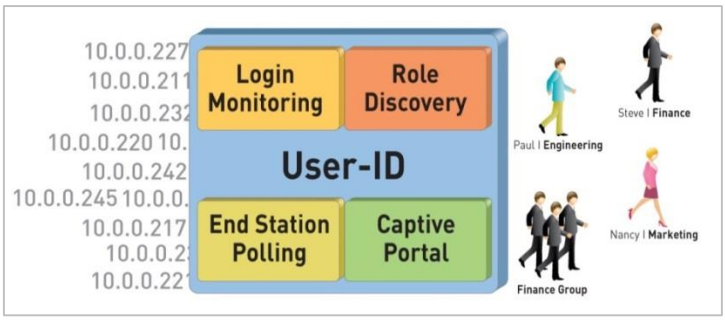


Figura. 2.18. Características principales User-ID ([20] Palo Alto Networks, 2012)

Esta tecnología se basa agentes o API's que interactúan y se comunican con los servidores de dominio (Active Directory, LDAP, Radius, Kerberos, etc). El procedimiento (ver Figura. 2.19.) se resume en que es capaz de realizar un monitoreo de logs para comprender todas las interacciones del servidor, además puede entender cuál es el rol del usuario mediante la creación o existencia de grupos. Posteriormente realiza polling de estación final para realizar consultas constantes y que no existan interrupciones del servicio y finalmente tiene la capacidad de crear un portal cautivo para lograr la autenticación de usuarios con dispositivos remotos. ([19] Palo Alto Networks, 2012)

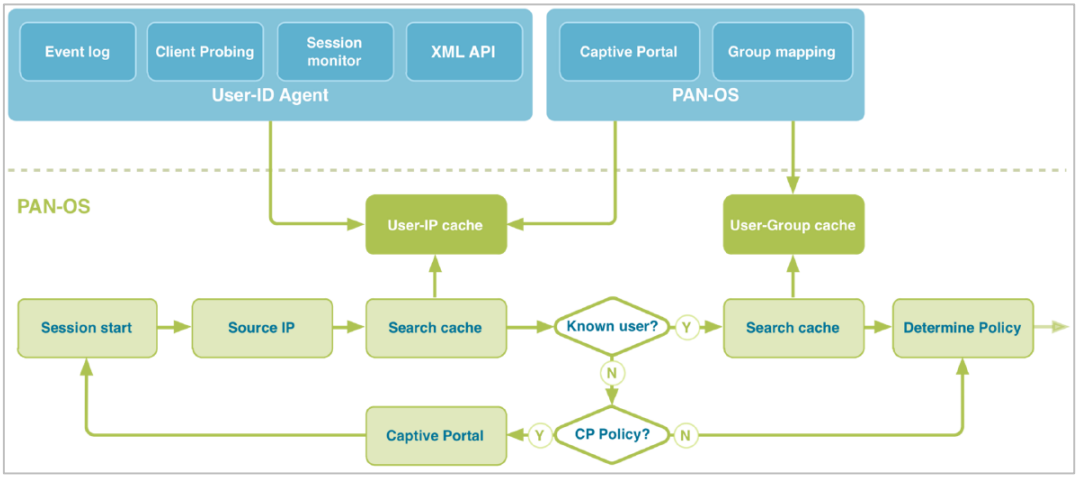


Figura. 2.19. Procedimiento User-ID ([19] Palo Alto Networks, 2012)

Content-ID es el encargado de inspeccionar el contenido transmitido dentro de las aplicaciones y lo hace en tres principales segmentos (ver Figura. 2.20.):

- Datos
- Amenazas
- URL's

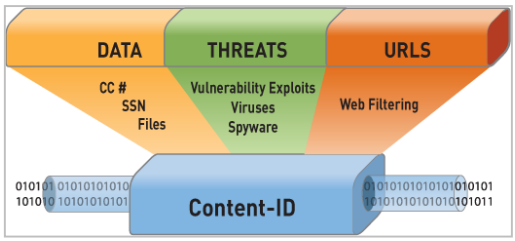


Figura. 2.20. Procedimiento User-ID ([20] Palo Alto Networks, 2012)

La parte de datos se encarga de investigar los tipos de archivos que se transmiten por la aplicación y además inspeccionar el contenido dentro de los mismos en busca de expresiones regulares definidas por el administrador (números de cédula, tarjetas de crédito, etc.). En la sección de amenazas el equipo buscará virus, spyware, tráfico que se identifique como exploits que pueden aprovechar una vulnerabilidad conocida. Finalmente la parte de URL consiste en un filtrado orientado únicamente al tráfico web que permitirá conocer la categorización de la dirección a la que se está navegando.

2.1.4.5. Ventajas y desventajas

Ventajas:

- Amigable
- Latencia muy baja
- Políticas unificadas
- Puede descifrar el tráfico SSL y SSH
- Líder en el cuadrante de Gartner y el más visionario
- Identifica aplicaciones
- Identifica usuarios
- Puede crear firmas de ataques basados en su comportamiento
- Degradamiento de rendimiento muy bajo
- Es muy versátil en networking, sobre todo para la creación de VPN’s
- Da protección completa a usuarios remotos

Desventajas:

- Es el firewall más costoso del mercado.
- El sistema de prevención de intrusos es basado en firmas

2.1.5. Sistema de detección de intrusos (Snort)

2.1.5.1. Introducción.

Snort es un sistema de detección y prevención de intrusos de red. Es un software de código abierto gratuito creado por Martin Roesch en 1998. Actualmente Snort es desarrollado por SourceFire, empresa de la cual Roesch es fundador y CTO. Snort ha tenido varios reconocimientos muy importantes, quizá el más destacado sea el haber ingresado al “Salón de la Fama” de InfoWorld (ver Figura. 2.21.) en el 2009 en la categoría de mejor software de código abierto de todos los tiempos. ([21] Doug Dineley, 2009)

Figura. 2.21. Mejor software de código abierto de todos los tiempos InfoWorld ([21] Doug Dineley, 2009)

Snort permite analizar tráfico en tiempo real en redes IP. Snort permite análisis de protocolos y contenido mediante el uso de reglas específicas.

Snort fue originalmente lanzado en Linux, actualmente se lo puede instalar en las distribuciones más populares de Linux y también en Windows.

A lo largo de los años se han creado varios proyectos que utilizan en su base a Snort lo que le ha permitido tener millones de colaboradores alrededor del mundo. Entre los proyectos más importantes están los siguientes:

- Sourcefire (comercial)
- Snorby (gratuito)
- Sguil (gratuito)
- Aanval (comercial)
- BASE (gratuito)
- Squert (gratuito)

Lo más importante que proveen estas herramientas es administración, reportes y análisis de logs.

Además existe un proyecto que está tomando mucha fuerza en los últimos tiempos, este es “Security Onion”, el cual consiste en una instalación integral de varias herramientas basadas en Ubuntu para lograr tener un ambiente muy completo de análisis para la detección y prevención de intrusos solo basado en herramientas gratuitas de código abierto. Las herramientas que están englobadas en este proyecto son: Snort, Suricata, Bro, Sguil, Squert, Snorby, Xplico, NetworkMiner entre otras. Otra de las grandes ventajas de este proyecto es la facilidad en la instalación que se la realiza en cuestión de minutos. ([22] Burks, 2012)

2.1.5.2. Funcionamiento interno.

Snort al igual que todos los sistemas de detección de intrusos tradicionales funcionan a través de reglas que permiten configurar varios parámetros identificativos del tráfico de red de manera que se detecten determinados patrones de comunicación del software malicioso.

La secuencia de acción de Snort se da de la siguiente manera (ver Figura. 2.22.): ([23] Montoro, 2012)

- Captura del paquete.
- Decodifica con la información de protocolos conocidos.
- Se ejecutan preprocesadores predefinidos dependiendo del tipo de tráfico (FTP, SSH, HTTP, IMAP, POP, RPC, Skype, Stream5, entre otros).
- Se compara el resultado con las reglas pre definidas y activadas.
- En caso de que no empate con ninguna regla, el tráfico continúa.
- En caso de que empate con alguna regla, el tráfico continúa a los plugins de salida y toma la acción definida por la regla, se procede a generar un log de alerta dentro del servidor y, en caso de estar configurado, realiza el envío del evento (vía syslog, e-mail, etc.)

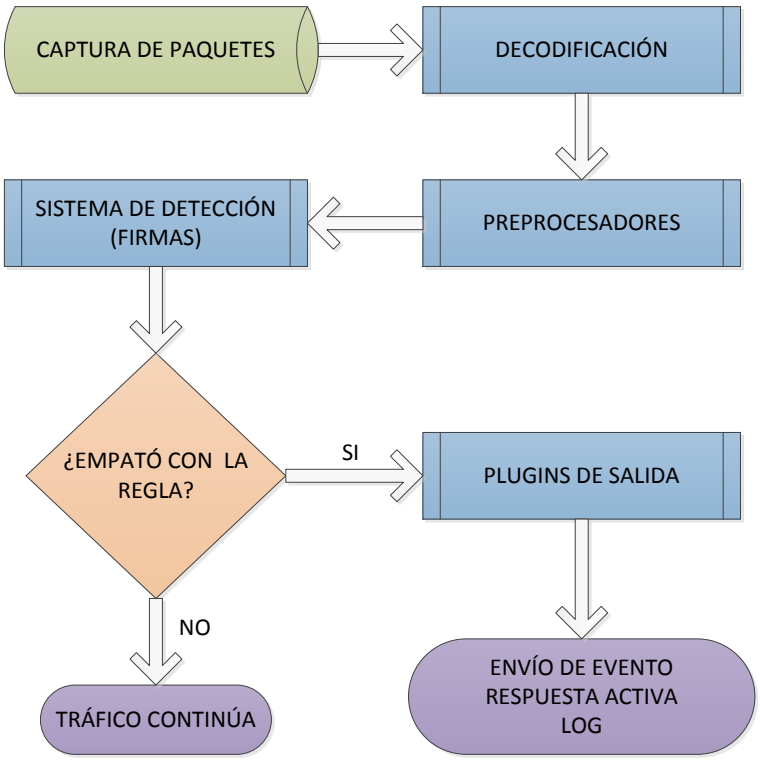


Figura. 2.22. Diagrama de flujo del funcionamiento de Snort

La parte principal configurable dentro de Snort es la sección de reglas, aquí podemos realizar la descarga de reglas creadas por terceros o colocar reglas definidas por el usuario.

Una regla se forma de dos partes principales: cabecera y opciones (ver Figura. 2.23.)

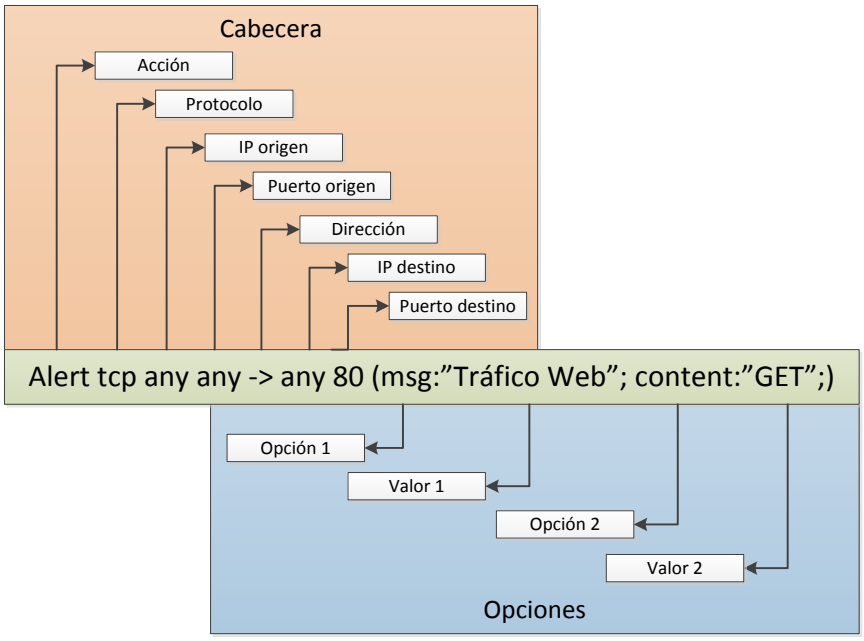


Figura. 2.23. Componentes de una regla de Snort

La cabecera se encarga de identificar el tráfico basado en la dirección IP y el puerto y la acción que va a realizar con el mismo. La parte de opciones contiene condiciones más específicas para filtrar de forma más granular el tráfico buscado.

La cabecera se compone de acción, protocolo, dirección IP origen, puerto origen, dirección, dirección IP destino y puerto destino.

La acción indica que es lo que va a hacer con el paquete. Este valor puedes se configurado con cualquiera de los siguientes valores: ([24] The Snort Project, 2013)

- Pass.- indica que Snort debe ignorar el paquete.
- Log.- indica que Snort debe generar un log del paquete que empate con una regla.
- Alert.- se generará una alerta y un log del evento.
- Activate.- es utilizado para generar una alerta y activar otra regla para verificar la legitimidad de la naturaleza del tráfico.

- Dynamic.- estas reglas son única y exclusivamente activadas por reglas de acción “Activate”. Esta es una buena forma de realizar reglas con mayor complejidad con el objetivo de generar una menor cantidad de falsos positivos.
- Acciones definidas por el usuario.- Snort permite a sus usuarios crear sus propias acciones personalizadas. Aquí se puede configurar por ejemplo enviar a un correo electrónico o enviar a un archivo o base de datos específica.

El campo de protocolo busca paquetes transmitidos con ese protocolo. Este puede ser configurado con las siguientes opciones:

- TCP
- UDP
- ICMP
- IP
- Any.- encaja con todos los protocolos

En los campos de dirección IP y puertos origen y destino, se debe colocar los valores que se desee para que se dispare la alerta. Se acepta el valor de “any” para que acepte todos los valores y variables predefinidas por el usuario.

El campo de dirección indica el flujo del dato desde el origen hacia el destino. Este puede ser configurado con las siguientes dos opciones:

- Unidireccional.- La dirección IP y puerto de la izquierda son el origen y la dirección IP y puerto de la derecha son el destino. La nomenclatura utilizada es “->” (guion medio seguido de mayor que).
- Bidireccional.- Esto generará que el evento se disparé con cualquier flujo de datos que involucre las direcciones IP y puertos especificados. La nomenclatura utilizada es “<>” (menor que seguido de mayor que).

La sección de opciones de la regla es donde la misma se vuelve eficiente, provee la capacidad de detectar actividad específica y flexibilidad en la generación de reglas. Cada opción se compone de una palabra clave que indica la opción que

se va a utilizar seguido del símbolo “:” (dos puntos) y el valor que se va a configurar en la opción.

Las palabras claves para configurar las opciones son las siguientes: ([24] The Snort Project, 2013)

- msg.- es el mensaje que se va a mostrar al momento de generar una alerta.
- sid.- es un número que identifica todas las reglas de snort. Entre 0 y 99 están reservados para uso futuro, entre 100 y 1000000 están reservados para reglas de distribución oficial de Snort y a partir de 1000001 se pueden utilizar para reglas personalizadas por los usuarios.
- logto.- indica que debe crear un log en un archivo o base de datos específica.
- minfrag.- configura un umbral del mínimo de tamaño de fragmentación de un paquete.
- dsize.- configura el tamaño que debe tener la carga útil del paquete. Se puede utilizar los símbolo de mayor y menor que.
- content.- busca un patrón determinado dentro de la carga útil del paquete.
- flags.- busca por determinadas banderas TCP configuradas en determinados valores.
- seq.- busca un número de secuencia TCP específico.
- ack.- busca el campo de acknowledge dentro de la cabecera TCP.
- itype.- busca el campo ICMP type dentro del paquete.
- icode.- busca el campo ICMP code dentro del paquete.
- session.- vuelca la información de la capa de aplicación de determinadas sesiones, utilizado para mostrar información como usuarios, contraseñas, comandos, etc.
- offset.- modificador de la opción “content”, configura un desfase para la búsqueda de un patrón específico.
- depth.- modificador de la opción “content”, configura un valor de profundidad (ubicación máxima) para la búsqueda de un patrón específico.
- ttl.- busca el parámetro Time-To-Live en la cabecera del paquete.
- id.- busca el campo de ID en la cabecera del paquete IP.
- ipopts.- busca determinadas opciones IP dentro de la cabecera IP. Las opciones más utilizadas son:

  - Record Route (rr)
  - Time Stamps (ts)
  - Loose Source Routing (lssr)
  - Strict Source Routing (ssrr)
- pcre.- permite a los usuarios utilizar expresiones regulares en perl para buscar patrones dentro de la carga útil del paquete.

2.1.5.3. Ventajas y Desventajas

Ventajas:

- Es un software gratuito y de código abierto.
- Tiene gran cantidad de colaboradores alrededor del mundo.
- Es posible la creación de software adicional para mejorar la capacidad de detección de amenazas.
- Se pueden crear reglas propias.
- Proporciona bastante información para un análisis forense.

Desventajas:

- Genera gran cantidad de falsos positivos.
- Requiere bastante esfuerzo, tunning de reglas y análisis.
- No es capaz de detectar malware avanzado no basado en firmas.

2.2. SEGURIDAD EN APLICACIONES WEB

2.2.1. Definiciones dentro del entorno web

Cuando se utiliza el término entorno web, se refiere a un conjunto de herramientas que lo conforman, estas son necesarias para el desarrollo y ejecución de una aplicación web. El entorno web está formado por:

Servidor de aplicaciones: el servidor web o también llamado servidor HTTP se define como un programa informático que es el encargado de procesar las aplicaciones del lado del servidor, es decir; es el encargado de establecer comunicación con el cliente, y lo hace enviando respuestas en un lenguaje que logre ser interpretado por la aplicación. Este código que ha sido recibido normalmente es compilado y finalmente se lo ejecutará en un navegador web. Para que se realice la transmisión de datos anteriormente mencionada se utiliza el protocolo HTTP. El servidor está en la capacidad de restringir el acceso a las páginas web, haciendo que la comunicación sea únicamente para redes privadas o se puede publicar las páginas en la World Wide Web.

Aplicaciones web: Son las herramientas que el usuario final utiliza para poder acceder al servidor web, esto se lo realiza a través de internet o intranet mediante un navegador web, al cual la comunicación va codificada para que pueda ser entendida por el mismo. Una de las características que hacen que las aplicaciones web sean tan populares, es debido a la eficacia de los navegadores web, ya que son clientes que se instalan en el sistema operativo, en cualquier plataforma, y que se actualizan constantemente sin poner en riesgo las aplicaciones web.

Navegador: El navegador es una aplicación que opera a través de Internet, interpreta la información proveniente de sitios web o de archivos para que estos puedan ser leídos por el usuario final. Su principal característica es que permite observar documentos de texto a través de herramientas inmersas en el navegador, estos documentos son normalmente llamados páginas web, tienen hipervínculos,

los cuales le permiten enlazar parte de un texto hacia otros documentos. Este seguimiento de enlaces se denomina navegación.

Word Wide Web: Es la red informática mundial, normalmente conocida por sus siglas WWW, es una red de distribución que se basa en hipertexto el cual es accesible a través de internet.

Página Web: Es un documento o información electrónica que ha sido adaptada para el formato WWW y a la cual se puede acceder mediante un navegador. Los principales formatos en los que encontramos las páginas web son HTML o XHTML. Las páginas web pueden estar almacenadas en un servidor web o en un equipo local. En ellas podemos encontrar otros elementos como hojas de estilos, scripts e imágenes lo cual las hace amigable al usuario, ya que permiten una información activa entre el usuario y la información que la página contiene.

Trafico web: Se define como la cantidad de tráfico que es recibido y enviado en la red, al ser visitado un sitio web. El tráfico se determina por la cantidad de usuarios y por la actividad que tengan los mismos al visitar diversas páginas.

Sitio Web: Es una recopilación de páginas web las cuales tratan de un tema en común y se alojan en un dominio de Internet. Todos los sitios web se encuentran en la Word Wide Web y forman una gran red que se expande a nivel mundial. Para acceder a los sitios web se necesita una URL, posteriormente se ingresará a una primera página llamada portada, en la misma se puede ver un conjunto de elementos entre los cuales están los hiperenlaces que son los que dirigirán al usuario a otras páginas del mismo sitio.

Alojamiento Web: También conocido como web hosting, el cual es un servicio para almacenar información de los usuarios en Internet. Es el lugar que ocupa dentro de un servidor cualquier contenido que sea accesible vía web, como por ejemplo sitios web, documentos, páginas web entre otras, generalmente un servidor aloja varias aplicaciones web.

2.2.2. Importancia de proteger las aplicaciones web.

Todas las aplicaciones empresariales son de gran importancia ya que poseen datos sensibles, tanto de usuarios como de clientes y proyectos, por lo que se encuentran amenazados con ser atacados por virus, hackers y hasta posibles competidores que se encuentran interesados en obtener dicha información. Cuando el servicio logra ser vulnerado, la empresa pierde credibilidad y por lo tanto clientes, ya que nadie confiará en una organización que entregue servicios que pueden ser vulnerados fácilmente poniendo en riesgo la información de su cartera de clientes, por lo que toda empresa que entregue servicios en línea debe proteger las aplicaciones web, buscando siempre la manera más rentable de hacerlo y sobre todo que abarque todas sus necesidades de protección.

Es necesario que las organizaciones tomen ventaja de los hackers, realizando periódicamente pruebas de vulnerabilidades de manera que puedan encontrar brechas de seguridad y al mismo tiempo logren corregirlas antes de recibir un ataque por parte de alguien que conozca de estas debilidades, estas correcciones son los llamados parches, la cual es una tarea que está a cargo del equipo de TI (Tecnologías de la Información) de cada empresa.

Las aplicaciones web dependen de algunos componentes de software como: sistema operativo, servidor web y bases de datos, por lo que en las pruebas de penetración es necesario analizar estos elementos.

Las empresas deben contar con herramientas para proteger sus sitios web, o a la vez contratar a personal especializado para que realice un análisis exhaustivo, ya que así no solo protegen aplicaciones sino que también están al día con las normas que rigen la seguridad en aplicaciones web, especialmente en la actualidad, donde las empresas están migrando a aplicaciones basadas en web para una mejor funcionalidad.

A nivel mundial han incrementado las normativas gubernamentales las cuales día a día son más estrictas, por lo que proteger las aplicaciones web ya no es una

opción sino una obligación para las empresas que manipulan datos confidenciales de sus clientes

Se debe implementar fuertes medidas de seguridad en las comunicaciones HTTP, HTTPS y FTP ya que son el punto más vulnerable en la infraestructura de la red, siendo el blanco perfecto, las aplicaciones web públicas hacia Internet. Cuando un hacker logra ingresar a la red interna no solo busca la información personal de los usuarios sino que también busca atacar otros servidores internos.

Cuando el equipo de TI realiza los parches de seguridad, se interrumpen momentáneamente las operaciones normales, aunque con esto no necesariamente se puede asegurar que el sistema está totalmente protegido contra ataques como: SQL Inyection, XSS (Cross Site Scriptting), DoS (denegación de servicio), desbordamiento de búffer, manipulación de parámetros, envenenamiento de cookies entre otros.

Los firewall de red y los sistemas de prevención de intrusos trabajan en la capa 3 y 4 del modelo OSI (red y transporte), mientras que las aplicaciones web trabajan en la capa 7 (aplicación), es por esto que se inventó y se volvió necesario el Web Application Firewall (WAF), el cual está especializado en comprender la aplicación y bloquear intentos de explotación de vulnerabilidades a pesar de que la misma exista.

2.2.3. Firewall de aplicaciones web (ModSecurity)

2.2.3.1. Introducción

Es un firewall de aplicaciones web open source, encargado de prevenir ataques contra aplicaciones web, funciona de manera integrada con el servidor web. Es un sistema de detección de intrusos pero trabaja a nivel de HTTP, esto le permite hacer cosas que son difíciles en un IDS clásico, la función de prevención de ataques se interpone entre el cliente y el servidor, si encuentra una carga maliciosa, puede rechazar la solicitud.

Permite observar el tráfico de la web en tiempo real. Este punto es muy importante para el tema de seguridad, ya que tiene la capacidad de ver el tráfico HTTP el cual puede ser grabado en caso de que sea necesario para poder reaccionar ante los eventos encontrados.

Una de las características principales de ModSecurity es que todas las acciones que toma, lo hace sin tocar las aplicaciones web, esto se puede hacer con cualquier aplicación, incluso si no se tiene acceso al código fuente.

Cada día se van realizando más ataques sobre el protocolo HTTP, por lo cual se da la necesidad de tener herramientas que lleven la seguridad a otros niveles. Las herramientas comunes trabajan sobre TCP/IP, por lo que no pueden obtener detalles del protocolo HTTP, por lo que se utiliza ModSecurity para crear pasarelas de aplicación.

Estas son sus principales características: ([25] Mischel, 2009)

- Las solicitudes entrantes son analizadas a medida que van llegando, y pueden ser filtradas antes que lleguen al servidor web.
- Se utilizan técnicas anti evasión, las rutas y parámetros se normalizan antes de que sean analizados.
- Tiene la capacidad de entender el protocolo HTTP, con lo que se puede realizar filtrado de manera granulada. Por lo que se puede llegar a ver los valores de cookies.
- Se puede interceptar los contenidos transmitidos por medio del método POST.
- Todos los detalles de las solicitudes realizadas se pueden registrar para un análisis forense posterior.
- Filtrado HTTPS; se puede tener acceso a los datos requeridos una vez que hayan sido descifrados.
- Filtrado de contenido comprimido; el motor de seguridad tendrá acceso una vez que se realice la descomprensión de los datos.

2.2.3.2. Funcionamiento Interno

ModSecurity realiza un monitoreo en tiempo real las aplicaciones web. Sin embargo no tiene un conjunto de reglas fijas, por lo que depende de cada administrador elegir las funcionalidades que va a entregar ModSecurity, esta es una de sus principales características al ser de código abierto.

Cuando la aplicación permite un libre acceso al código, se da una gran facilidad al administrador para personalizar ModSecurity de manera que la herramienta se ajuste a las necesidades de cada usuario.

Estos son los principales contextos de uso de ModSecurity:

Monitoreo y control de acceso a las aplicaciones en tiempo real.

ModSecurity da acceso al tráfico HTTP en tiempo real, además tiene la capacidad de inspeccionar dicho tráfico, rastreando los elementos del sistema y realizando una correlación de los eventos recibidos.

Parches Virtuales.- Es la mitigación que se realiza a la vulnerabilidad encontrada, esto se lo realiza en un capa separada de manera que la aplicación real no es intervenida en ningún momento, de esta manera se logra solucionar los problemas encontrados. Estos parches son aplicables para cualquier protocolo de comunicación, aunque es principalmente utilizado con HTTP.

Registro completo de tráfico HTTP.- ModSecurity tiene la capacidad de registrar todo lo que se necesita, lo cual es primordial para un posterior análisis forense. Además se puede escoger cuales son las transacciones web que se registren, que partes de las transacciones podrán ingresar al sistema y cuáles serán desinfectadas.

Evaluación continua de seguridad pasiva.- Se realiza constantemente un análisis de seguridad, de manera que se realiza un ataque simulado para evaluar en tiempo real cualquier variación en el monitoreo del tráfico, se basa en el

comportamiento del sistema para detectar cualquier anomalía y cualquier deficiencia de seguridad antes de que sean explotados.

Hardening de aplicaciones web.- Una de las características de ModSecurity es la reducción de la superficie de ataque, en donde se puede reducir de manera selectiva las características del tráfico HTTP que se desea aceptar, como por ejemplo métodos de petición, encabezados de solicitudes, tipos de contenidos que se van a recibir, etc. ModSecurity permitirá realizar este tipo de restricciones, puede ser de manera directa o trabajando en conjunto con otros módulos de apache.

2.2.3.3. Registro de transacciones http

Es importante conocer los efectos que va a tener ModSecurity sobre el servicio web. Un firewall de aplicaciones web como ModSecurity permite observar el comportamiento interno de una petición HTTP, además de observar el tiempo de procesamiento cuando se realiza una descarga de una página web, así se puede observar cualquier tiempo extra que se genere al realizar una solicitud.

Cuando un usuario visita una página web, el navegador se conectará al servidor donde se descarga el archivo solicitado por el usuario; generalmente un archivo html. Posterior a esto se analiza el archivo descargado de manera que se puedan descubrir archivos adicionales dentro de él, como imágenes o líneas de comando. La siguiente secuencia de eventos ocurre para cada archivo: ([26] Ristic, 2012)

- Conectar con el servidor web.
- Solicitar el archivo requerido.
- Esperar por el servidor para realizar la entrega del archivo.
- Descargar el archivo.

Cada uno de estos pasos agrega retrasos o latencia en la comunicación. Normalmente el tiempo que se demora en realizar una descarga está en el orden de cientos de milisegundos por medio de un cable DSL. Esta latencia puede variar dependiendo de la velocidad de la conexión y de la distancia existente entre el cliente y el servidor.

ModSecurity va a aumentar el uso de memoria de Apache, por lo que Apache generará un nuevo proceso para cada conexión activa al servidor. Es decir que el número de instancias de Apache aumentará o disminuirá en función de las conexiones del cliente al servidor.

2.2.3.4. Ventajas y desventajas.

Ventajas:

- ModSecurity permite a los desarrolladores y administradores proteger sus servicios web sin necesidad de realizar modificaciones en el código fuente de las aplicaciones, es decir; se puede implementar defensa adicional sin necesidad de tener numerosas líneas de código.
- Tiene la capacidad de inspeccionar el lenguaje SSL ya que puede desencriptarlo para su análisis.
- Fácil instalación.
- Realiza correlación de los datos y alertas, ya que las peticiones HTTP pasan por el servidor proxy.
- Filtrado simple
- Validación de codificación URL.
- Permite realizar auditorías.
- Prevención de ataques de byte nulo.
- Enmascara la identidad del servidor.

Desventajas:

- No puede detectar ataques de día cero.
- Se demora en obtener nuevas actualizaciones de firmas.
- Disminuye la capacidad de los servidores por lo tanto también disminuye la capacidad de las aplicaciones.
- Es necesario tener una buena base de conocimiento para lograr entender los ataques que están intentando ingresar a la red, con el fin de poder crear reglas para mitigar estos riesgos.

- La configuración se la realiza de manera manual, pues la versión gratuita de ModSecurity no incluye soporte, por lo que las actualizaciones necesitarán un mantenimiento constante.

2.3. ANALISIS DE MALWARE BASADO EN COMPORTAMIENTO

2.3.1. Introducción

Identificar malware basado en comportamiento es un complemento obligatorio a los sistemas de protección basados en firmas ya que son dos sistemas totalmente diferentes. Los sistemas basados en firmas se encargan de investigar el ataque como tal para posteriormente comprender la matriz del mismo y poder identificar a ese ataque en específico, en cambio los sistemas de detección de amenazas basado en comportamiento se encargan de realizar un monitoreo en tiempo real del tráfico del equipo y tienen la capacidad de identificar los comportamientos típicos maliciosos.

Es muy difícil que un sistema que detecta malware basado en comportamiento le pueda poner un nombre al mismo, este tipo de sistemas lo que hacen es proveer un perfil del huésped infectado listado todas las acciones sospechosas que demuestran un comportamiento malicioso.

Hoy en día se incorporan estos sistemas de detección y bloqueo basados en el comportamiento como parte de una estrategia de protección global.

2.3.2. Herramientas que permiten analizar malware basado en comportamiento.

Varias empresas están realizando esfuerzos investigativos para encontrar nuevas formas de detectar ataques dejando de lado el sistema de creación de firmas. Realmente hay muchos sistemas y teorías por lo que es difícil catalogarlos, sin embargo, entre los más conocidos están los siguientes:

- Tecnologías basadas en sandbox

- Tecnologías especializadas en procesos y registros a nivel de host
- Tecnologías basadas en patrones a nivel de red
- Tecnologías basadas en investigación de vulnerabilidades

Las principales herramientas basadas en sandbox las tienen FireEye y Palo Alto Networks, estas tecnologías consisten en ejecutar los archivos en diferentes ambientes virtuales con diferentes técnicas de detección para definir su comportamiento benigno o malicioso.

Existen varias herramientas (por lo general software) que se encargan de monitorear a tiempo real actividades en dispositivos de usuarios finales, aplicaciones y servidores de manera que puedan permitir o bloquear la ejecución de aplicaciones o de acciones específicas sospechosas como cambios de registros, acceso a directorios sensibles, descarga de archivos, etc. Una herramienta gratuita que permite un análisis con este tipo de tecnología es ThreatFire y también existen herramientas pagadas que se encargan de dar protección a nivel empresarial como es Bit9.

Las herramientas basadas en patrones a nivel de red se colocan a nivel perimetral o en sectores específicos de la red y buscan diferentes acciones comunes como callbacks, descargas de ejecutables, conexiones a URL maliciosas, etc. Las principales herramientas que permite este tipo de análisis son FireEye y BotHunter (código abierto).

Las herramientas basadas en investigación de vulnerabilidades tienen equipos sofisticados que buscan vulnerabilidades y cuando las detectan son capaces de crear “parches virtuales” que lo que buscan es patrones de comportamiento que intenten explotar esta vulnerabilidad y en cuanto detectan este tipo de tráfico son capaces de desechas estos paquetes. Por lo general estas suelen ser características de diferentes sistemas de protección, los más conocidos que son capaces de hacer este tipo de análisis son: Tipping Point (IPS), McAfee (IPS), SourceFire (IPS) e Imperva (WAF)

2.3.3. BotHunter

2.3.3.1. Introducción.

Esta es una nueva estrategia para vigilancia del perímetro de la red, la cual se basa en el reconocimiento del diálogo existente durante una infección exitosa. BotHunter está diseñado para dar un seguimiento en la comunicación entrante y saliente entre los activos internos y la red, se realiza un rastreo del intercambio de datos detectando las etapas específicas del proceso de infección.

Para declarar a cierto diálogo como un bot, se utiliza el motor de correlación de diálogo de BotHunter, el cual se encarga de analizar los flujos de comunicación que son intercambiados entre el host interno y o más entidades externas, como son escaneo del destino, ejecución de un exploit, descarga de un binario de malware, comunicación con el Servidor de Command & Control y escaneo de salida. Vale la pena acotar que no es necesario que se ejecuten todos estos pasos para que se pueda declarar la presencia de un bot en el sistema, el sistema de correlación de diálogo recoge un rastro de evidencia buscando una combinación de secuencias para dar la respuesta final. ([27] Guofei Gu, 2007)

BotHunter es un sistema que se enfoca principalmente en la detección de bots y botnets, realiza análisis en tiempo real además de detectar la fuente de donde ha sido descargado el binario y del servidor de Command & Control de manera que ayudará a restringir los accesos de los usuarios.

2.3.3.2. Funcionamiento Interno.

Durante el ciclo de vida der una infección se puede dar las siguientes fases: ([28] Phillip Porras, 2012)

- Escaneo del objetivo.
- Infección mediante un exploit.
- Descarga y ejecución de un binario de malware.
- Comunicación con el servidor Command & Control (C&C).

- Escaneo hacia el exterior en busca de nuevas víctimas.

Se debe tomar en cuenta que para que BotHunter lo considere como una actividad de bot no necesariamente deben darse todas estas fases en su totalidad y tampoco en un determinado orden.

Una infección es vista como un conjunto de participantes basándose en una determinada secuencia como se muestra a continuación.

"Infección I = < A,V,C,V',E,D >" ([27] Guofei Gu, 2007)

Donde:
A = Atacante.
V = Víctima.
E = Descarga de Binario
C = Comunicación con el servidor C&C
V' = Siguiente víctima.
D = Diálogo de la infección compuesto de flujos bidireccionales, el cual está compuesto por las siguientes transacciones:

- E1: Escaneo realizado desde un elemento del exterior hacia uno de la red interna.
- E2: Exploit inyectado desde un elemento del exterior hacia un elemento interno.
- E3: Descarga de un binario de malware de un elemento interno desde un elemento ubicado en el exterior.
- E4: Comunicación con el servidor de Command & Control por parte de un elemento del interior.
- E5: Escaneo de un elemento de la red interna en busca de nuevas víctimas.

En el proceso de infección (ver Figura. 2.24.) de muestra la fase de reconocimiento, es decir como el atacante realiza un escaneo hacia la víctima (E1), posteriormente se ejecutan exploits hacia la máquina víctima (E2) con lo cual esta buscará realizar la descarga de un binario malicioso (E3). En este punto pueden suceder dos cosas:

- Se realiza un escaneo en busca de nuevas víctimas (E5).
- Se establece comunicación con el servidor Command & Control (E4), para posteriormente buscar nuevas víctimas (E5).

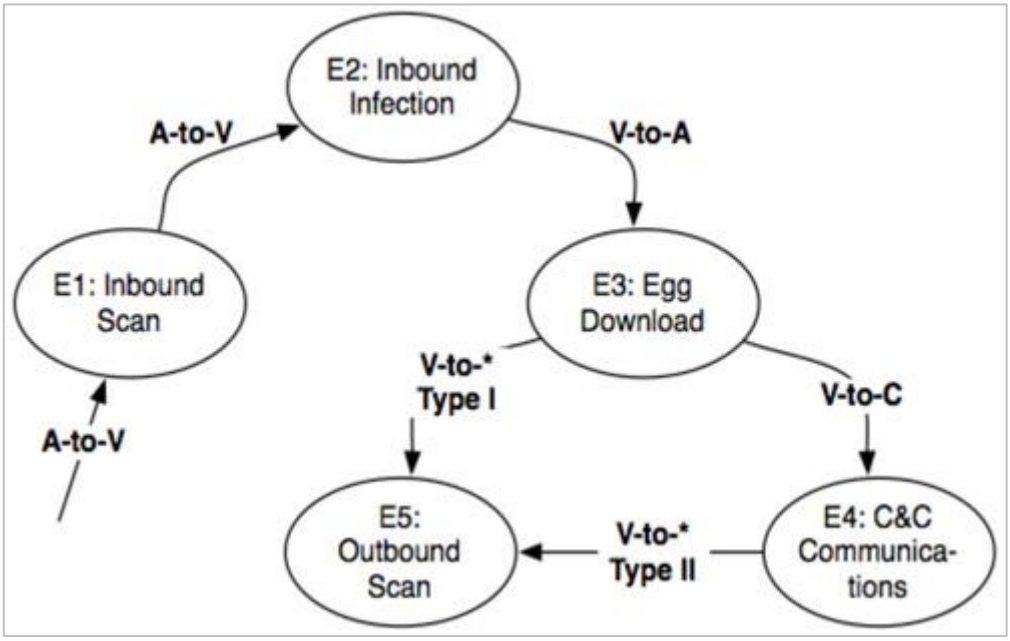


Figura. 2.24. Ciclo de vida de una infección ([28] Phillip Porras, 2012)

El correlador de BotHunter está basado en el IDS Snort del cual se han modificado un conjunto de reglas enfocadas en malware para que pueda ser utilizado por BotHunter, además se han aumentado dos plugins llamados SCADE (Statistical sCan Anomaly Detection Engine o Analizador de escaneo de puertos tanto de entrada como de salida) y SLADE (Statistical PayLoad Anomaly Detection Engine o Analizador de flujos de tráfico), que analizan el flujo de tráfico.

2.3.3.3. Arquitectura

Dentro de BotHunter existen tres fuentes (ver Figura. 2.25.) de las cuales se obtienen los diferentes mensajes, se puede observar que del plugin SLADE obtenemos mensajes del tipo E2 (Inyección de exploit), del plugin SCADE se obtienen salidas del tipo E1 y E5 (Escaneo del exterior al interior y escaneo en búsqueda de nuevas víctimas), mientras que de las reglas de Snort basadas en malware encontramos salidas del tipo E2, E3 y E4 (Exploits, descarga de binarios, comunicación con servidor C&C). Una vez que todos estos datos son obtenidos

durante el escaneo pasan al correlador de BotHunter, el cual utiliza una matriz que en donde cada una de las entradas corresponde a un elemento que ha generado una actividad, y finalmente se obtienen los eventos encontrados. ([28] Phillip Porras, 2012)

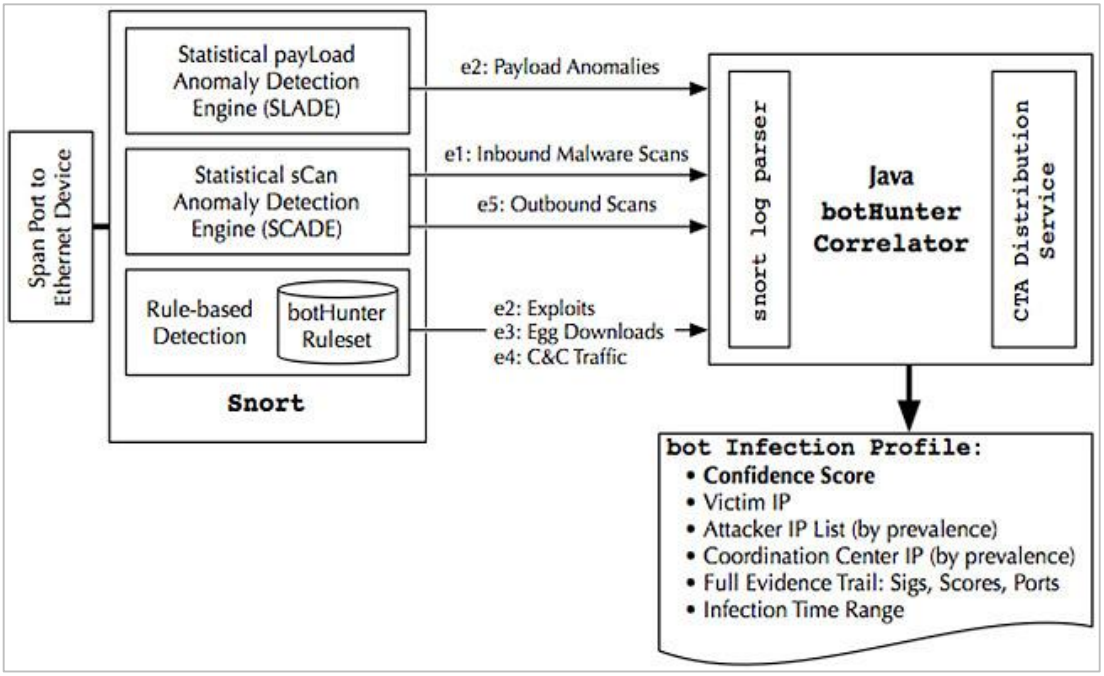


Figura. 2.25. Arquitectura de BotHunter ([28] Phillip Porras, 2012)

2.3.3.4. Ventajas y desventajas.

Ventajas:

- Es un software gratuito al cual se puede tener acceso desde el sitio oficial de BotHunter.
- Está disponible para varias plataformas (Windows, Linux, FreeBSD, Mac OS) en sus diferentes distribuciones.
- Es un sistema que no se basa en firmas sino en comportamiento.
- Ayuda a detectar si los sistemas están formando parte de botnets.
- Genera pocos falsos negativos.
- Se pueden detectar las etapas de infección del malware.
- Su configuración es bastante sencilla e intuitiva para los usuarios.

- Además de incorporar un amplio conjunto de firmas al motor de Snort, incorpora dos plugins que complementan el funcionamiento de Snort para dar una secuencia válida del ciclo de malware.
- Toma ventaja en relación de los IDS ya que por medio del plugin SLADE se optimiza la utilización de recursos y el tiempo de ejecución es más corto.

Desventajas:

- Requiere realizar un análisis exhaustivo de los resultados para llegar a conclusiones finales
- Entrega gran cantidad de falsos positivos
- No se puede tomar acción sobre el malware que intenta ingresar al equipo víctima.

2.3.4. Honeypot KFsensor

2.3.4.1. Introducción

La creciente cantidad y diversidad del tráfico de red ha ocasionado que dispositivos como los IDS entreguen una gran cantidad de falsos positivos, lo cual aumenta la cantidad de datos a analizar significando pérdida de tiempo y dinero para las organizaciones.

Además los IDS, al basarse en firmas conocidas para detectar los ataques, son totalmente incapaces de reconocer amenazas nuevas y a su vez no reconocen ataques que llevan mensajes encriptados permitiendo el paso de los mismos al interior de la red. Por lo cual es necesario un nuevo enfoque con una nueva herramienta que analice lo que otros dispositivos dejan pasar.

Un honeypot es un sistema que simula ser un servidor en la red vulnerable y se lo pone en la red de manera que pueda ser sondeado y atacado y así se pueda obtener información del atacante. KFsensor es un enfoque diferente en seguridad pero bastante eficaz en la detección de ataques.

Al permitir que el atacante ingrese al sistema del honeypot, se pueden observar todas las técnicas y herramientas manejadas para ingresar al sistema, y como normalmente nadie debería acceder a este sistema (ya que no es real), la cantidad de falsos positivos que se presentan con KFsensor son bastante bajos en relación con otras herramientas.

KFsensor es un Honeypot de mediana interacción que se ejecuta bajo Windows y permite simular servicios vulnerables, escuchar el tráfico de red y además interactuar con servicios o aplicaciones instalados en el sistema operativo. Adicionalmente, posee las siguientes características:

- Permite la identificación de ataques basadas en firmas de Snort.
- Permite enviar alertas vía Syslog CEF.
- Permite enviar alertas vía Email.
- Posee mecanismos de protección contra ataques de denegación de servicio.
- Almacena los eventos en una base de datos MySQL.

2.3.4.2. Funcionamiento interno

KFsensor es fácil de instalar y configurar, no requiere de especificaciones de hardware especiales y funciona sin problema en cualquier máquina con sistema operativo Windows. Dependiendo de la necesidad de la empresa, se deben cargar los principales servicios pero no es necesario editar archivos de configuración, y tiene una interfaz sencilla de Windows que controla todas las funcionalidades.

KFsensor trabaja simulando servicios de un sistema operativo, en la capa más alta del modelo OSI; la capa de aplicación, lo cual permite que pueda hacer uso de los mecanismos de seguridad propios de Windows, de manera que se disminuya el riesgo de ser descubierto y al mismo tiempo impedirá la introducción de controladores adicionales al sistema original. Un equipo que está ejecutando KFsensor puede ser visto y tratado como cualquier otro servidor en la red, y sin necesidad de realizar cambios complejos en routers y firewalls.

KFsensor es un honeypot híbrido, lo que quiere decir que puede implementar tanto servicios simulados (programados por KFSensor) como servicios nativos

(instalados y configurados por el usuario), lo que permite dar un ambiente mucho más maduro y real.

El lugar óptimo es colocar el servidor KFSensor dentro de la DMZ o dentro de la zona de servidores internos, justamente para que se lo vea como un servidor más dentro de la red (ver Figura. 2.26.).

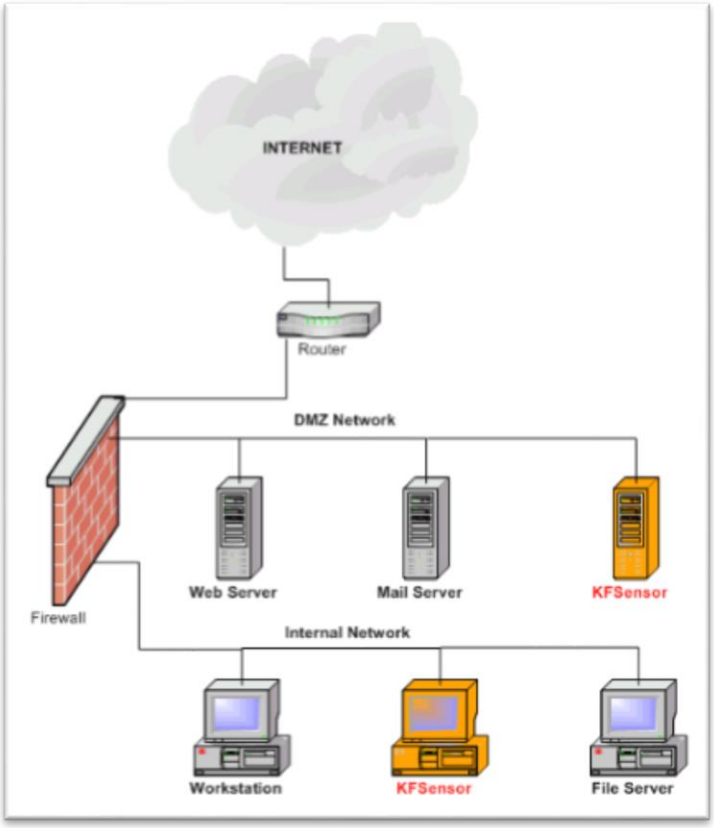


Figura. 2.26. Ubicación de KFSensor dentro de la red ([29] Keyfocus Ltda., 2013)

KFsensor es totalmente útil desde que empieza su funcionamiento, pues proporciona datos acerca del tipo de ataques a la red y la continuidad con que estos suceden. Al unir todo el tráfico de red como un ataque, KFsensor genera una alerta que nos indicará el proceso de la amenaza, es así como es fácil de entender para personal no especializado.

KFsensor puede ser utilizado para redefinir o afinar reglas del firewall según los resultados obtenidos, además se pueden crear nuevas reglas para los sistemas

de detección de intrusos en la red. Por lo que se puede decir que KFsensor es un sistema muy rentable para mejorar la infraestructura de la red.

Se basa en un demonio de Internet, el cual está diseñado para manejar varias direcciones IP y puertos, además ha sido diseñado para soportar ataque de denegación de servicio y de desbordamiento de búfer.

El sistema interno de KFsensor puede trabajar de múltiples maneras, desde un funcionamiento bastante simple como sería un puerto de escucha, hasta un funcionamiento tan complejo que puede simular un sistema completo con los servicios estándar.

En cuanto al protocolo HTTP, KFsensor es capaz de simular con precisión la forma en que IIS responde a las solicitudes tanto válidas como inválidas, además puede alojar un sitio web que puede manejar solicitudes más complejas como negociaciones caché y solicitudes de intervalo. Por lo que hace para el atacante una tarea difícil el identificar que KFsensor es un honeypot.

Cada byte generado en un ataque es almacenado en los registros de KFsensor, los eventos pueden ser diferenciados según su nivel de gravedad por medio de un código de colores, de manera pueda ser detectado cualquier intento de intrusión o comportamiento inusual en el servidor. Con KFsensor se pueden crear informes personalizados, así se podrán realizar filtros para mostrar únicamente la información de determinados puertos, protocolos o direcciones IP. ([29] Keyfocus Ltda., 2013)

2.3.4.3. Ventajas y desventajas

Ventajas:

- Realiza la detección de intrusos basado en Honeypot.
- Detecciones en tiempo real.
- Puede detectar amenazas desconocidas.
- Es eficaz ante amenazas internas y externas.
- Es fácil de usar.
- Se puede configurar según los requerimientos del usuario.
- Emula eficazmente a un servidor.
- Realiza un registro detallado de todas las transacciones.
- Muy bajo número de falsos positivos.
- Se complementa con Snort para trabajar con sus reglas.

Desventajas:

- No sirve para eliminar o corregir fallas de inseguridad.
- Aunque genera patrones para un IDS no es capaz de reemplazarlo.
- Si la red posee vulnerabilidades, instalar un Honeypot no ayudará a mitigar estas fallas.
- No evitará que un atacante intente ingresar a la red.

CAPÍTULO III

ANÁLISIS Y CORRECCIÓN DE VULNERABILIDADES

3.1. INTRODUCCIÓN

El reto de toda empresa es poder mantener su red segura, de manera que esta pueda estar abierta e interconectada para facilitar el intercambio de la información entre los clientes, proveedores y socios del negocio a nivel mundial.

Desafortunadamente al hacer que toda la información se encuentre disponible, también se abre una brecha de seguridad en donde virus, gusanos y otros riesgos de seguridad amenazan constantemente con robar la información e interrumpir las comunicaciones.

Una vulnerabilidad es un agujero existente en los sistemas, estas vulnerabilidades permiten violar la seguridad dentro de la red. El creciente número de vulnerabilidades creadas diariamente hacen que su eliminación sea un desafío mucho mayor.

Las vulnerabilidades pueden existir en los enlaces, en los servidores, en los dispositivos finales e incluso en los elementos de seguridad, es decir en todos los dispositivos que formen parte de la red como tal.

Las vulnerabilidades han afectado a los sistemas operativos y aplicaciones desde los primeros días de la computación. La conectividad universal ha proporcionado a los hackers un fácil acceso a la red y a sus recursos informáticos, por lo que cualquier empresa es susceptible si las vulnerabilidades no son identificadas y corregidas.

Existen diversas etapas en el desarrollo de las vulnerabilidades, inicialmente cuando se lanza al mercado un producto, este viene con brechas de seguridad, las cuales pueden ser defectos de diseño, implementación o gestión. Algunos de estos errores pueden convertirse en riesgos para la seguridad pues podrían ser utilizados para tener un acceso no autorizado, denegación de servicio u otras acciones que podrían poner en riesgo la seguridad del sistema.

La siguiente etapa se da una vez que se ha descubierto la existencia de la vulnerabilidad, y se determinan los defectos causados por la misma. Posteriormente viene la fase de divulgación, la cual puede ser pública, de manera que todo el mundo conozca la existencia de dicha vulnerabilidad, o se la puede dar a conocer entre hackers y así puedan explotar este agujero de seguridad.

A continuación se da la creación de parches de seguridad, los cuales son creados por quien lanzó el producto al mercado, donde se buscará remediar la vulnerabilidad.

Para un criminal cibernético, las vulnerabilidades en una red son activos que se encuentran normalmente ocultos, pero que son considerados altamente valiosos. Por lo que al ser expuestos pueden provocar: ingreso no autorizado a la red, exposición de información confidencial, robo de credenciales, infracción de políticas de seguridad, etc.

Dentro de una organización se busca proteger los activos, es decir todos los recursos que forman parte de la red y a los cuales se tiene acceso constante por parte del personal. Los recursos se encuentran agrupados en:

- Hardware.- son los elementos físicos que se encuentran dentro del sistema, como son los procesadores, y medios de almacenamiento.
- Software.- dentro de este grupo se encuentran los programas que se ejecutan sobre el hardware, entre estos están las aplicaciones que el usuario ejecuta.
- Datos.- entre estos está la información de los usuarios, como son bases de datos o información que viaja por la red.

- Otros.- dentro de este grupo se encuentra el material utilizado, y el personal de la organización.

El recurso más crítico dentro de la red son los datos. Ya que los otros activos pueden ser repuestos fácilmente en caso de ser dañados, mientras que recuperar los datos es una tarea complicada especialmente si la empresa no tiene buenas políticas de seguridad y se realizan constantemente copias de seguridad de los datos almacenados, en caso de que accidentalmente se pierda la información esta debería poder ser recuperada a su estado anterior, evitando así la pérdida innecesaria de tiempo y dinero. Es por esto que todos y cada uno de los negocios que tengan acceso a internet está en riesgo debido a las vulnerabilidades existentes en la red, sin importar si la empresa es pequeña o grande no hay diferencia; todas las organizaciones están expuestas.

Es así como se puede definir vulnerabilidad como cualquier debilidad que pueda comprometer la seguridad de la red. Las vulnerabilidades pueden se agrupadas en función de:

- Diseño.-Se da por la debilidad existente en el diseño de los protocolos utilizados en la red, y por la ineficiencia o falta de políticas de seguridad.
- Implementación.- Debido a errores de programación, causando la existencia de puertas traseras en los sistemas debido a descuidos de los fabricantes.
- Uso.- Mala configuración de los sistemas o errores de los usuarios o desarrolladores encargados del manejo de la red. Además hoy en día existen gran cantidad de herramientas que facilitan la creación de nuevos ataques.
- Vulnerabilidad de día Cero.- Son vulnerabilidades para las cuales no existe una solución conocida, por lo cual se convierte en una amenaza inminente, pues aunque no hay un procedimiento para remediarla, se conoce como explotarla.

Estas son unas de lasis principales vulnerabilidades que es posible encontrar en la red:

- Vulnerabilidad de desbordamiento de buffer.- Cuando un programa pierde la capacidad de controlar la cantidad de datos que se almacenan en el buffer, llega un momento en que esta información puede ser copiada en zonas de memoria adyacentes debido a un desbordamiento en el buffer. Cuando sucede esto, los atacantes pueden aprovechar para inyectar código malicioso que permite al atacante actuar como administrador de la red.
- Vulnerabilidad de condición de carrera (Race Condition).- Esta vulnerabilidad se produce cuando varios procesos intentan ingresar a un recurso al mismo tiempo. En este caso una variable puede cambiar su estado y obtener un valor no esperado.
- Vulnerabilidad de Cross Site Scripting (XSS).- Vulnerabilidad típica de las aplicaciones web, permite el ingreso de código en las páginas web que han sido visitadas, una aplicación típica basada en XSS en es el phishing, en donde la víctima es engañada para creer que está accediendo a un sitio verídico, pero en realidad está siendo redireccionado a otro sitio el cual normalmente es un sitio de malware, en donde puede ser almacenada la información que el usuario ingresa; como sus credenciales.
- Vulnerabilidad de denegación del servicio.- Esta vulnerabilidad ocasiona que el sistema no se encuentre disponible para los usuarios, su principal consecuencia es un consumo excesivo de ancho de banda ocasionando pérdida de conectividad de la red.
- Vulnerabilidad de ventanas engañosas (Windows Spoofing).- Principalmente se las puede encontrar como pop-ups que son ventanas que se abren de manera automática, indicando promociones o haciendo creer que el usuario es el ganador de concursos, con el único objetivo de recolectar información del usuario o del sistema de manera que el atacante puede realizar futuros ataques a partir de la información obtenida.

3.2. LAS VULNERABILIDADES DENTRO DE LA RED

Para solucionar las vulnerabilidades existentes en los enlaces se va a realizar la implementación de diferentes equipos. Sus funciones serán las siguientes:

Palo Alto Networks:

- Protección de control de aplicaciones, sistema de prevención de intrusos, filtrado de URL, bloqueo de archivos riesgosos en todos los enlaces existentes reemplazando a los actuales enrutadores.
- Visibilidad ante ataques de día cero.
- Cifrar las comunicaciones entre los diferentes firewalls.
- Proteger a los dispositivos remotos que acceden a través de la VPN

FireEye:

- Bloqueo de infiltración de ataques de día cero.
- Bloqueo de exfiltración de datos.

Snort:

- Visibilidad adicional mediante un sistema de detección de intrusos en el enlace de internet.

BotHunter:

- Visibilidad de botnets mediante el comportamiento de los dispositivos finales en el enlace hacia internet.

KFSensor:

- Protección adicional para la DMZ mediante un honeypot.

A continuación se precederá a explicar los modos de operación y configuraciones necesarias de los equipos antes mencionados.

3.2.1. Palo Alto Networks

3.2.1.1. Modos de operación

Principalmente existen 5 modos de operación en los que se puede colocar las interfaces del cortafuegos de Palo Alto Networks:

- TAP
- Virtual Wire
- Capa 2
- Capa 3
- Alta disponibilidad

El modo TAP funciona principalmente para monitoreo, aquí el equipo tiene todas las características de identificación de aplicación, usuario y contenido pero no puede tomar acciones de bloqueo ya que solo visualiza el tráfico reflejado de un segmento de la red mediante un puerto SPAN o un TAP. En este modo tampoco es capaz de descifrar tráfico.

El modo de Virtual Wire es el más sencillo para colocar el equipo en modo in-line, donde todo el tráfico para por el equipo y puede tomar acciones de bloqueo. Este también es llamado modo bridge o transparente, aquí las interfaces no tienen direcciones IP's y el tráfico simplemente entra por una interface y sale por otra haciendo lo que se conoce como un man-in-the-middle transparente.

El modo de capa 2 además de lo antes descrito permitirá la creación de VLAN's con el equipo para realizar una correcta segmentación de la red sin que requiera una gran administración.

El modo de capa 3 permitirá tener la capacidad de crear enrutadores virtuales y lograr un ambiente que soporta varios protocolos de ruteo sumamente personalizado, además permite la creación de VPN's (site-to-site y client-to-site). Para cumplir con todas las necesidades este será el modo que se utilizará en la implementación.

El modo de alta disponibilidad nos permitirá conectar a dos cortafuegos de Palo Alto Networks de manera que si uno de ellos falla no exista suspensión del servicio. Esta configuración se puede establecer en modo activo-activo (los dos equipos se dividen la carga) o activo-pasivo (un solo equipo está en funcionamiento y el otro está en modo de espera).

3.2.1.2. Creación de políticas de seguridad.

Para la creación de políticas se empezará a analizar el ambiente de red (ver Figura. 3.1.).

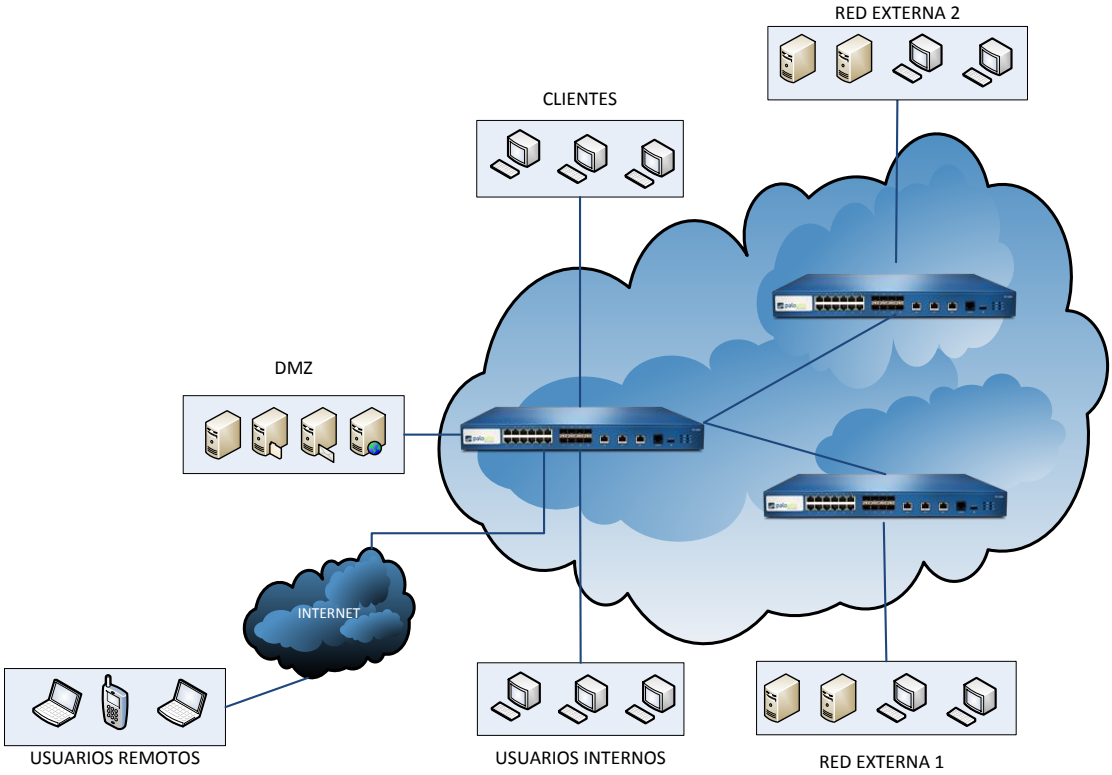


Figura. 3.1. Diagrama de red Palo Alto Networks

De acuerdo al dimensionamiento realizado se utilizará el equipo PA-200 que cuenta con las siguientes características: ([30] Palo Alto Networks, 2013)

- 100 Mbps firewall throughput
- 50 Mbps IPS throughput
- 50 Mbps IPSec VPN throughput
- 64,000 sesiones concurrentes

- 1,000 nuevas sesiones por segundo
- 25 túneles IPSec VPN
- 25 usuarios SSL VPN
- 10 zonas de seguridad
- 250 políticas de seguridad

El equipo tiene 4 interfaces de tráfico, uno de administración y uno de consola (ver Figura. 3.2.).

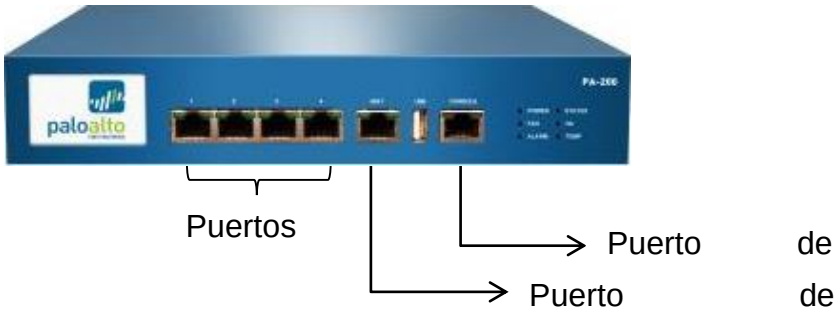


Figura. 3.2. Vista frontal PA-200 ([30] Palo Alto Networks, 2013)

Cada interface de tráfico estará asociada a una zona específica (ver Tabla. 3.1.)

#	Descripción	Detalle	Zona
1	Configuración vía consola	Console	N/A
2	Administración	Management	N/A
3	Conectado a la red interna	ethernet1/1	Egovsolutions
4	Conectado al acceso a la red de clientes externos	ethernet1/2	Clients
5	Conectado a la red WAN	ethernet1/3	Untrust
6	Conectado a la red de servidores	ethernet1/4	Servers

Tabla. 3.1. Detalle de interfaces Palo Alto Networks

Esta configuración se la realizará en la sección Network → Interfaces (ver Figura. 3.3.).

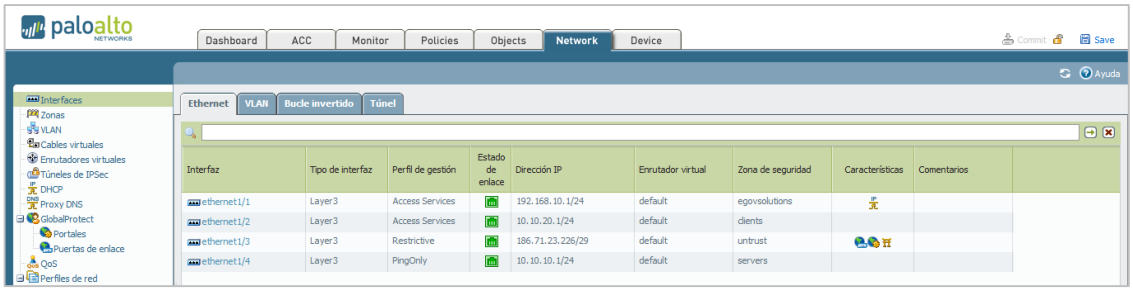


Figura. 3.3. Configuración de interfaces Palo Alto Networks

A continuación se definirán los siguientes requerimientos para la posterior creación de políticas:

- Permitir navegación segura hacia la nube por aplicaciones “no maliciosas” conocidas definidas por el administrador de la red desde las zonas egovsolutions, clients y servers
- Bloquear navegación hacia la nube por aplicaciones “maliciosas” conocidas definidas por el administrador de la red desde las zonas egovsolutions, clients y servers
- Permitir navegación segura hacia la nube por aplicaciones no categorizadas pr el administrador desde las zonas egovsolutions, clients y servers
- Permitir el ingreso de tráfico desde la nube mediante aplicaciones de enrutamiento hacia la zona e-govsolutions de manera que los equipos internos puedan acceder a VPN’s externas.
- Permitir el ingreso de tráfico de la nube a la zona sslvpn para permitir que los usuarios remotos puedan ingresar a la VPN interna.
- Permitir las solicitudes DNS desde la zona sslvpn hacia la nube para que los usuarios que se conecten a la VPN sigan teniendo acceso a internet.
- Permitir comunicación segura desde la zona egovsolutions hacia la zona servers.

Para lograr estas políticas primero es necesario definir los objetos de prevención de intrusos para lo denominado como “navegación segura”. Para esto se van a definir los siguientes objetos:

- Antivirus
- Antispyware
- Exploits de vulnerabilidades

- Filtrado de URL
- Inspección de archivos

Para antivirus se ha creado un objeto que bloquee cualquier virus que sea transmitido desde cualquier protocolo y que además realice la captura de paquete para posterior análisis (ver Figura. 3.4.).

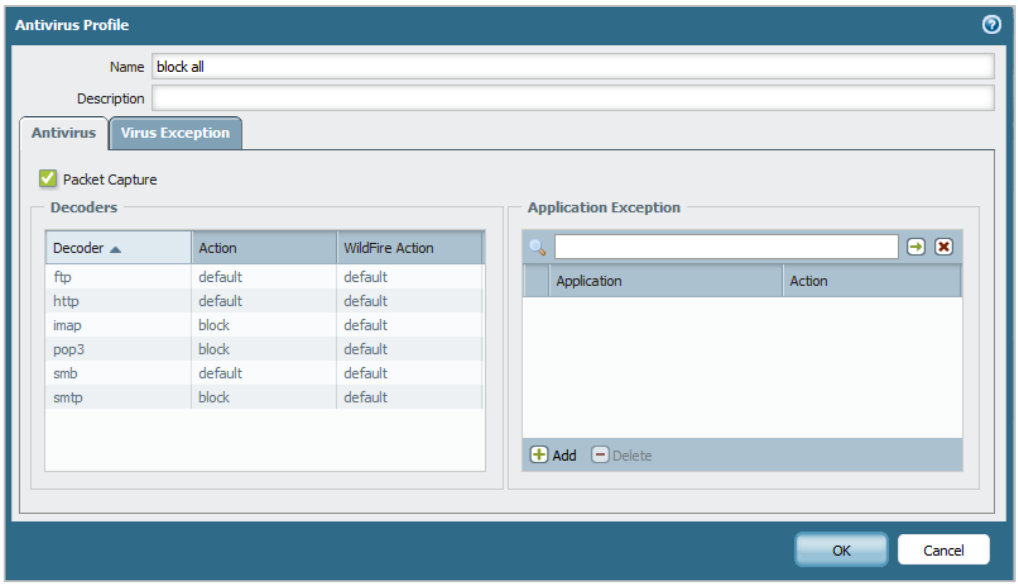


Figura. 3.4. Objeto de antivirus

Para antivirus se ha creado un objeto que bloquee cualquier spyware que sea transmitido sin importar la severidad y que además realice la captura de paquete para posterior análisis de los spyware de severidad mediana, alta o crítica (ver Figura. 3.5.).

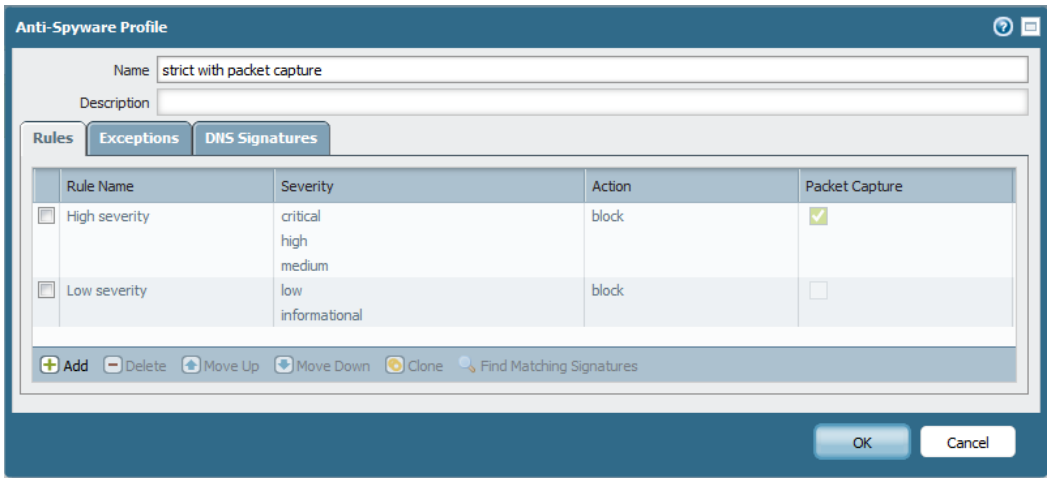


Figura. 3.5. Objeto de antispyware

Para la protección de exploits de vulnerabilidades se ha creado un objeto que bloquee cualquier intento de explotación de vulnerabilidades que sea transmitido de severidad mediana, alta o crítica realizando también la captura de paquete para posterior análisis y que además alerte cualquier intento de explotación de vulnerabilidades que sea transmitido de severidad informacional y baja (ver Figura. 3.6.).

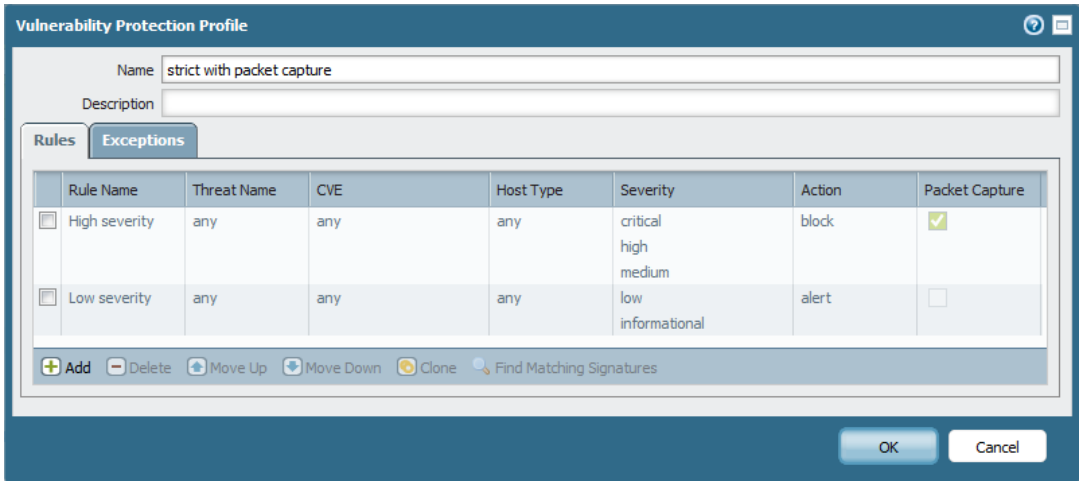


Figura. 3.6. Objeto de protección de vulnerabilidades

Para filtrado de URL se ha creado un objeto que bloquee todas las categorías de URL que no deberían ser permitidas en el ambiente empresarial y que además alerte el resto de las mismas, esto para analizar el uso de todas las categorías (ver Figura. 3.7.).

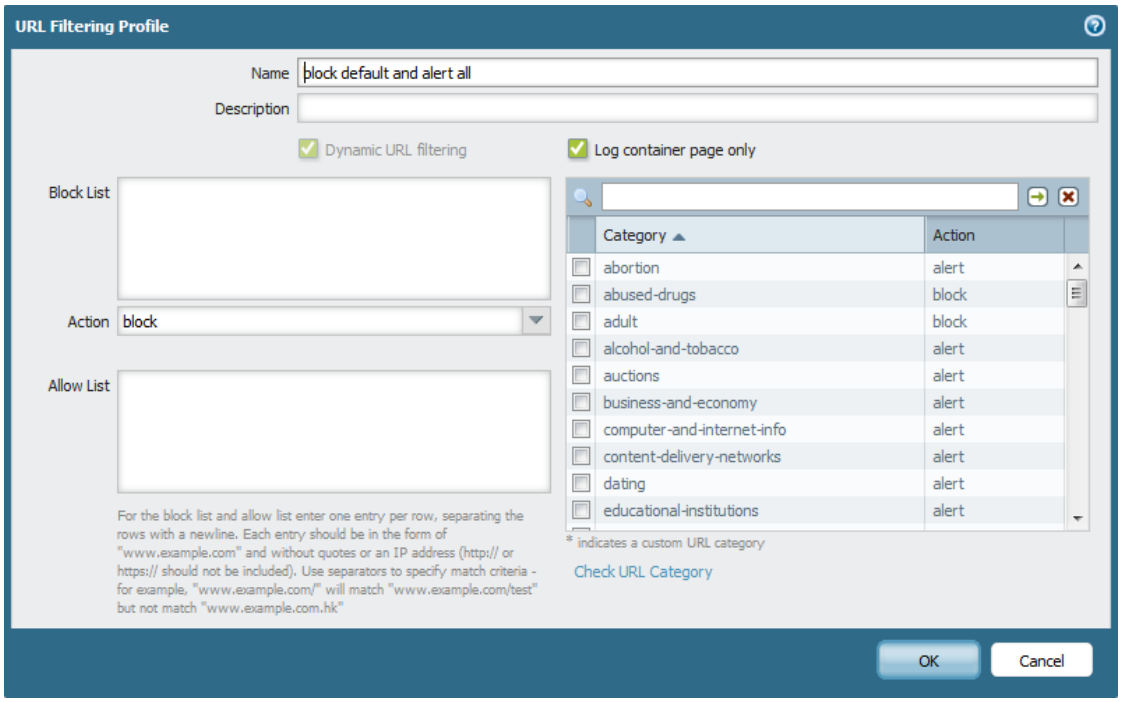


Figura. 3.7. Objeto de filtrado de URL

Para la inspección de archivos se ha creado un objeto alerte todos los archivos que son transmitidos por la red y que además tipos de archivos de alto riesgo sean enviados al análisis de la nube de Palo Alto Networks, llamado Wildfire. (ver Figura. 3.8.).

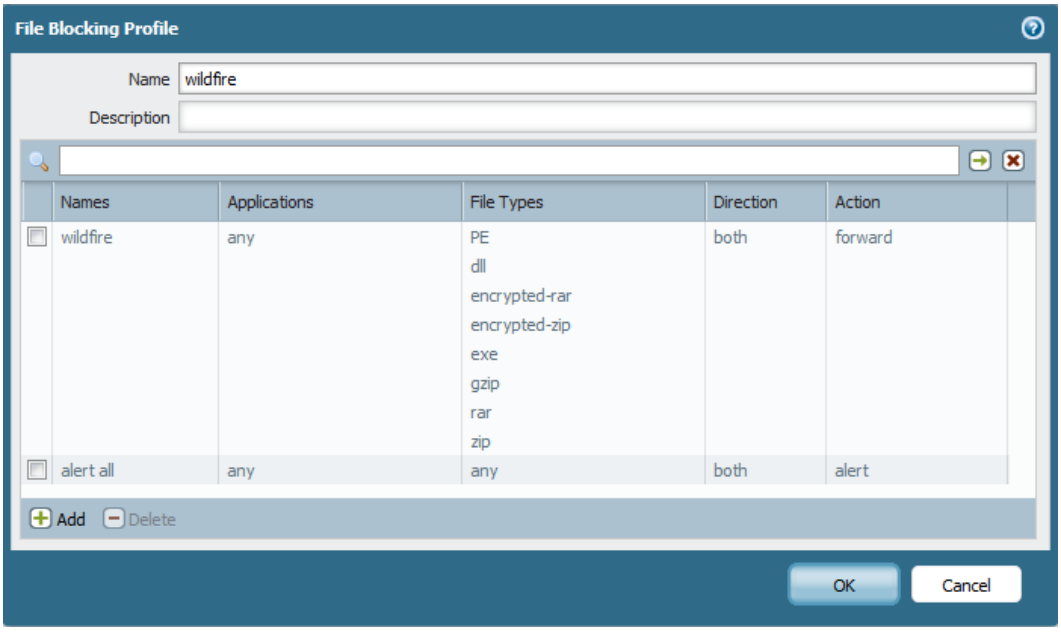


Figura. 3.8. Objeto de inspección de archivos

Una vez creados todos los objetos se los colocará en un grupo para posteriormente aplicarlos a las políticas (ver Figura. 3.9.).

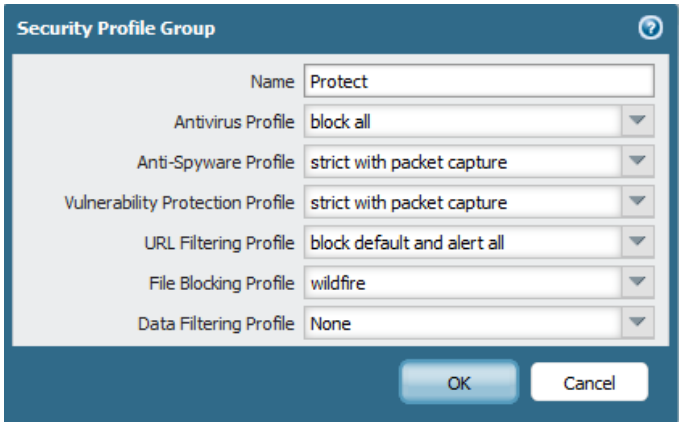


Figura. 3.9. Grupo de objetos creados

Una vez creados los objetos se procederá a la creación de políticas.

Para empezar se debe configurar las características generales. En las cuales se especificará el nombre de la regla y una breve descripción (ver Figura. 3.10.).

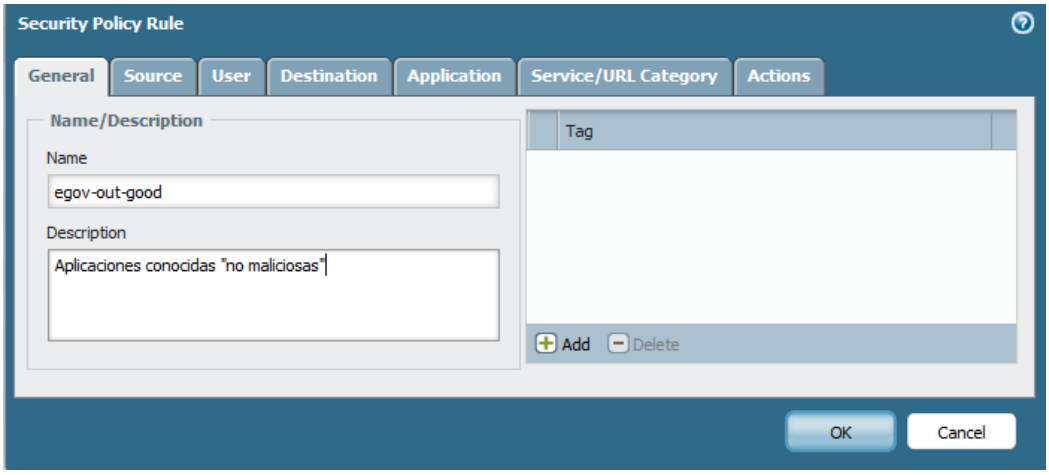


Figura. 3.10. Configuraciones generales de una política de seguridad

A continuación se da las características del origen del tráfico, especificando la zona y las direcciones IP's, en el presente caso, los requerimientos no incluyen segmentos de red en específico (ver Figura. 3.11.).

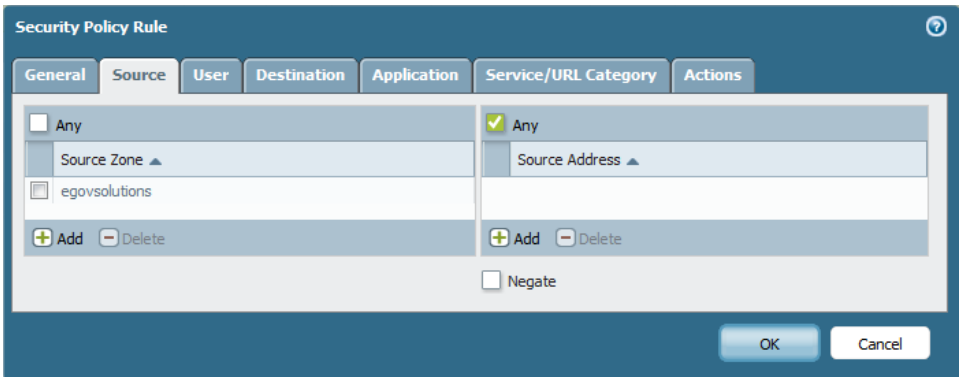


Figura. 3.11. Configuración del origen en una política de seguridad

Opcionalmente se puede establecer la política a un usuario o u grupo de usuarios específicos, en el presente caso, los requerimientos no solicitan esta opción, por lo que se aplicará la política a todos los usuarios (ver Figura. 3.12.).

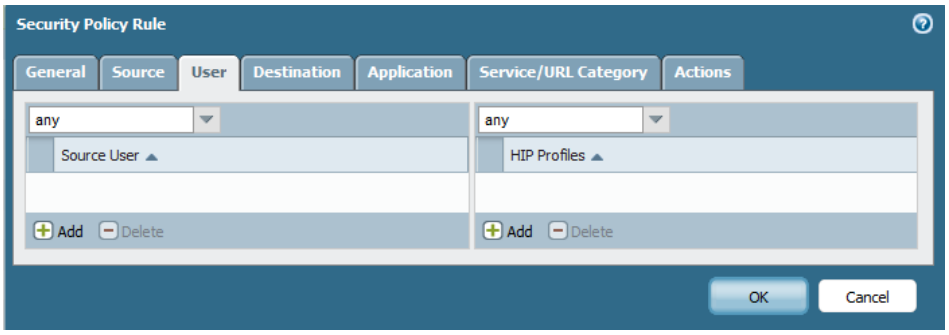


Figura. 3.12. Configuración del usuario en una política de seguridad

Posteriormente se establecerán la características del destino del tráfico, especificando la zona y las direcciones IP's, en el presente caso, los requerimientos no incluyen segmentos de red en específico (ver Figura. 3.13.).

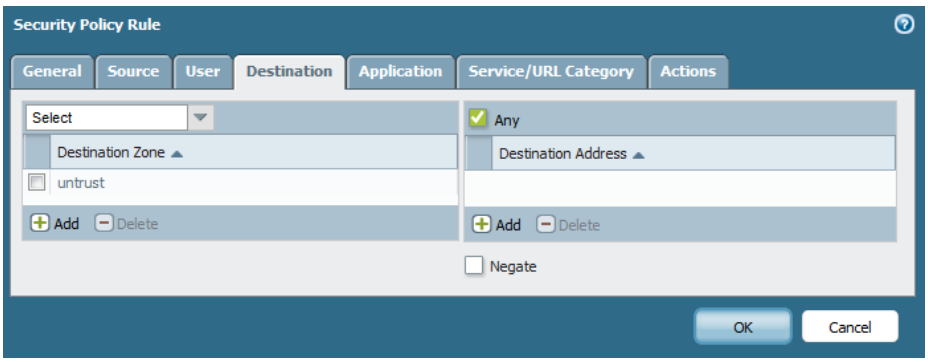


Figura. 3.13. Configuración del destino en una política de seguridad

Adicionalmente se especificarán las aplicaciones a la cual se aplicará la política, en el presente caso, se ha establecido un grupo de aplicaciones definidos por el administrador como aplicaciones conocidas “no maliciosas” (ver Figura. 3.14.).

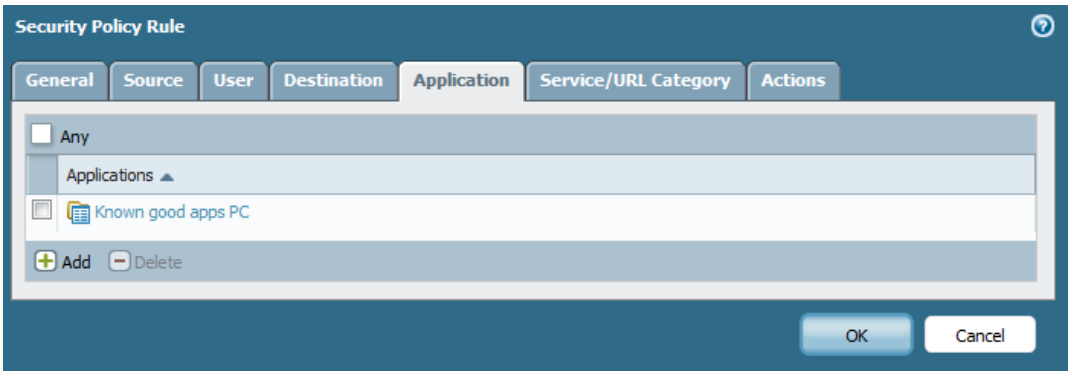


Figura. 3.14. Configuración de aplicaciones en una política de seguridad

Además se puede especificar un servicio (http, https, ftp, etc) y/o una categoría de url específica a la cual se aplicará la política, en el presente caso, no es necesario utilizar ninguna de estas opciones (ver Figura. 3.15.).

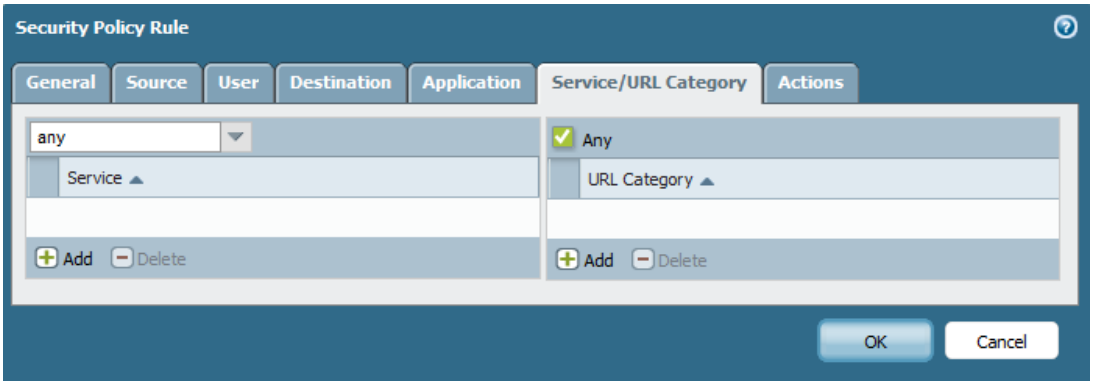


Figura. 3.15. Configuración de servicio y categoría URL en una política de seguridad

Finalmente es necesario especificar las acciones a tomar con la política. En esta pestaña se configurará las siguientes opciones:

- Configuraciones de acción
- Configuraciones de perfil
- Configuraciones de logs
- Otras configuraciones

En las configuraciones de acciones se determinará si se bloqueará o permitirá el tráfico que coincida con los parámetros antes definidos, en este caso se permitirá el tráfico.

En las configuraciones de perfil se especificará los objetos a ser utilizados (IPS, filtrado URL, inspección de archivos). En este caso aplicaremos el grupo creado previamente llamado “Protect”.

En las configuraciones de logs se especificará el momento en el que se crea el log, existen tres opciones: cuando la sesión inicia, cuando finaliza o un log cuando inicia y otro cuando finaliza. Además se puede configurar un perfil automático de envío de logs por diferentes protocolos (syslog, e-mail o SNMP), en este caso se ha configurado para que se cree el log una vez finalizada la sesión y para que se envíen logs específicos vía syslog.

En otras configuraciones es posible aplicar la regla para horas específicas, aplicar acciones relacionadas con calidad de servicio y deshabilitar la inspección de las respuestas de servidores (en caso de que se desee disminuir el procesamiento del equipo), en este caso no se utilizó ninguna de estas opciones (ver Figura. 3.16.).

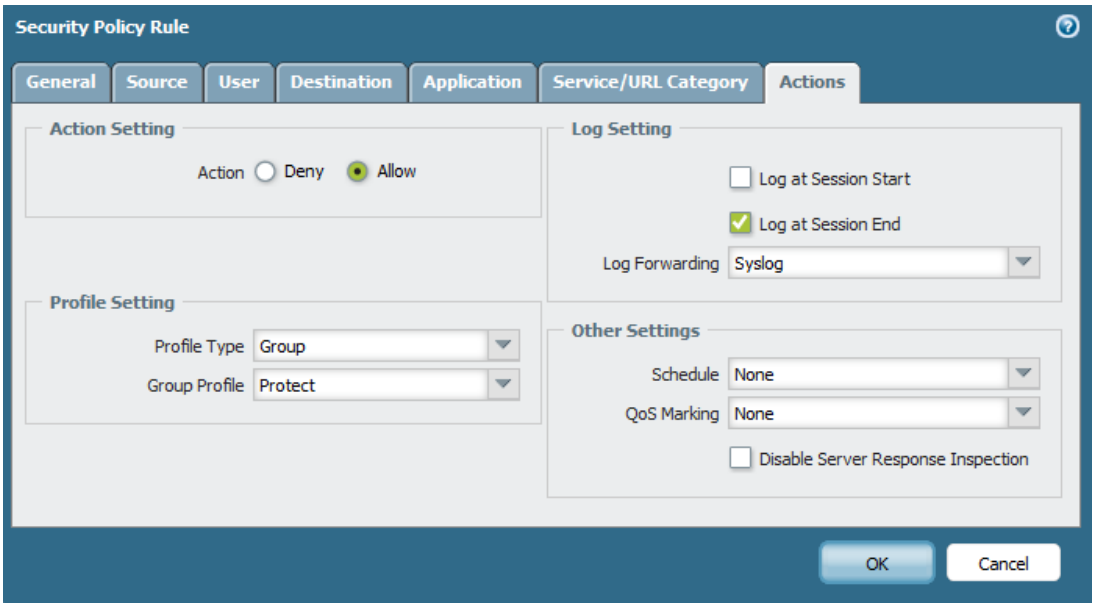


Figura. 3.16. Configuración de acciones en una política de seguridad

Una vez finalizada la configuración se procederá de manera similar a la creación de las políticas que permitan cumplir con los parámetros previamente definidos. De esta forma se ha llegado a la creación de trece políticas (ver Figura. 3.17.), en las cuales la jerarquía se establece de arriba hacia abajo; esto quiere decir que por cada flujo de tráfico generado, se empezará a evaluar desde la primera política hasta la última y en el momento que cumpla los parámetros de una política, se ejecutará la misma y finalizará el procesamiento en ese momento.

		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
egov-out-good	none	egovsolutions	any	any	any	untrust	any	Known good apps PC	any	✓		
egov-out-bad	none	egovsolutions	any	any	any	untrust	any	Known bad apps PC	any	✗	none	
egov-out	none	egovsolutions	any	any	any	untrust	any	any	any	✓		
servers-out-good	none	servers	any	any	any	untrust	any	Known good apps servers	any	✓		
servers-out-bad	none	servers	any	any	any	untrust	any	Known bad apps servers	any	✗	none	
servers-out	none	servers	any	any	any	untrust	any	any	any	✓		
clients-out-good	none	clients	any	any	any	untrust	any	Known good apps PC	any	✓		
clients-out-bad	none	clients	any	any	any	untrust	any	Known bad apps PC	any	✗	none	
clients-out	none	clients	any	any	any	untrust	any	any	any	✓		
egov-in	none	untrust	any	any	any	egovsolutions	any	routing apps	any	✓	none	
egov-servers	none	egovsolutions	any	any	any	servers	any	any	any	✓		
sslvpn-out	none	sslvpn	any	any	any	untrust	any	dns	any	✓	none	
sslvpn-in	none	untrust	any	any	any	sslvpn	any	any	any	✓		

Figura. 3.17. Políticas de seguridad configuradas

3.2.1.3. Protección contra ataques de DoS

Un ataque de denegación de servicio consiste en que un servicio o recurso informático se vuelve inaccesible por usuarios legítimos, generalmente ocasionado por la sobrecarga de dicho servicio o recurso.

El firewall de Palo Alto Networks es capaz de proteger a servidores y/o redes de las siguientes inundaciones relacionadas con ataques de denegación de servicio:

- Inundación SYN
- Inundación ICMP e ICPMv6
- Inundación UDP

Para entender la inundación SYN, es necesario comprender el funcionamiento del “3-way handshake”. Al realizar una comunicación, la fuente envía un paquete SYN, con lo que el destinatario responde con un SYN-ACK y para finalizar la comunicación, la fuente envía un ACK (ver Figura. 3.18.).

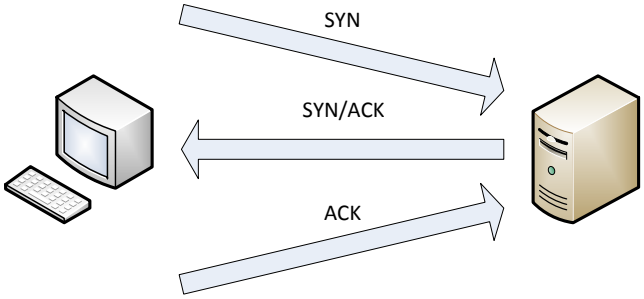


Figura. 3.18. 3-way handshake

La inundación SYN consiste en envía paquetes SYN falsos desde una o varias direcciones IP's (por lo general falsas); al ser solicitudes falsas nunca existirá la respuesta ACK después del SYN-ACK y el servidor se quedará esperando este paquete. Esta espera demanda bastantes recursos por parte del servidor generando una saturación del número de peticiones que este pueda manejar, y esto provoca que solicitudes legítimas no puedan ser procesadas. ([31] Palo Alto Networks, 2010)

La inundación ICMP se da cuando el atacante genera una gran cantidad de paquetes ICMP (ping) de tamaño considerable, de manera que el servidor responda igualmente con paquetes ICMP (pong) para finalmente sobrecargar el servidor y la red. ([31] Palo Alto Networks, 2010)

La inundación UDP consiste en generar grandes cantidades de paquetes UDP para sobrecargar el servidor, y debido a la naturaleza de los paquetes UDP, da libertad a la generación de IP Spoofing (sustituir la dirección IP origen por otra). ([31] Palo Alto Networks, 2010)

Dentro del equipo de Palo Alto Networks es necesario crear un objeto para protección contra ataques de DoS para posteriormente aplicarlo en la política.

Dentro del objeto se debe definir un nombre y establecer el tipo entre uno de los siguientes:

- Aggregate: aplica el perfil directamente a la política.

- Clasified: aplica el perfil especificando si se lo debe hacer a la dirección ip origen, destino o a ambas.

En este caso se seleccionará “Aggregate” ya que las características del origen y destino se la realizarán dentro de la política (ver Figura. 3.19.).

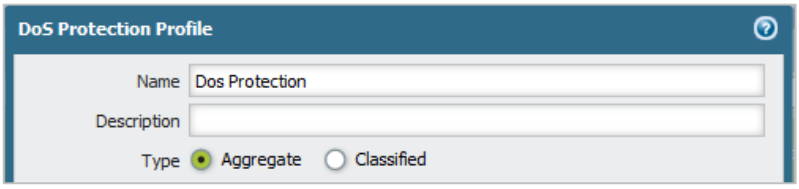


Figura. 3.19. Nombre y tipo del objeto de protección contra ataques de DoS

Posteriormente se configurarán los parámetros para para protección contra ataques de inundación.

Para la protección contra inundación SYN se debe establecer el número de paquetes por segundo para alertar, activar una acción y bloquear. La acción que se puede setear puede ser cualquiera de las siguientes: ([32] Palo Alto Networks, 2012)

- Random Early Drop.- elimina paquetes aleatoriamente
- SYN Cookies.- genera reconocimiento para que no sea necesario la eliminación de paquetes

En este caso se ha seleccionado la acción “Random Early Drop” y finalmente se debe establecer el tiempo que va a permanecer bloqueadas este tipo de solicitudes. Los parámetros se han configurado respecto a un análisis previo de la red (ver Figura. 3.20.).

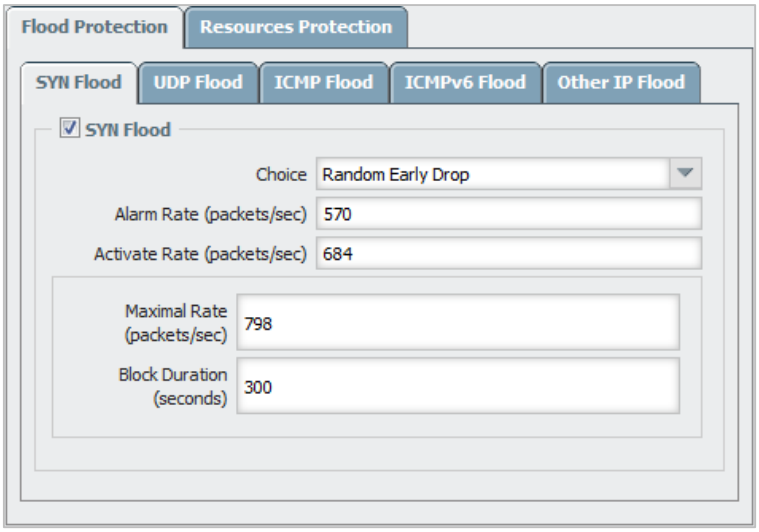


Figura. 3.20. Protección contra ataques de inundación SYN

Para la protección contra inundación UDP se debe establecer el número de paquetes por segundo para alertar, activar una acción y bloquear. Además se debe establecer el tiempo que va a permanecer bloqueadas este tipo de paquetes. Los parámetros se han configurado respecto a un análisis previo de la red (ver Figura. 3.21.). ([32] Palo Alto Networks, 2012)

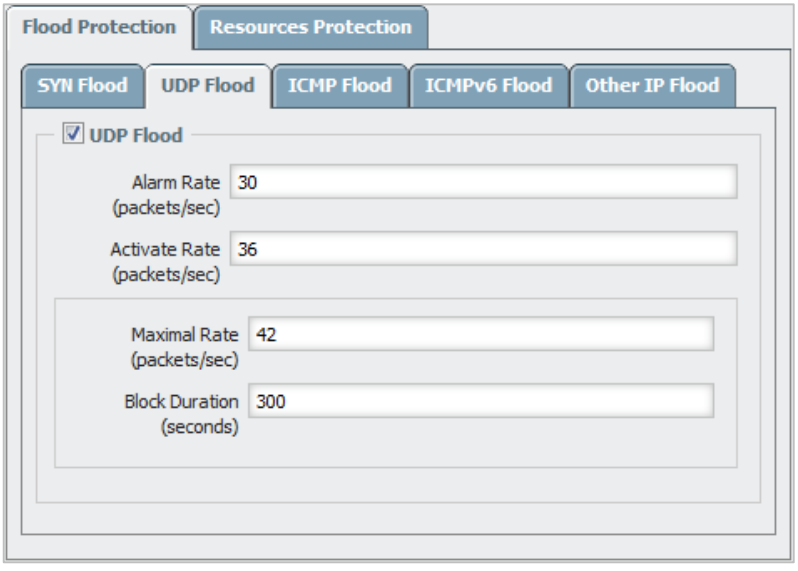


Figura. 3.21. Protección contra ataques de inundación UDP

Para la protección contra inundación ICMP se debe establecer el número de paquetes por segundo para alertar, activar una acción y bloquear. Además se debe establecer el tiempo que va a permanecer bloqueadas este tipo de paquetes. Los

parámetros se han configurado respecto a un análisis previo de la red (ver Figura. 3.22.). ([32] Palo Alto Networks, 2012)

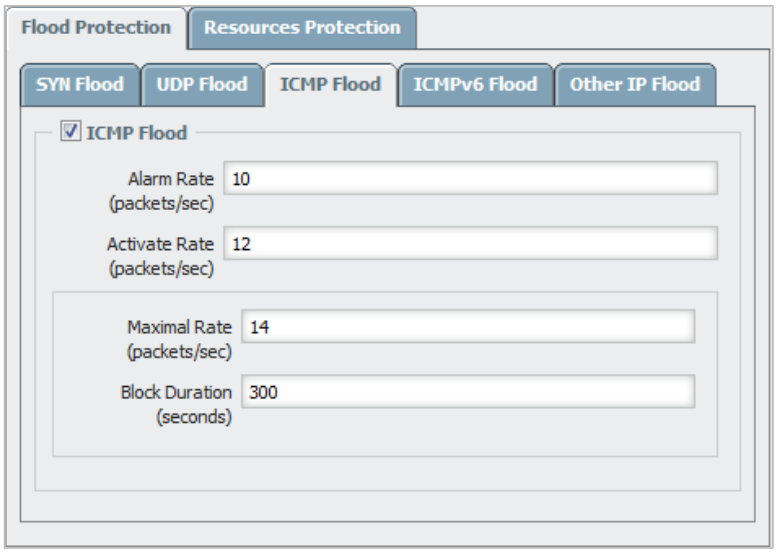


Figura. 3.22. Protección contra ataques de inundación UDP

Además se pueden realizar configuraciones para inundación ICMPv6 e inundación a una IP con cualquier tipo de paquetes. En los requerimientos no existe esta configuración.

Finalmente una vez creado el objeto es necesario crear la política, la misma que se aplicará a todo el tráfico que se dirija de la zona de usuarios (egovsolutions) hacia la zona de servidores (servers) con acción de protección (ver Figura. 3.23.).

		Source			Destination				Protection	
Name	Tag	Zone/Interface	Address	User	Zone/Interface	Address	Service	Action	Aggregate	Classified
DoS Protection	none	egovsolutions	any	any	servers	any	any	protect	DoS Protection	none

Figura. 3.23. Política de protección contra ataques de DoS

3.2.1.4. Versatilidad en Networking

Cuando las interfaces del firewall de Palo Alto Networks se encuentran configuradas en modo de capa 3, el mismo es capaz de crear rutas mediante varios protocolos conocidos (RIP, OSPF, BGP). Además es capaz de crear subinterfaces, vlans y políticas de nateo.

Todas las interfaces de capa 3 tienen que estar asociadas a un enrutador virtual. Al mismo hay que asignarle un nombre y especificarle todas las interfaces que pertenecen a este enrutador. En este caso se asignarán todas las interfaces físicas además de dos interfaces de tipo túnel que son utilizadas para la creación de VPN's (ver Figura. 3.24.).

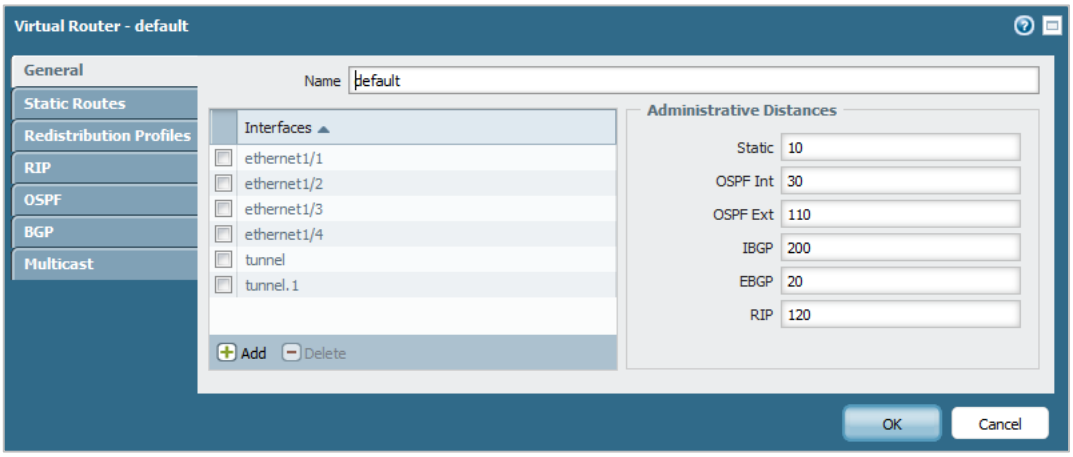


Figura. 3.24. Características generales de un enrutador virtual

Posteriormente se crearán las rutas estáticas para el flujo de tráfico. En este caso únicamente se necesitan tres. La primera para que exista conexión a la nube, el destino serán todas las direcciones IP (0.0.0.0/0) y se establecerá como salto a la dirección IP más cercana a las nube (186.71.23.225) y además dos rutas adicionales que servirán para las dos VPN's, una site-to-site y otra client-to-site (ver Figura. 3.25.).

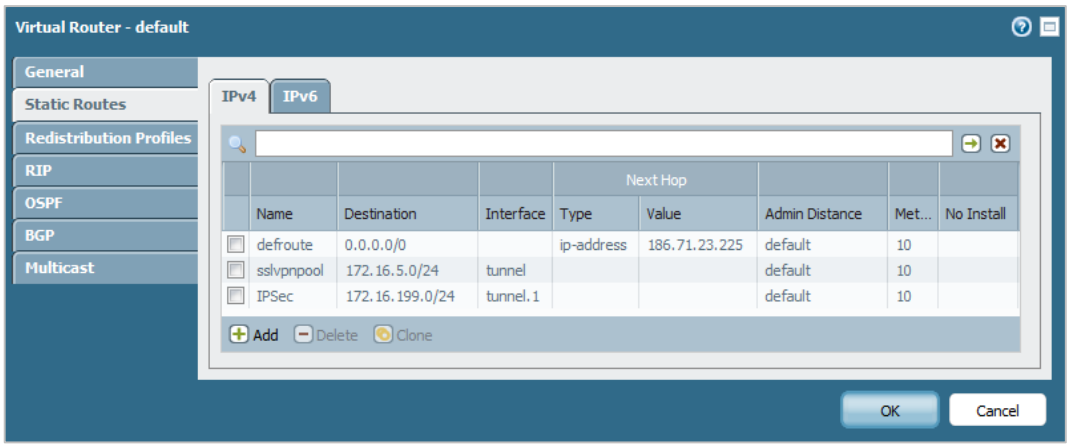


Figura. 3. 25. Rutas estáticas de un enrutador virtual

Además se deben crear las políticas de nateo correspondientes, estas servirán para que dos redes totalmente diferentes sean capaces de comunicarse entre ellas mediante una traducción de dirección de red. Aquí es posible realizar traducción en el origen, en el destino o una combinación de los dos. Para este caso se va a realizar una traducción en el origen.

Para la creación de las políticas de nateo se debe entender el escenario. En este caso la creación de la primera política va a permitir la comunicación entre la red de la zona “egovsolutions” (192.168.10.0/24) y la red de la zona “untrust” (186.71.23.224/29) que se encuentran conectadas a la interface 1 y 3 respectivamente (ver Figura. 3.26.).

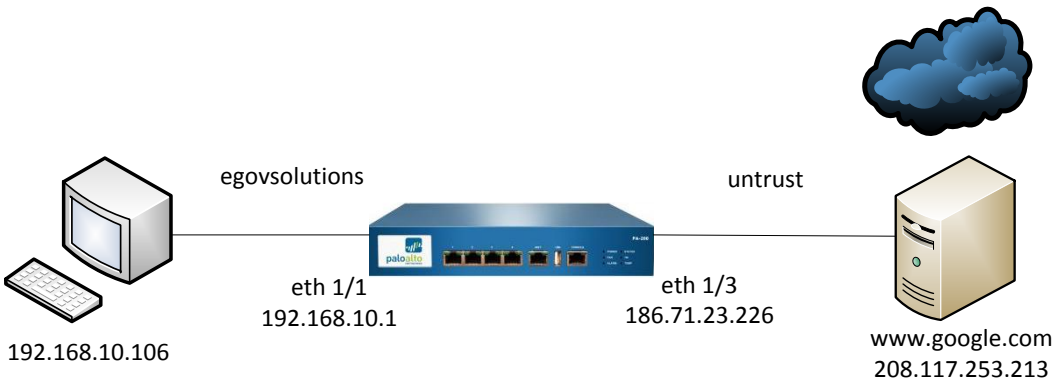
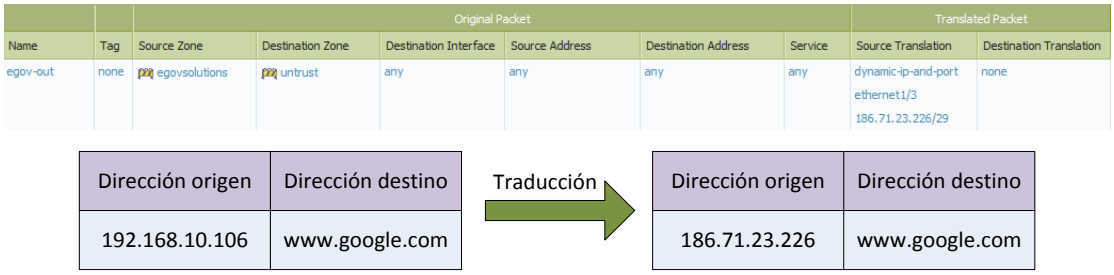


Figura. 3.26. Diagrama de red para política de nateo

Antes de la traducción de dirección de red, la dirección IP 192.169.10.106 es incapaz de comunicarse con la dirección www.google.com. Después de la

traducción, cuando se realice una petición, el tráfico cambiará su dirección origen y tomará la dirección 186.71.23.226 para de esta manera lograr la comunicación con la dirección www.google.com. Esto se plasmará en una política de nateo, realizando una traducción de dirección de origen y seleccionando la opción de IP y puerto dinámico que permitirá que la selección de la dirección será basada en el hash de la dirección IP origen. En esta configuración, el firewall usará la misma dirección origen traducida para todas las sesiones, para esto también se especificará la interface y dirección en la cual se realizará la traducción (ver Figura. 3.27.).



		Original Packet						Translated Packet	
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
egov-out	none	egovsolutions	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/3 186.71.23.226/29	none

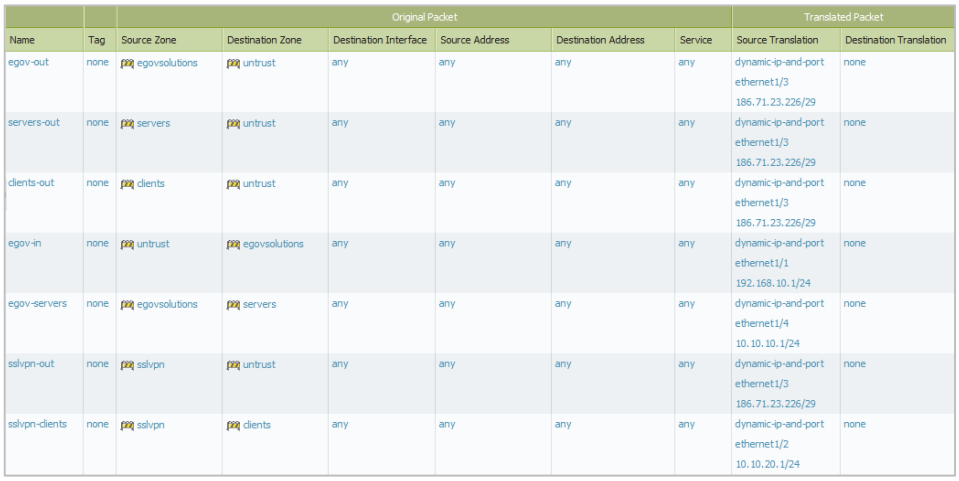
Dirección origen	Dirección destino
192.168.10.106	www.google.com

Traducción

Dirección origen	Dirección destino
186.71.23.226	www.google.com

Figura. 3.27. Funcionamiento de política de nateo

A continuación se realizarán las políticas de nateo necesarias para permitir el flujo de tráfico requerido por EGOVERMENT SOLUTIONS S.A. y explicado anteriormente en la creación de políticas de seguridad (ver Figura. 3.28.).



		Original Packet						Translated Packet	
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
egov-out	none	egovsolutions	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/3 186.71.23.226/29	none
servers-out	none	servers	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/3 186.71.23.226/29	none
clients-out	none	clients	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/3 186.71.23.226/29	none
egov-in	none	untrust	egovsolutions	any	any	any	any	dynamic-ip-and-port ethernet1/1 192.168.10.1/24	none
egov-servers	none	egovsolutions	servers	any	any	any	any	dynamic-ip-and-port ethernet1/4 10.10.10.1/24	none
sslvpn-out	none	sslvpn	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/3 186.71.23.226/29	none
sslvpn-clients	none	sslvpn	clients	any	any	any	any	dynamic-ip-and-port ethernet1/2 10.10.20.1/24	none

Figura. 3.28. Políticas de nateo configuradas

3.2.1.5. Políticas de desciframiento

Una comunicación cifrada, es aquella que mediante un algoritmo y una clave transforma el mensaje incluido en la comunicación de manera que sea extremadamente complicado para un intermediario entender el mismo.

El principal protocolo de cifrado en redes es SSL (Secure Sockets Layer), es muy utilizado en comunicaciones seguras, sobre todo las que se dirigen hacia internet (HTTPS) y se compone principalmente de los siguientes pasos:

- El cliente solicita la conexión SSL
- El servidor envía el certificado
- El cliente verifica el certificado enviado por el servidor
- El cliente envía la llave de la sesión cifrada
- El servidor inicia la comunicación cifrada

El protocolo SSL se lo creó justamente para que se puedan realizar conexiones seguras y que los cibercriminales no sean capaces de obtener información sensible durante la comunicación. En la actualidad varias aplicaciones muy utilizadas son transmitidas por HTTPS (Facebook, twitter, gmail, hotmail, etc.) y los cibercriminales han aprovechado las vulnerabilidades de estas aplicaciones para que diferentes amenazas sean transmitidas de manera cifrada al usuario final y de esta forma evitar la detección mediante antivirus o cualquier otro dispositivo de seguridad que no sea capaz de descifrar la comunicación.

El equipo de Palo Alto Networks es capaz de descifrar la comunicación realizando un “hombre en el medio”, es decir colocándose entre el cliente y el servidor y lo realizará de dos formas posibles: ([32] Palo Alto Networks, 2012)

- Inspección de entrada
- Proxy de reenvío

En el desciframiento por inspección de entrada es necesario importarle al equipo de Palo Alto Networks un certificado creado por una autoridad certificadora. De esta manera el equipo podrá descifrar con un certificado reconocido por el servidor y el cliente y el proceso de comunicación quedará de la siguiente forma:

- El cliente solicita la conexión SSL

- El servidor envía el certificado
- El firewall descifra el tráfico con el certificado válido
- El cliente verifica el certificado enviado por el servidor
- El cliente envía la llave de la sesión cifrada

El servidor inicia la comunicación cifrada

En el desciframiento por proxy de reenvío, el equipo de Palo Alto Networks debe crear un certificado digital propio que obviamente no es conocido por el cliente, por lo que el mismo deberá aceptar el certificado como válido o importarlo directamente dentro de sus navegadores para que la navegación sea transparente. En este caso el proceso de comunicación será de la siguiente manera:

- El cliente solicita la conexión SSL
- El servidor envía el certificado
- El firewall descifra el tráfico y envía al cliente el certificado creado previamente por el firewall.
- El cliente verifica el certificado enviado por el firewall
- El cliente envía la llave de la sesión cifrada al firewall a partir del certificado creado por el firewall
- El firewall envía la llave de la sesión cifrada al servidor a partir del certificado original del servidor
- El servidor inicia la comunicación cifrada

En vista de que no se tiene un certificado digital de una autoridad certificadora, se procederá a realizar la configuración de proxy de reenvío.

Primeramente se debe crear el certificado por medio del firewall (ver Figura. 3.29.).

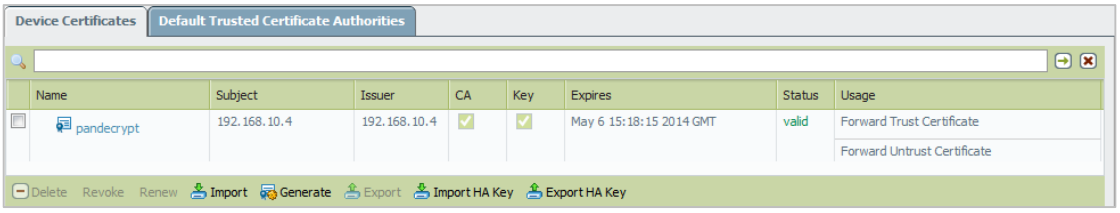


Figura. 3.29. Certificado para políticas de desciframiento

Las políticas de desciframiento se crean a partir de categorías de navegación esto debido a que existen categorías de muy buena reputación y sobre todo que transmiten información muy sensible como para que sea descifrada la misma. Las categorías que se han elegido para no ser descifradas son las siguientes:

- Economía y negocios
- Informática
- Servicios financieros
- Apuestas
- Gobierno
- Medicina y salud
- Comunicaciones y telefonía

De esta manera se van a crear dos políticas, una inicial que no descifre el tráfico de las categorías antes mencionadas y otra siguiente que descifre todo lo que pertenezca al resto de categorías (ver Figura. 3.30.).

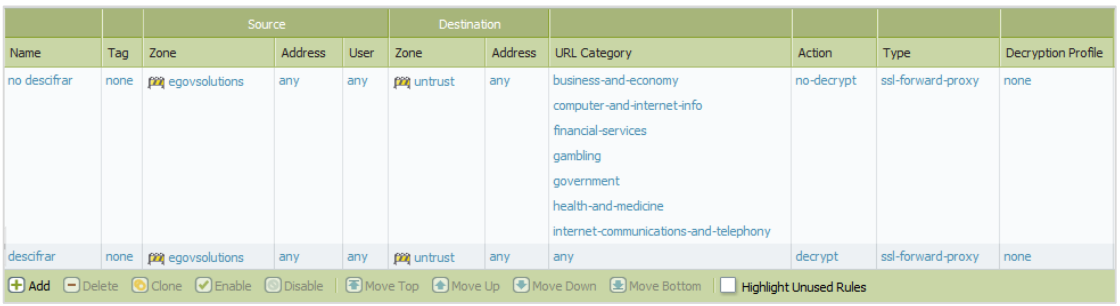


Figura. 3.30. Políticas de desciframiento

3.2.1.6. Creación y protección de VPN's.

Con el firewall de Palo Alto Networks es posible crear dos tipos de VPN's

- SSL-VPN

- IPSec-VPN

La VPN SSL-VPN es una VPN client-to-site, la misma se utiliza para que los dispositivos móviles de usuarios autorizados puedan conectarse a segmentos específicos de la red y además se puedan proteger mediante reglas aplicadas dentro del firewall y que justamente el usuario no pierda la protección que tiene dentro de la oficina, independientemente del dispositivo que use (teléfono inteligente, tableta o computador portátil) o en donde realice la conexión (aeropuerto, casa, cafetería, etc.).

Para la creación de la VPN SSL-VPN inicialmente se debe crear dos certificados digitales, el primero para el cliente y el segundo para el servidor, de manera que la comunicación viaje cifrada a través de la nube (ver Figura. 3.31.).

Figura. 3.31. Certificados para creación de SSL-VPN

Además se debe establecer el método de autenticación para realizar el logueo dentro de la VPN, para este caso se utilizará una base de datos creada dentro del equipo (ver Figura. 3.32.)

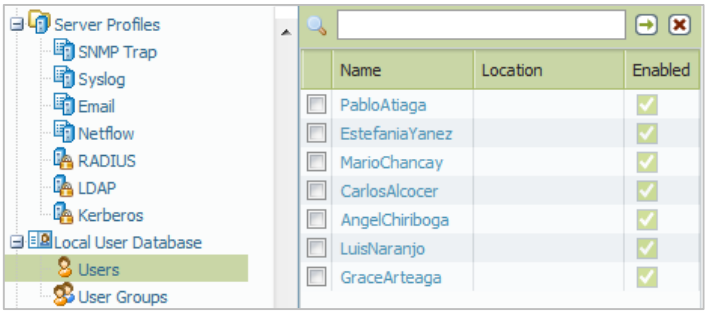


Figura. 3.32. Base de datos de usuarios local

A continuación se debe crear un perfil de autenticación especificando que la autenticación se lo va a realizar mediante la base de datos local (ver Figura. 3.33.).

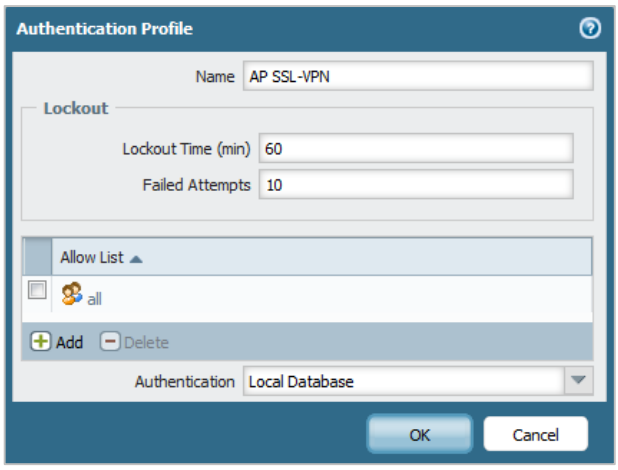


Figura. 3.33. Perfil de autenticación SSL-VPN

Es necesario crear una interface túnel que esté asociada a la zona a la que se van a conectar los usuarios remotamente, esta zona se llamará “sslvpn” (ver Figura. 3.34.).

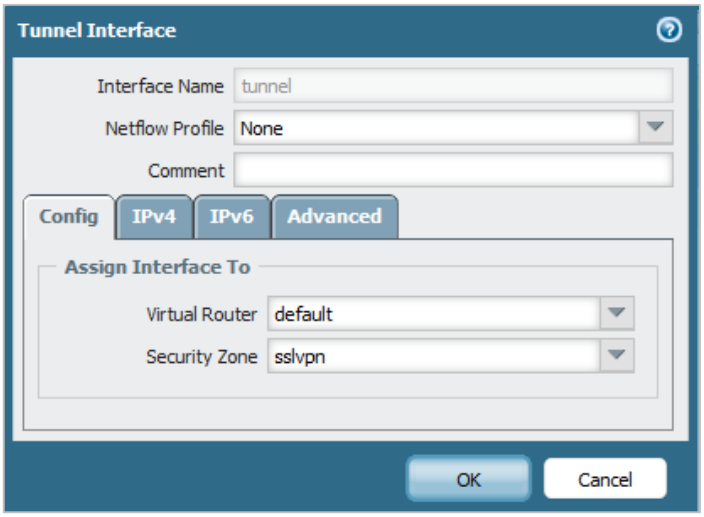


Figura. 3.34. Interface túnel SSL-VPN

Ahora se procederá a crear el Global Protect Gateway, el cuál será el punto de entrada a la red privada. En las configuraciones general se establecerá la interface, la dirección IP pública a la cual se van a conectar los equipo, el certificado del servidor y el perfil de autenticación a ser utilizado (ver Figura. 3.35.).

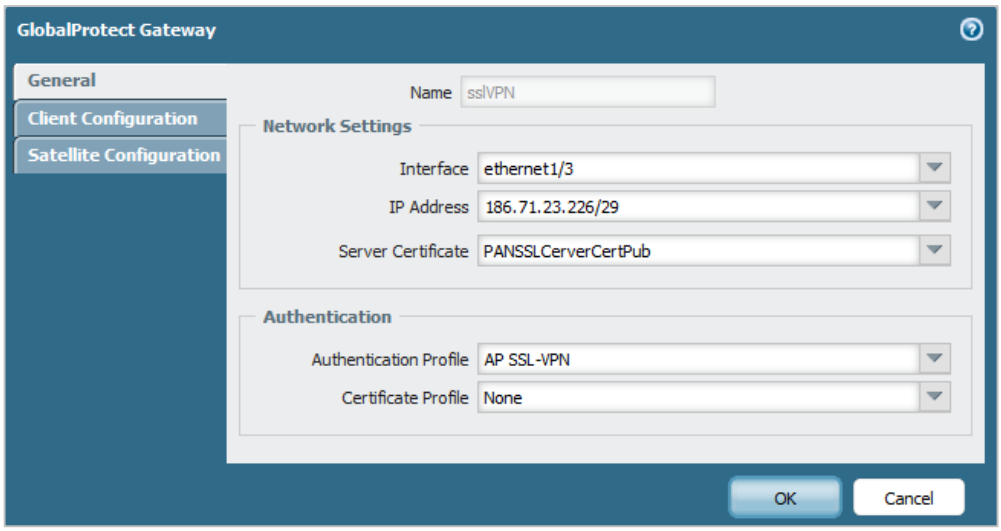


Figura. 3.35. Configuraciones generales de Global Protect Gateway

En la sección de configuración de cliente se deberá especificar la interface túnel a utilizar (antes creada), los parámetros de configuración de cierre de sesión (timeout) (ver Figura. 3.36.) y los parámetros de red, que incluyen servidores DNS y el rango de direcciones IP's que se asignarán a los usuarios que se conecten (ver Figura. 3.37.)

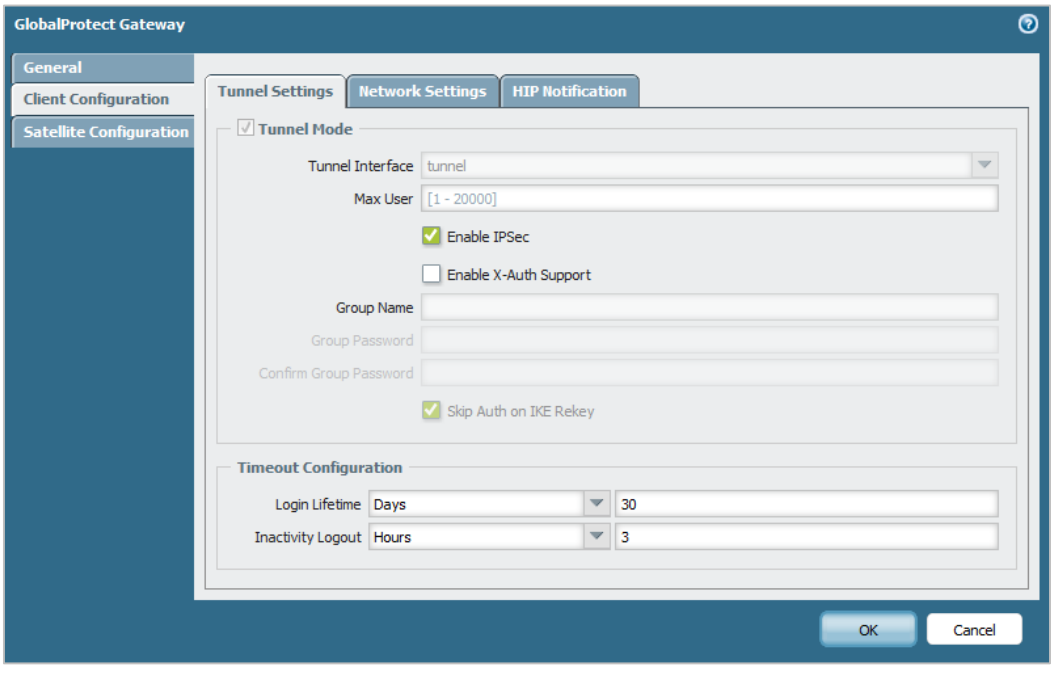


Figura. 3.36. Configuraciones de la interface túnel del Global Protect Gateway

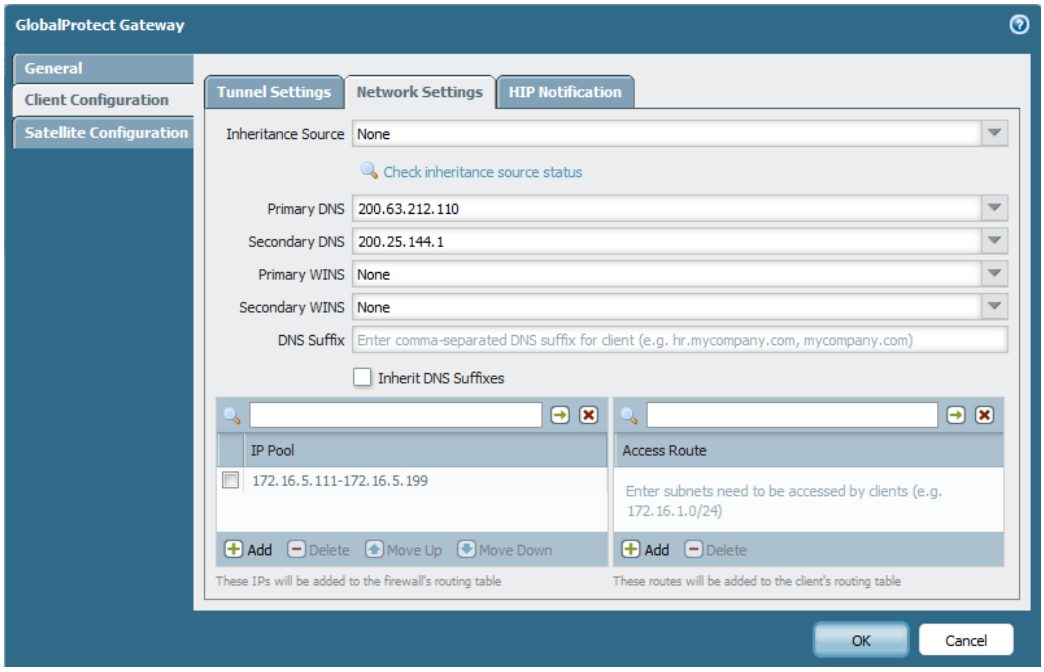


Figura. 3.37. Configuraciones de red de Global Protect Gateway

La siguiente etapa a configurar es el Global Protect Portal, este será el portal al cuál se conectarán los usuarios finales para realizar la descarga de los clientes (software necesario para conectarse a la VPN). Las configuraciones iniciales son similares a las de Global Protect Gateway, es necesario especificar una dirección IP pública que se encuentre conectada a una interface física del equipo, un certificado digital del servidor, un método de autenticación y un certificado digital del cliente (ver Figura. 3.38.).

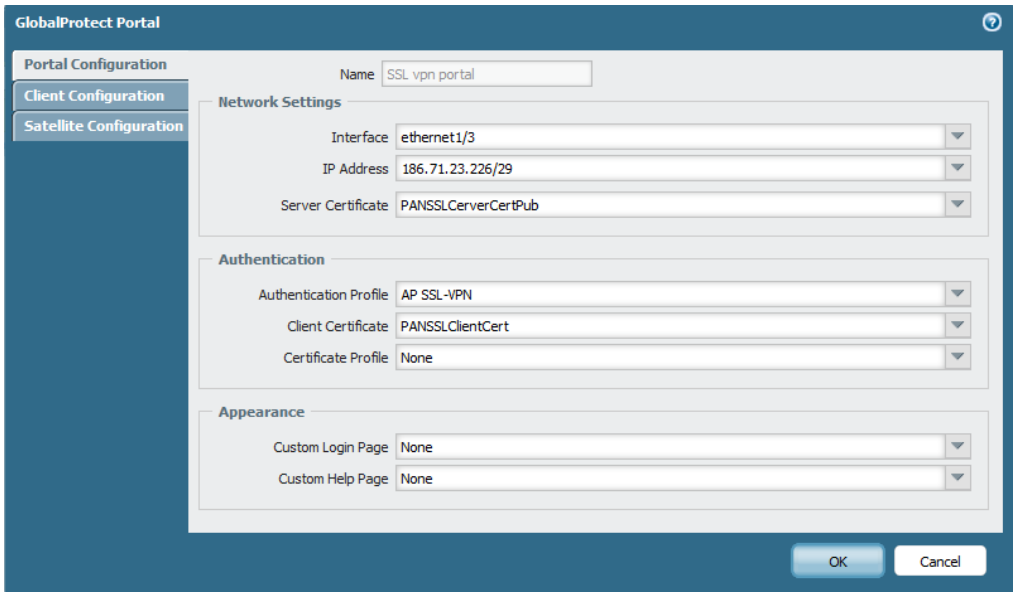


Figura. 3.38. Configuraciones de portal de Global Protect Portal

En la sección de cliente es necesario especificar la puerta de enlace por la cual los clientes se van a conectar a la red y además el método se conexión, aquí se puede especificar que los usuarios se conecten bajo demanda o que automáticamente el cliente se conecte cada vez que tenga internet. En este caso se lo va a configurar para que automáticamente el cliente busque conectarse cuando detecta conexión a internet (ver Figura. 3.39.).

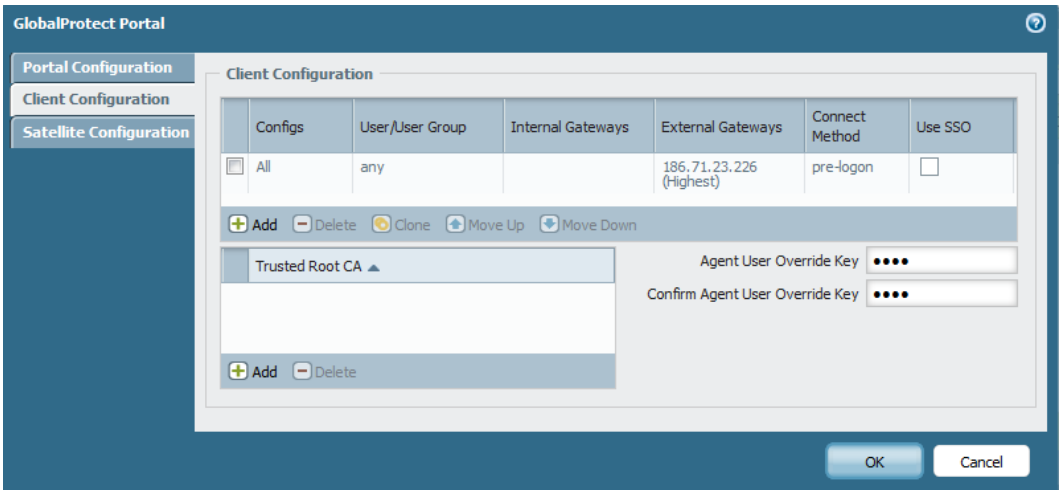


Figura. 3.39. Configuraciones de cliente de Global Protect Portal

Las mencionadas anteriormente son todas las configuraciones necesarias dentro del equipo del Palo Alto Networks. A continuación se debe realizar las configuraciones del agente dentro de los dispositivos finales. Inicialmente se debe

descargar el software desde el Global Protect Portal (para computadores Windows o MAC), desde la tienda de Google (dispositivos Android) o desde la tienda Apple (dispositivos iOS). Después de la descarga del software únicamente se debe configurar el Global Protect Gateway y su respectivo usuario y contraseña (ver Figura. 3.40.).

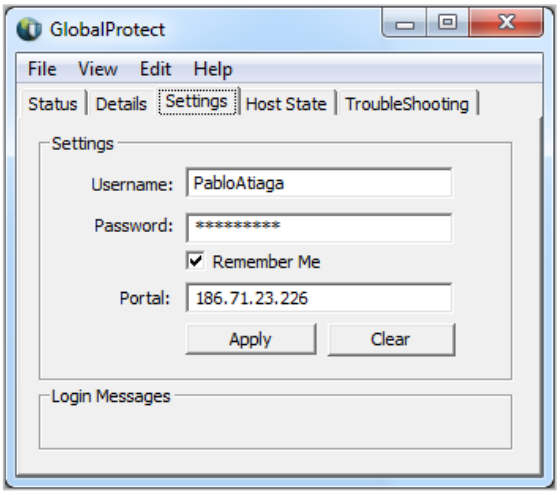


Figura. 3.40. Configuración del cliente de Global Protect en el dispositivo final

A partir de este momento, se puede visualizar todo el tráfico que genera el usuario hacia internet (ver Figura. 3.41.) a pesar de estar conectado en cualquier lugar del mundo y gracias a eso es posible aplicar políticas a nivel de aplicación, usuario y contenido (amenazas, filtrado de URL, archivos y datos).

(user.src eq pabloatiaga)

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes
	06/18 11:30:05	end	sslvpn	untrust	172.16.5.113	pabloatiaga	65.55.223.17	40010	skype-probe	allow	sslvpn-out	283
	06/18 11:30:05	end	sslvpn	untrust	172.16.5.113	pabloatiaga	157.55.130.160	40035	skype-probe	allow	sslvpn-out	303
	06/18 11:30:05	end	sslvpn	untrust	172.16.5.113	pabloatiaga	213.199.179.150	40030	skype-probe	allow	sslvpn-out	144
	06/18 11:30:05	end	sslvpn	untrust	172.16.5.113	pabloatiaga	111.221.74.18	40024	skype-probe	allow	sslvpn-out	138
	06/18 11:30:05	end	sslvpn	untrust	172.16.5.113	pabloatiaga	65.55.223.24	40039	skype-probe	allow	sslvpn-out	138
	06/18 11:29:45	end	sslvpn	untrust	172.16.5.113	pabloatiaga	54.244.30.186	443	brightcloud	allow	sslvpn-out	7.1 K
	06/18 11:29:32	end	sslvpn	untrust	172.16.5.113	pabloatiaga	186.107.223.137	50955	skype-probe	allow	sslvpn-out	489
	06/18 11:29:30	end	sslvpn	untrust	172.16.5.113	pabloatiaga	199.7.52.72	80	incomplete	allow	sslvpn-out	348
	06/18 11:29:28	end	sslvpn	untrust	172.16.5.113	pabloatiaga	199.7.52.72	80	incomplete	allow	sslvpn-out	348
	06/18 11:29:27	end	sslvpn	untrust	172.16.5.113	pabloatiaga	72.167.218.192	995	ssl	allow	sslvpn-out	138.2 K
	06/18 11:29:27	end	sslvpn	untrust	172.16.5.113	pabloatiaga	199.7.52.72	80	incomplete	allow	sslvpn-out	348
	06/18 11:29:27	end	sslvpn	untrust	172.16.5.113	pabloatiaga	199.7.52.72	80	incomplete	allow	sslvpn-out	348
	06/18 11:29:26	end	sslvpn	untrust	172.16.5.113	pabloatiaga	54.244.30.186	443	brightcloud	allow	sslvpn-out	5.7 K
	06/18 11:29:26	end	sslvpn	untrust	172.16.5.113	pabloatiaga	54.244.30.186	443	brightcloud	allow	sslvpn-out	5.7 K

Figura. 3.41. Logs del usuario remoto a través de la VPN hacia Internet

La VPN IPSec-VPN se utilizará para simular los enlaces entre diferentes sedes de manera que los datos viajen cifrados a través de la nube mediante una comunicación entre sus firewalls.

Para la creación de la misma es necesario realizar configuraciones en ambos cortafuegos (sin importar el proveedor), las direcciones IP's públicas y las direcciones IP's internas de ambos lados que deseemos que se comuniquen. En este caso se realizará la comunicación de la red interna 10.10.20.0/24 a través de la IP pública 186.71.23.226 y tendrán como destino una red que se mantendrá al anonimato, pero que para razones prácticas, la red interna destino se denominará X.X.X.X/X y la IP pública destino se denominará Y.Y.Y.Y. (ver Figura. 3.42.).

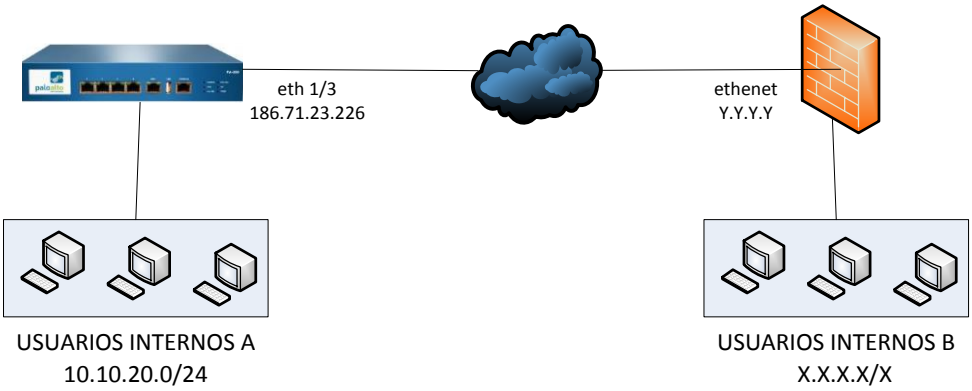


Figura. 3.42. Topología de red VPN IPSEC

Para realizar este tipo de comunicación, es necesario realizar dos fases de cifrado y esta información debe ser compartida con el destinatario para que sea capaz de descifrar el mensaje, la primera fase es denominada IKE y la segunda, IPSec.

Inicialmente se debe crear un perfil IKE que contendrá todos los datos necesarios para la fase 1, estos son:

- Grupo de Diffie Hellman
- Método de cifrado
- Método de autenticación

Para el ejemplo actual, se utilizará el grupo de DH 5, el método de cifrado será aes256 y el método de autenticación será sha512 (ver Figura. 3.43.).

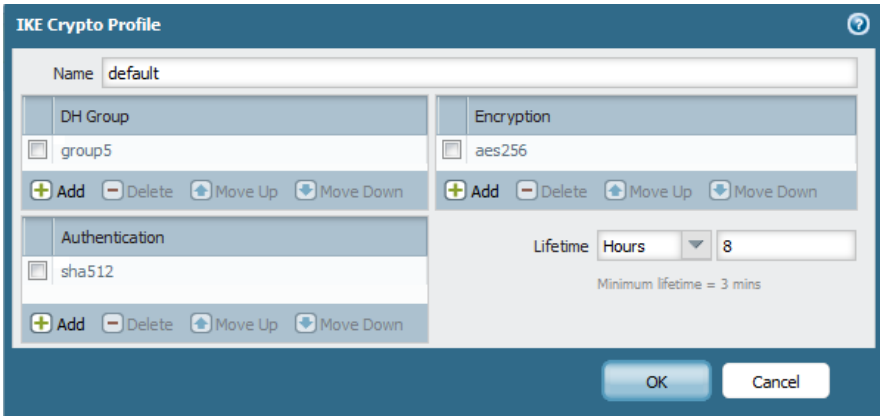


Figura. 3.43. Perfil IKE

A continuación se debe crear la puerta de enlace IKE. Entre las características más importantes se especificará la dirección IP pública local, la dirección IP pública remota, una clave compartida previamente, el modo de intercambio de información (principal o agresivo) y el perfil IKE previamente creado (ver Figura. 3.44.).

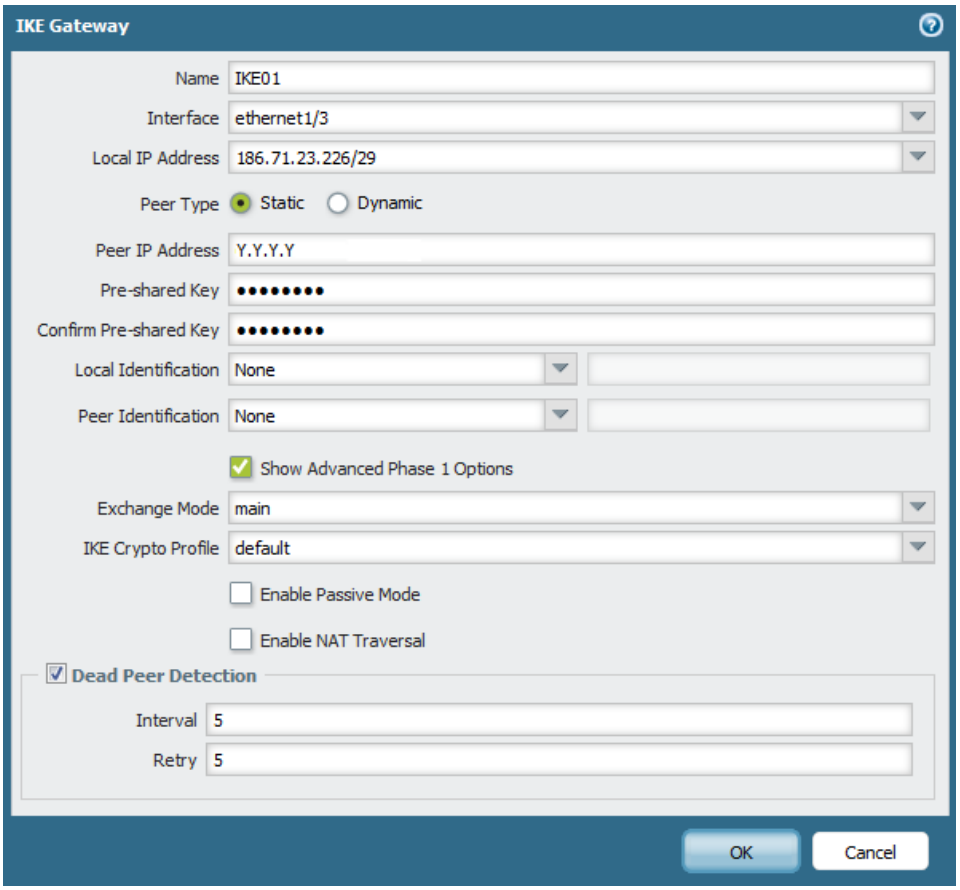


Figura. 3.44. Puerta de enlace IKE

Una vez finalizada la configuración de la fase uno, se debe proceder de la misma forma a crear un perfil IPSec para el cifrado de la fase dos. Se debe configurar los siguientes parámetros:

- Protocolo IPSec
- Grupo de Diffie Hellman
- Método de cifrado
- Método de autenticación

Para el ejemplo actual, se utilizará el protocolo ESP, grupo de DH 2, método de cifrado aes256 y método de autenticación sha256 (ver Figura. 3.45.).

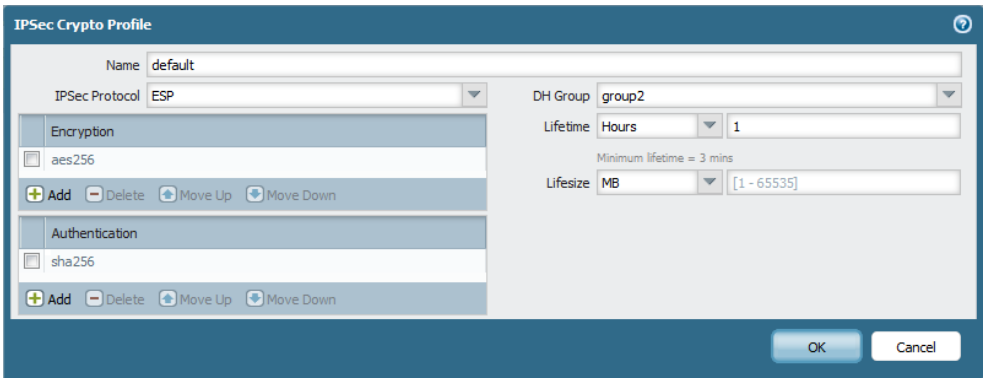


Figura. 3.45. Perfil IPSec

Finalmente se debe crear el túnel IPSec que contendrá un interface túnel, el perfil IPSec y la puerta de enlace IKE antes creados (ver Figura. 3.46.) y en la sección de Proxy ID's se especificará los hosts o redes internas que se pueden comunicar (mediante políticas de seguridad se puede restringir accesos a aplicaciones específicas) (ver Figura. 3.47.).

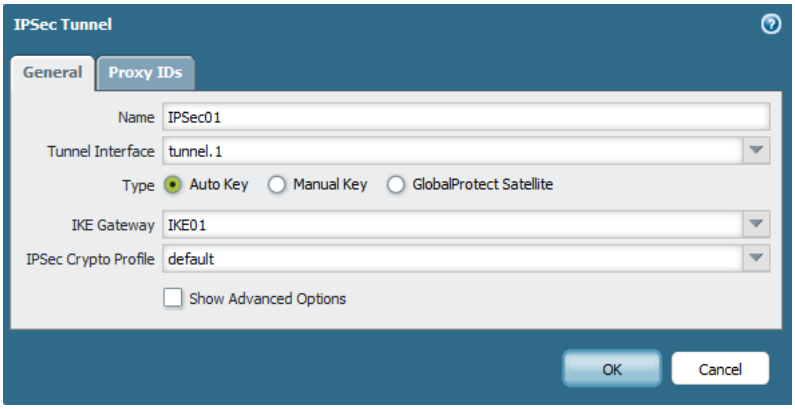


Figura. 3.46. Configuraciones generales túnel IPSec

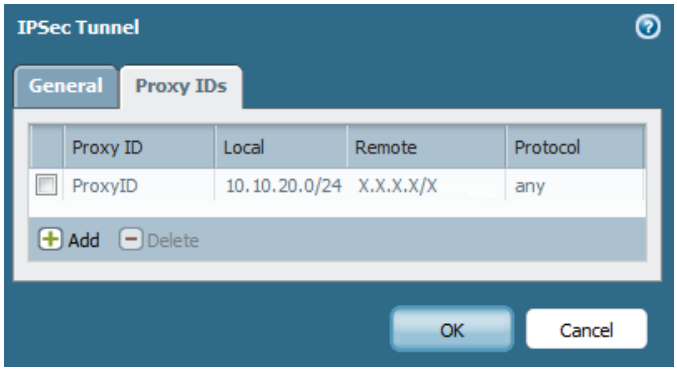


Figura. 3.47. Proxy ID's del túnel IPSec

Una vez realizadas todas las configuraciones, es posible visualizar la conectividad de las dos fases configuradas mediante el color del círculo de cada fase (verde significa que si hay conectividad y rojo que no hay conectividad) (ver Figura. 3.48.).

				IKE Gateway/Satellite				Tunnel Interface				
	Name	Status	Type	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
☐	IPSec01	●	auto-key	ethernet1/3	186.71.23.226/29	Y.Y.Y.Y	●	tunnel.1	default (Show Routes)	vsys1	untrust	▮

Figura. 3.48. Status del túnel IPSec

3.2.1.7. Wildfire

Wildfire es la seguridad en la nube para detección de ataques “no basados” en firmas que tiene el firewall de Palo Alto Networks, se podría decir que es similar a lo que hace FireEye pero lo realiza en la nube y con una tecnología diferente.

Wildfire recepta los archivos enviados por los clientes de Palo Alto Networks alrededor del mundo, los prueba en diferentes ambientes con más de 100 técnicas de detección de malware únicamente basándose en su comportamiento y finalmente, en caso de detectar que un archivo sea malicioso, procede a crear una firma automáticamente (sin un ente humano) para ese tipo de ataque y actualizar a todos los cortafuegos de Palo Alto Networks alrededor del mundo.

Dentro del firewall es necesario especificar que tipos de archivos deseamos que sean enviados a la nube de wildfire, esto se realiza creando un objeto de tipo inspección de archivos seleccionado las extensiones de los archivos y colocando la acción “forward” (significa que el archivo pasará a través de la red pero se enviará una copia a la nube de wildfire) que posteriormente se aplicará a una política (ver Figura. 3.49.). En este caso los tipos de archivos riesgosos seleccionados son:

- PE
- dll
- encrypted-rar
- encrypted-zip
- exe

- gzip
- rar
- zip

Una vez creado el objeto se aplicarán a las políticas de todas las zonas como se mostró anteriormente.

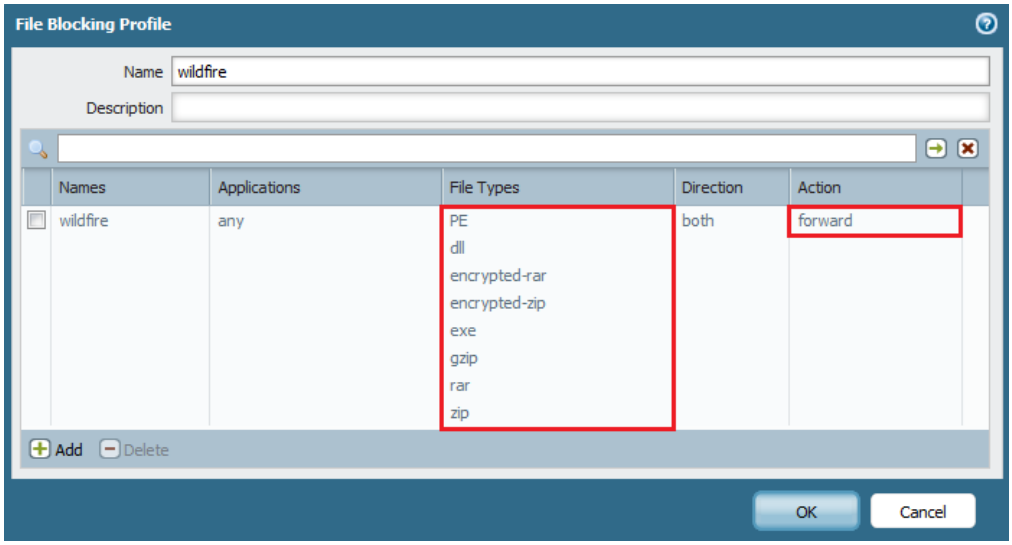


Figura. 3.49. Configuraciones de wildfire dentro de un objeto de inspección de archivos

Para ver los resultados del análisis de wildfire se lo puede visualizar a través de la sección de logs y para ver un reporte detallado es necesario ingresar al sitio https://wildfire.paloaltonetworks.com e ingresar con las credenciales de soporte de Palo Alto Networks. Dentro de este sitio es posible ver el panel principal que me mostrará el resumen de los análisis en periodos de tiempos específicos (ver Figura. 3.50.) además es posible ver todos los reportes generados de todos los archivos subidos a la nube (ver Figura. 3.51.) y se puede ver el detalle de este análisis (ver Figura. 3.52.) donde se puede encontrar las características generales, un resumen del análisis (comportamiento), datos de tráfico (dominio, url, protocolo, dirección IP, etc.) y eventos detallados (registros, procesos y archivos modificados, borrados o creados)

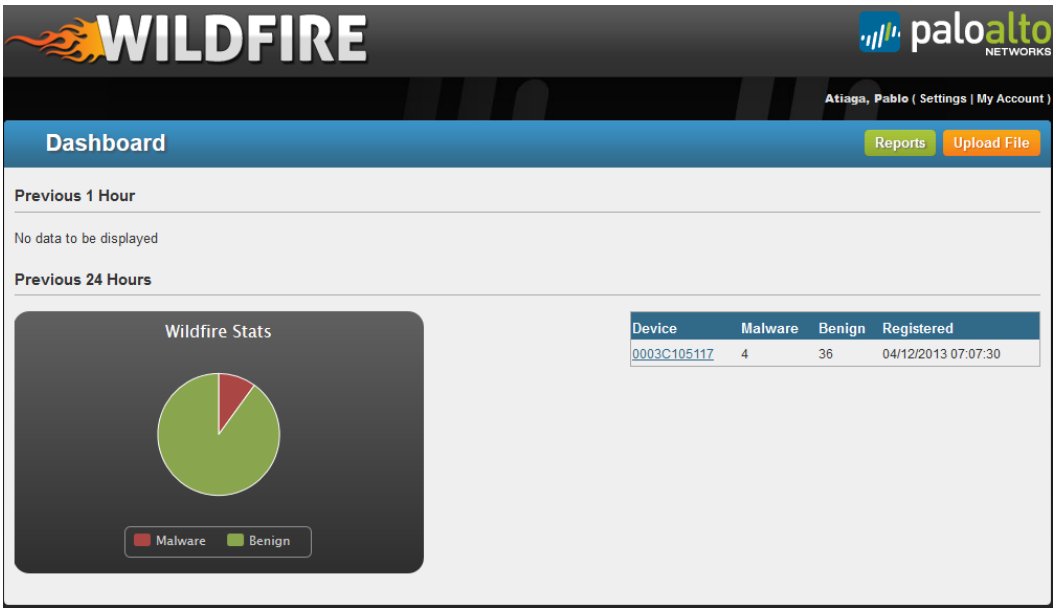


Figura. 3.50. Panel principal de Wildfire

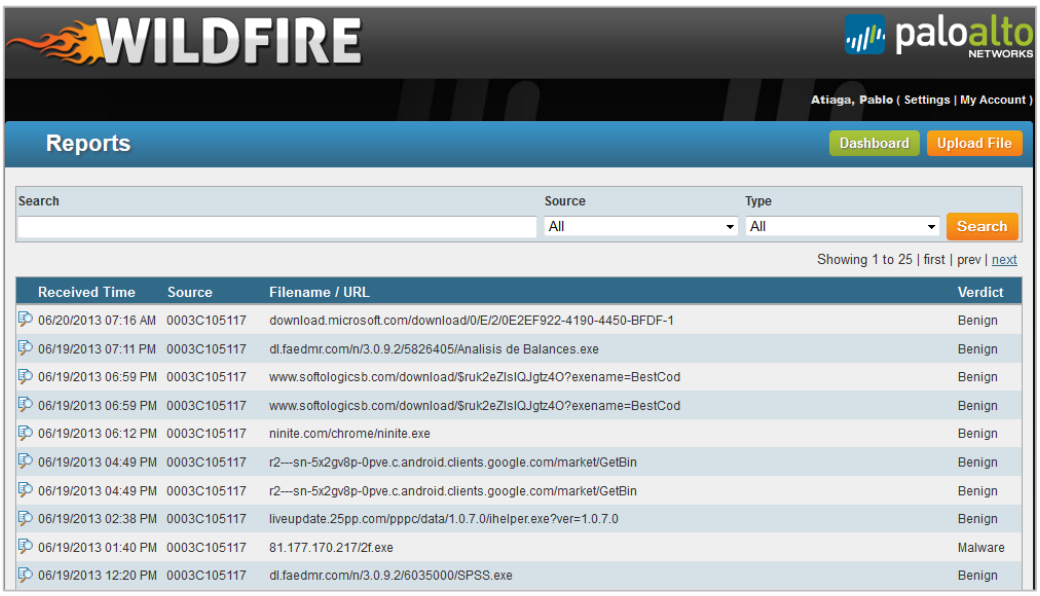
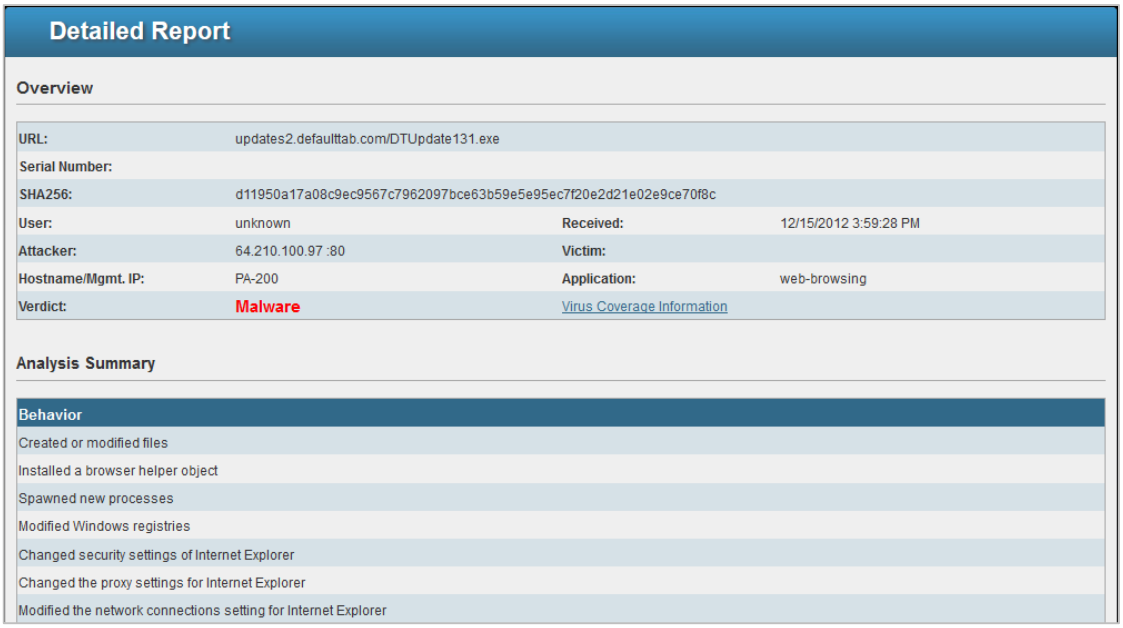


Figura. 3.51. Listado de reportes generados por Wilfire



Detailed Report

Overview

URL:	updates2.defaulttab.com/DTUpdate131.exe		
Serial Number:			
SHA256:	d11950a17a08c9ec9567c7962097bce63b59e5e95ec7f20e2d21e02e9ce70f8c		
User:	unknown	Received:	12/15/2012 3:59:28 PM
Attacker:	64.210.100.97 :80	Victim:	
Hostname/Mgmt. IP:	PA-200	Application:	web-browsing
Verdict:	Malware	Virus Coverage Information	

Analysis Summary

Behavior
Created or modified files
Installed a browser helper object
Spawned new processes
Modified Windows registries
Changed security settings of Internet Explorer
Changed the proxy settings for Internet Explorer
Modified the network connections setting for Internet Explorer

Figura. 3.52. Reporte detallado de Wildfire

3.2.2. FireEye

3.2.2.1. Configuración

Para la puesta en operación de la plataforma de FireEye Web MPS 2310 los requerimientos son los siguientes: ([33] FireEye, 2013)

- Físico:
  - Peso: 13 lbs.
  - Unidades de Rack: 1U.
- Eléctricos:
  - 1 toma eléctrica 110 V / 4.8 A.
- Funcionales:
  - Una IP para administración de la plataforma FireEye Web MPS 2310. Esta IP requiere navegación a Internet para descargar actualizaciones.

La plataforma FireEye Web MPS 2310 en se encuentra configurada en modo in-line, lo cual implica que será capaz de analizar el tráfico, generar alertas y tomar acciones de bloqueo.

El equipo se encontrará ubicado entre el router del proveedor y la red interna (ver Figura. 3.53.)

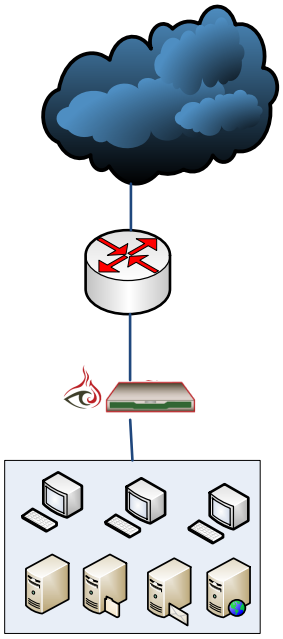


Figura. 3.53. Diagrama físico FireEye

El equipo posee cuatro interfaces (ver Figura. 3.54.) que serán utilizadas de la siguiente forma (ver Tabla. 3.2.):

#	Descripción	Detalle
1	Puertos configurado para administración	pether1
2	Puerto libre para administración	pether2
3	Puerto de tráfico configurado del lado de la nube	pether3
4	Puerto de tráfico configurado del lado de la red interna	pether4

Tabla. 3.2. Configuración de interfaces FireEye

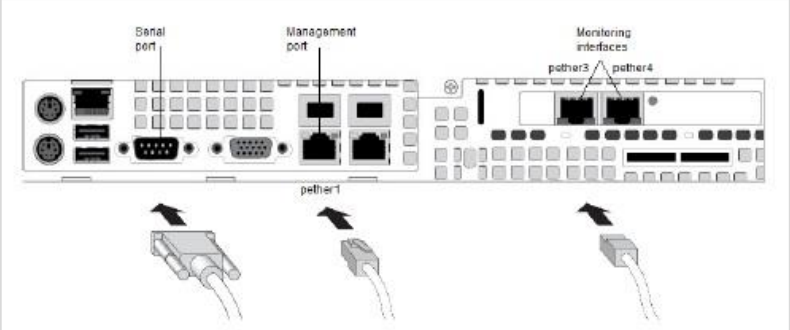


Figura. 3.54. Vista trasera FireEye

Dentro de la pestaña de Setting se han realizado todas las configuraciones necesarias.

Dentro de esta sección parámetros de red (ver Figura. 3.55.) se configuraron los siguientes parámetros de dirección IP, mascara, default gateway y el dns:

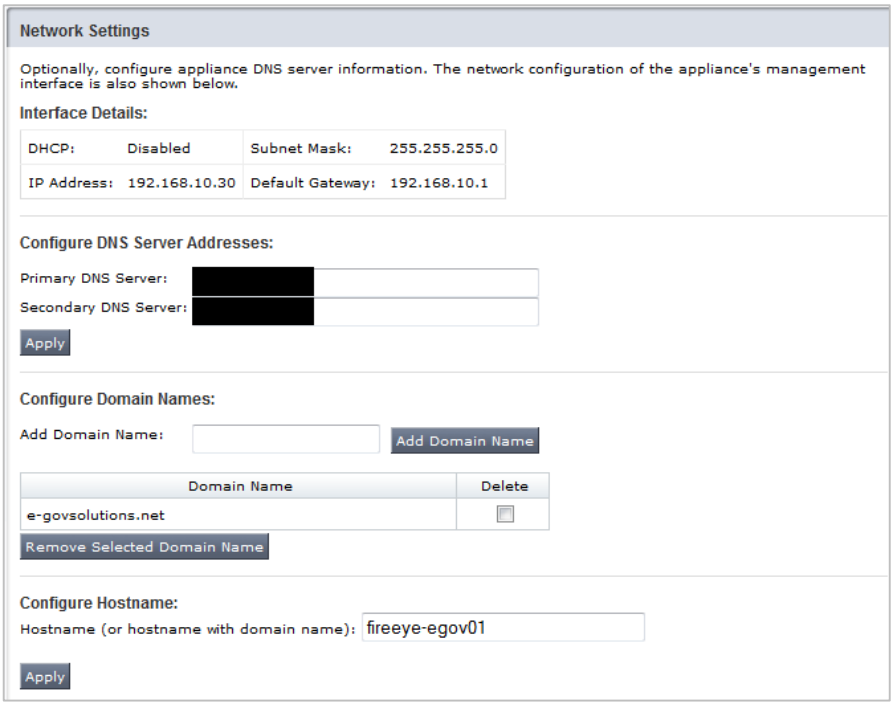


Figura. 3.55. Parámetros de red FireEye

Dentro de esta sección fecha y hora (ver Figura. 3.56.) se configuraron los siguientes parámetros tiempo.

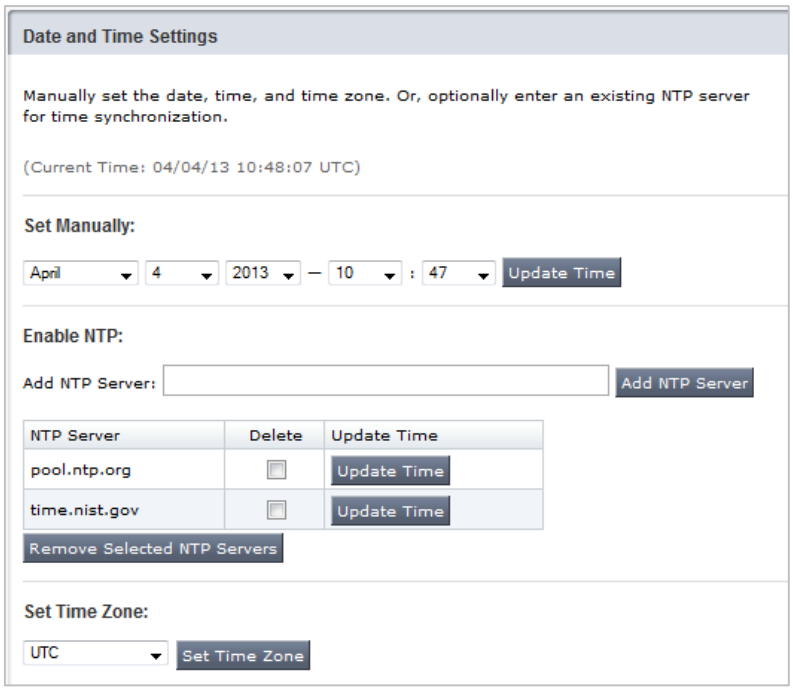


Figura. 3.56. Configuraciones de tiempo FireEye

En la sección de MPC Network (ver Figura. 3.57.) se realizarán las configuraciones para las actualizaciones del equipo.

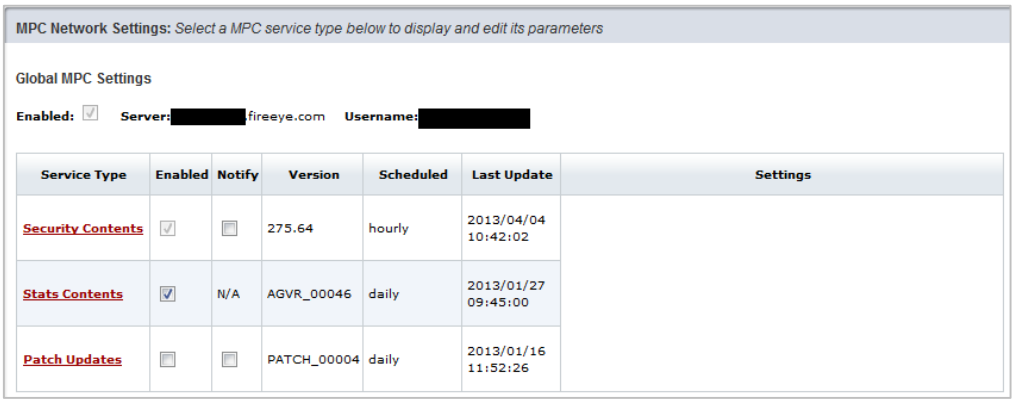
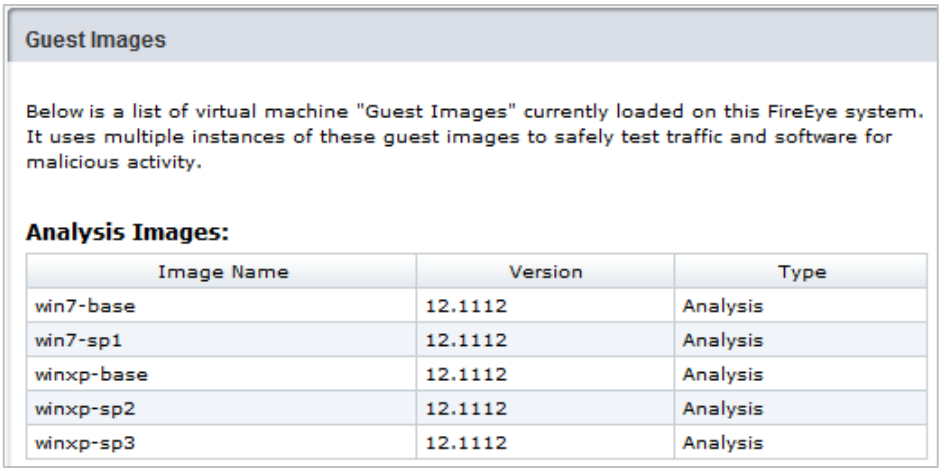


Figura. 3.57. Configuraciones de MPC FireEye

En la sección de Guest Images (ver Figura. 3.58.) se detallan las versiones de las máquinas virtuales instaladas en el appliance que simulan los sistemas operativos.



Guest Images

Below is a list of virtual machine "Guest Images" currently loaded on this FireEye system. It uses multiple instances of these guest images to safely test traffic and software for malicious activity.

Analysis Images:

Image Name	Version	Type
win7-base	12.1112	Analysis
win7-sp1	12.1112	Analysis
winxp-base	12.1112	Analysis
winxp-sp2	12.1112	Analysis
winxp-sp3	12.1112	Analysis

Figura. 3.58. Configuraciones de Guest Images de FireEye

En la sección de Appliance Licenses (ver Figura. 3.59.) se detalla el licenciamiento de la plataforma. La licencia CONTENT_UPDATES permitirá realizar la actualización de la plataforma, la licencia de FIREEYE_APPLIANCE permitirá el correcto funcionamiento del equipo y la licencia de FIREEYE_SUPPORT permitirá la asistencia del equipo de soporte de FireEye: ([34] FireEye, 2012)

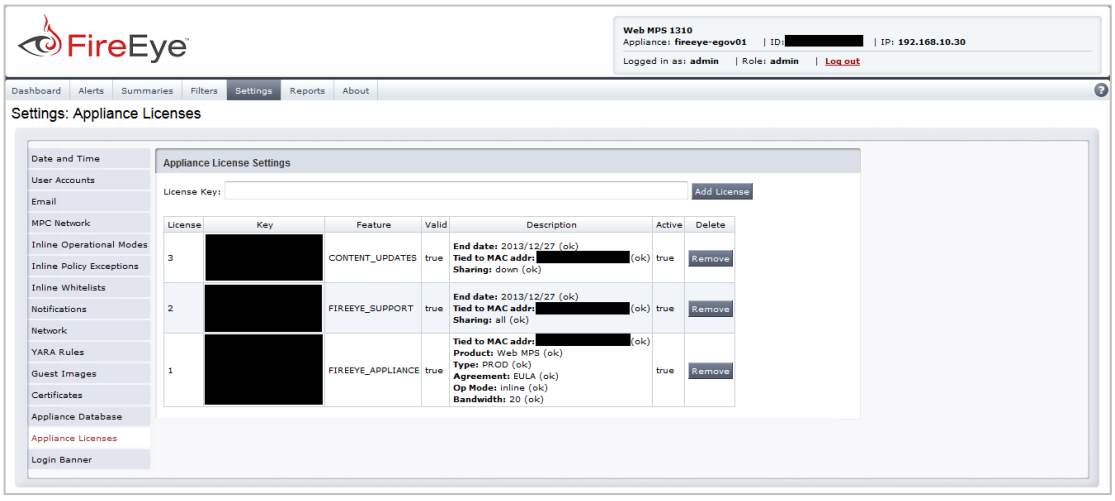


Figura. 3.59. Configuraciones de licenciamiento FireEye

En la sección de Inline Operational Modes (ver Figura. 3.60.) se configurará el modo de operación del equipo, en este caso se lo colocará en modo inline seleccionando la opción FS Open para que en caso de falla del equipo no exista interrupción del servicio y el tráfico pueda fluir sin problema.

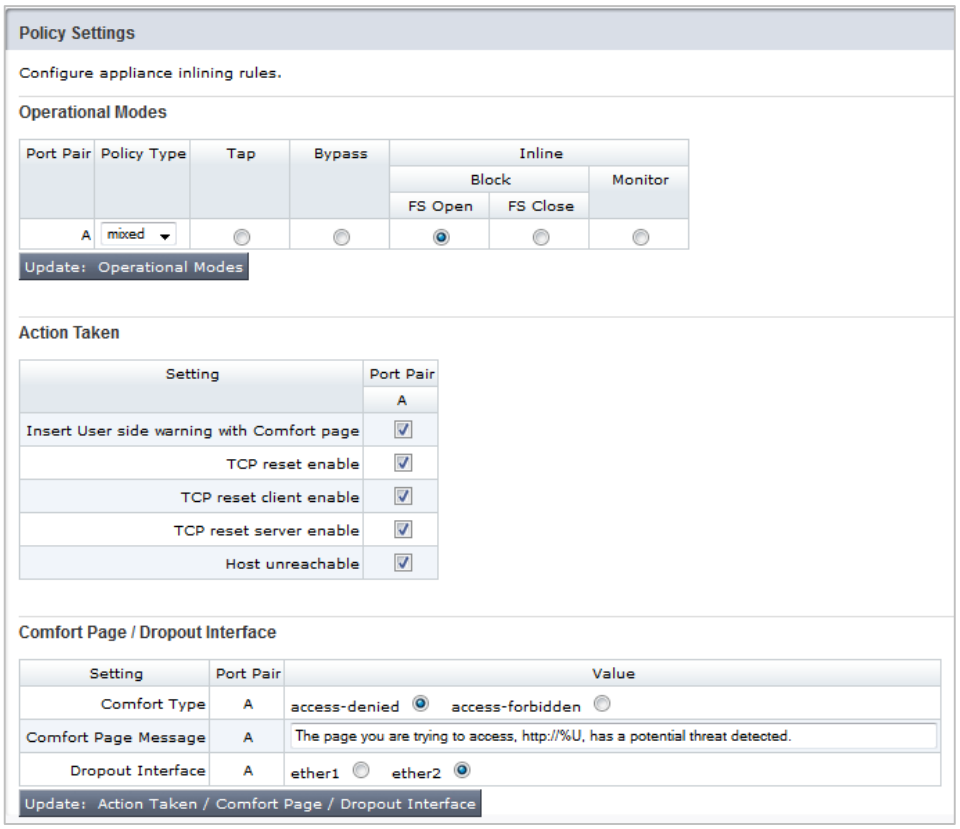


Figura. 3.60. Configuraciones de modo de operación FireEye

A nivel de reportes, la plataforma cuenta con cuatro tipos de reportes provistos de fábrica y que no pueden ser modificados:

- Callback Server Report
- Executive Summary
- Infected Hosts Trend
- Malware Activity

Cada reporte se puede generar en formato csv o pdf. Adicionalmente se pueden especificar las siguientes opciones de fecha:

- Última semana
- 1 mes
- 3 meses
- Rango de fechas específico

Las principales características del equipo y sus interfaces pueden ser visualizadas en la pestaña “About” (ver Figura. 3.61.).

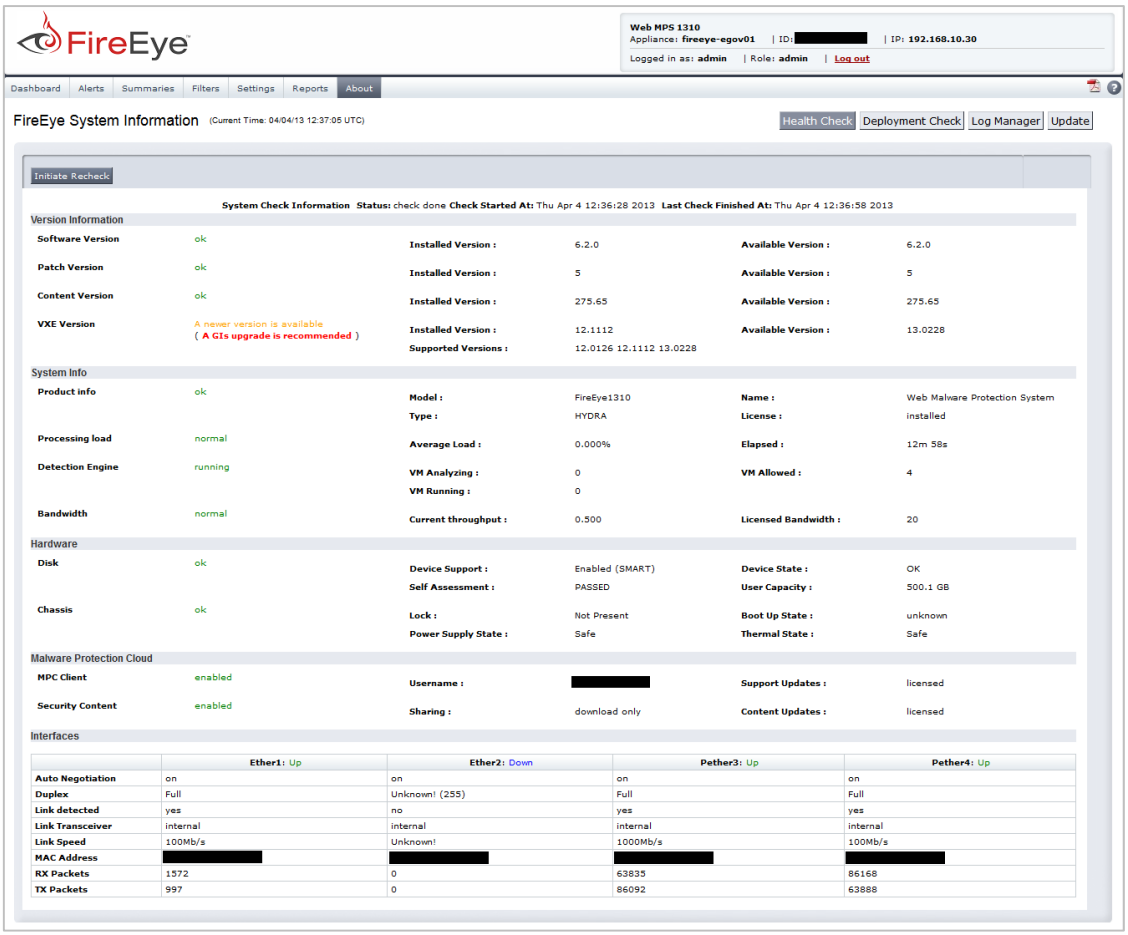


Figura. 3.61. Información del sistema FireEye

3.2.3. Snort

3.2.3.1. Modos de operación.

Snort principalmente posee 3 modos principales de operación los cuales son los siguientes:

- Modo de sniffer
- Modo de packet logger
- Modo de detección y prevención de intrusos

El modo de sniffer únicamente permitirá visualizar los paquetes en tiempo real en la consola.

El modo de packet logger nos permitirá registrar los paquetes en el disco para futuro análisis, lo cual demanda altas capacidades de almacenamiento.

El modo de detección y prevención de intrusos es el que requiere mayor complejidad en la configuración. En este modo Snort es capaz de analizar el tráfico a través de la red de manera que empate con un conjunto de reglas pre definidas por el usuario y configurar acciones basado en lo que ve. Este será el modo que se implementará, sin embargo Snort ha denotado mejores características como IDS que como IPS, esto debido a que al tener una gran cantidad de colaboración de la comunidad genera una gran cantidad de falsos positivos, así que debido a que Palo Alto Networks ya se encuentra configurado en modo de bloqueo, para el sistema integral propuesto, Snort nos ayudará de manera informativa y se lo configurará junto con un puerto SPAN para que no tenga influencia dentro del flujo de tráfico (ver Figura. 3.62.).

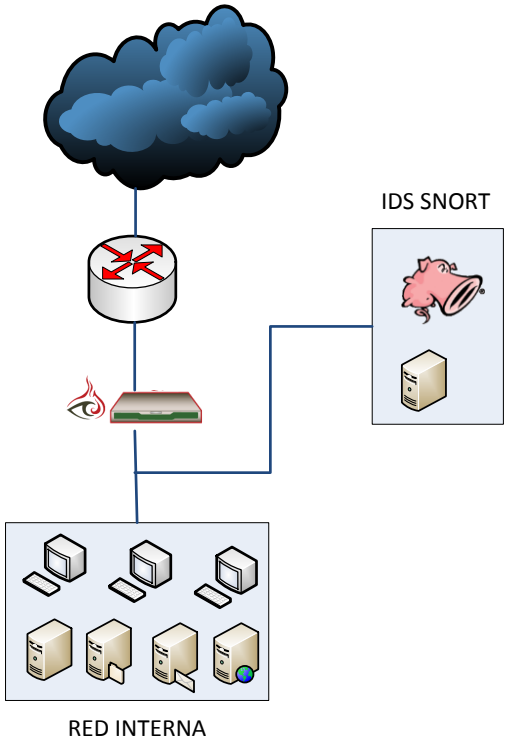


Figura. 3.62. Diagrama físico Snort

3.2.3.2. Configuración.

El equipo utilizado posee dos interfaces de red las cuales serán utilizadas de la siguiente manera:

- eth0.- puerto de administración
- eth1.- puerto de tráfico

A continuación se listan los parámetros de configuración TCP/IP implementados en el servidor (ver Tabla. 3.3).

#	Parámetro	Valor
1	Dirección IP	192.168.10.10
2	Máscara	255.255.255.0
3	Default Gateway	192.168.10.1
4	DNS	200.63.212.110 200.25.144.1
5	Usuarios Administradores	Root

Tabla. 3.3. Parámetros de Configuración Snort

Dentro del archivo de configuración de snort se realizarán las configuraciones principales del mismo, este archivo está ubicado en la siguiente ruta: /etc/nsm/angel-virtual-machine-eth0/snort.conf y a continuación se detallarán las secciones configuradas dentro del mismo.

Es necesario especificar el o los directorios de donde se tomarán los archivos de reglas que serán aplicadas. Para este caso todos los archivos de reglas se encontrarán en el directorio /etc/nsm/rules (ver Figura. 3.63.)

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH /etc/nsm/rules
var SO_RULE_PATH /etc/nsm/rules
var PREPROC_RULE_PATH /etc/nsm/rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/nsm/rules
var BLACK_LIST_PATH /etc/nsm/rules
```

Figura. 3.63. Directorio de reglas de Snort

Además se debe especificar los directorios (ver Figura. 3.64.) donde se encuentran las librerías de los módulos dinámicos (configuración por defecto) para mejorar la capacidad de detección dentro del código principal de SNORT.

```
##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory /usr/lib/snort_dynamicpreprocessor/

# path to base preprocessor engine
dynamicengine /usr/lib/snort_dynamicengine/libsf_engine.so

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Figura. 3.64. Librerías de los módulos dinámicos de snort

Posteriormente se debe especificar los archivos de reglas (dentro del directorio antes mencionado) que se desea aplicar al sensor. Para este caso se añadirán dos archivos de reglas que son los siguientes (ver Fig. 3.65).

- local.rules.- Archivo de reglas propias
- downloaded.rules.- Archivo de reglas que contiene las reglas oficiales de snort y las reglas de Emerging Threats

```
##################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
##################################################

# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/downloaded.rules
```

Figura. 3.65. Archivos de reglas de snort

Dentro de snort es posible especificar los rangos de IP's internas que perteneces a la red interna, las direcciones IP's de diferentes tipos de servidores (dns, smtp, web, sql, telnet, ssh, ftp, sip) (ver Figura. 3.66.) y los puertos aplicados a diferentes servicios (web, shellcode, oracle, ssh, ftp, file data, gtp) (ver Figura. 3.67.). Esto se realiza mediante la creación de variables que son muy utilizadas en las reglas antes mencionadas.

```
##################################################
# Step #1: Set the network variables.  For more information, see README.variables
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET

# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET
```

Figura. 3.66. Variables de red local y servidores utilizados por snort

```
# List of ports you run web servers on
portvar HTTP_PORTS [80,81,311,591,593,901,1220,1414,1830,2301
,2381,2809,3128,3702,4343,5250,7001,7145,7510,7777,7779,8000,
8008,8014,8028,8080,8088,8118,8123,8180,8181,8243,8280,8800,8
888,8899,9080,9090,9091,9443,9999,11371,55555]

# List of ports you want to look for SHELLCODE on.
portvar SHELLCODE_PORTS !80

# List of ports you might see oracle attacks on
portvar ORACLE_PORTS 1024:

# List of ports you want to look for SSH connections on:
portvar SSH_PORTS 22

# List of ports you run ftp servers on
portvar FTP_PORTS [21,2100,3535]

# List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]

# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]
```

Figura. 3.67. Variables de puertos asociados con servicios utilizados por snort

3.2.3.3. Envío de eventos (barnyard y mysql).

Para la investigación de eventos de snort, existe un programa específico llamado barnyard que permite el envío de eventos a una base de datos mysql para investigarlos mediante peticiones conocidas y también utilizar la misma para poder visualizar los eventos en una consola gráfica mediante a través del programa snorby.

Posterior a la instalación de barnyard es necesario editar ciertos parámetros en el archivo de configuración, el mismo que se encuentra ubicado en el siguiente directorio: /etc/nsm/angel-virtual-machine-eth0/barnyard2-1.conf. Dentro de este archivo se especificará el directorio de logs, el hostname, la interface, parámetros de la base de datos en la cual se guardarán los datos y los siguientes archivos configurados dentro de snort:

- reference_file → establece el formato de las referencias que aparecen en cada regla.

- classification_file → establece la clasificación de los grupos de reglas, cada una incluye un nombre corto, una descripción y una prioridad por defecto.
- gen_file → contiene el mapeo de todos los identificadores de generadores de manera que asocie un mensaje por cada gen_id.
- sid_file → contiene el mapeo de todos los identificadores de firma de manera que asocie un nombre por cada sig_id. (ver Figura. 3.68.)

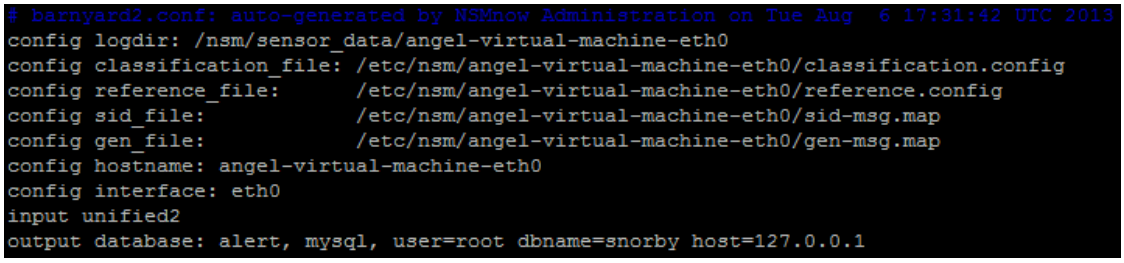


Figura. 3.68. Archivo de configuración de barnyard

La base de datos de mysql utilizada para el almacenamiento de las alertas se llama snorby. La cuál consta de las siguientes tablas:

- aggregated_events
- caches
- classifications
- daily_caches
- data
- delayed_jobs
- detail
- encoding
- event
- events_with_join
- favorites
- icmphdr
- iphdr
- lookups
- notes
- notifications
- opt
- reference
- reference_system
- search
- sensor
- settings
- severities
- sig_class
- sig_reference
- signature
- tcphdr
- udphdr
- users

La tabla más utilizada es la llamada “events_with_join”, la cual tendrá todos los detalles de las alertas (ver Figura. 3.69.).

```
mysql> DESCRIBE events_with_join;
+-------------------+------------------+------+-----+---------+-------+
| Field             | Type             | Null | Key | Default | Extra |
+-------------------+------------------+------+-----+---------+-------+
| sid               | int(11)          | NO   |     | NULL    |       |
| cid               | int(11)          | NO   |     | NULL    |       |
| signature         | int(11)          | YES  |     | NULL    |       |
| classification_id | int(11)          | YES  |     | NULL    |       |
| users_count       | int(11)          | YES  |     | 0       |       |
| user_id           | int(11)          | YES  |     | NULL    |       |
| notes_count       | int(11)          | YES  |     | 0       |       |
| number_of_events  | int(11)          | YES  |     | 0       |       |
| timestamp         | datetime         | YES  |     | NULL    |       |
| id                | int(11)          | NO   |     | 0       |       |
| ip_src            | int(10) unsigned | NO   |     | 0       |       |
| ip_dst            | int(10) unsigned | NO   |     | 0       |       |
| sig_priority      | int(11)          | YES  |     | NULL    |       |
| sig_name          | text             | YES  |     | NULL    |       |
+-------------------+------------------+------+-----+---------+-------+
14 rows in set (0.00 sec)
```

Figura. 3.69. Detalle de la tabla “events_with_join”.

Contra la tabla antes mencionada se pueden realizar una gran variedad de peticiones para la investigación de eventos (ver Figura. 3.70.).

```
mysql> SELECT COUNT(*) AS cnt, signature, sig_name FROM events_with_join GROUP BY signature
 ORDER BY cnt DESC LIMIT 5;
+------+-----------+-----------------------------------------------------------------+
| cnt  | signature | sig_name                                                        |
+------+-----------+-----------------------------------------------------------------+
| 9726 |       489 | ET POLICY PE EXE or DLL Windows file download                   |
| 1991 |       494 | ET POLICY Dropbox.com Offsite File Backup in Use                |
| 1403 |       510 | ET INFO Packed Executable Download                              |
| 1176 |       540 | GPL SNMP public access udp                                      |
| 1071 |       508 | ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)  |
+------+-----------+-----------------------------------------------------------------+
5 rows in set (0.00 sec)
```

Figura. 3.70. Ejemplo de petición a mysql para obtener los 5 eventos más detectados

3.2.3.4. Configuración de interfaz gráfica (Snorby)

Una vez realizada la instalación de Snorby, se puede acceder a la misma a través de https utilizando el puerto configurado (ver Figura. 3.71.)

Figura. 3.71. Pantalla de inicio de snorby

En la sección de configuraciones es posible editar las características del usuario logueado tales como nombre, correo electrónico y contraseña (ver Figura. 3.72.)

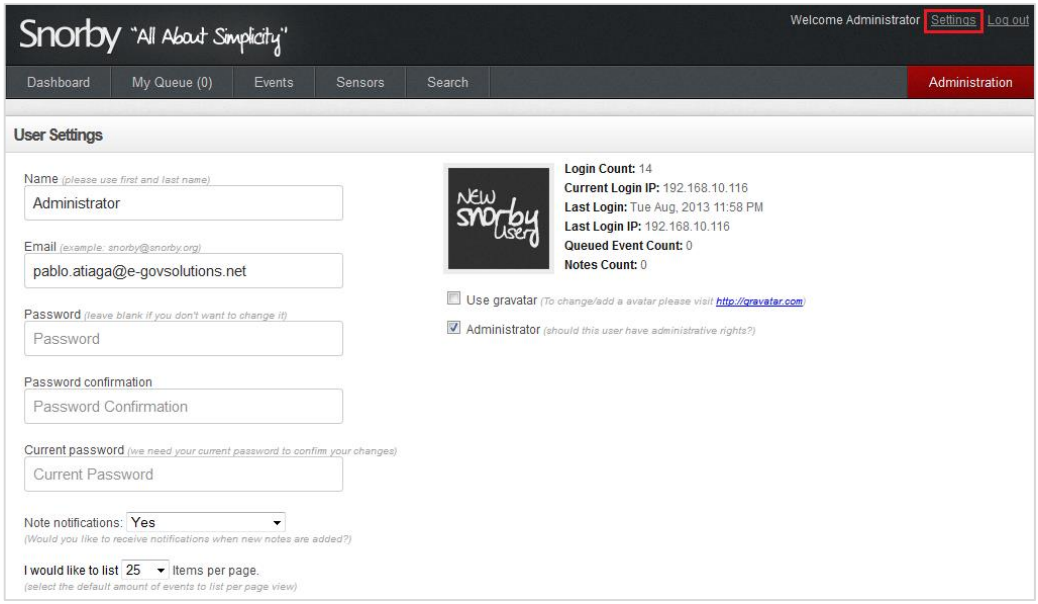


Figura. 3.72. Configuraciones de usuario de snorby

En la sección de configuraciones generales (Administration → General Settings) se podrá configurar el nombre y correo electrónico de la compañía

además de poder habilitar / deshabilitar características de repostería y visualización (ver Figura. 3.73.)

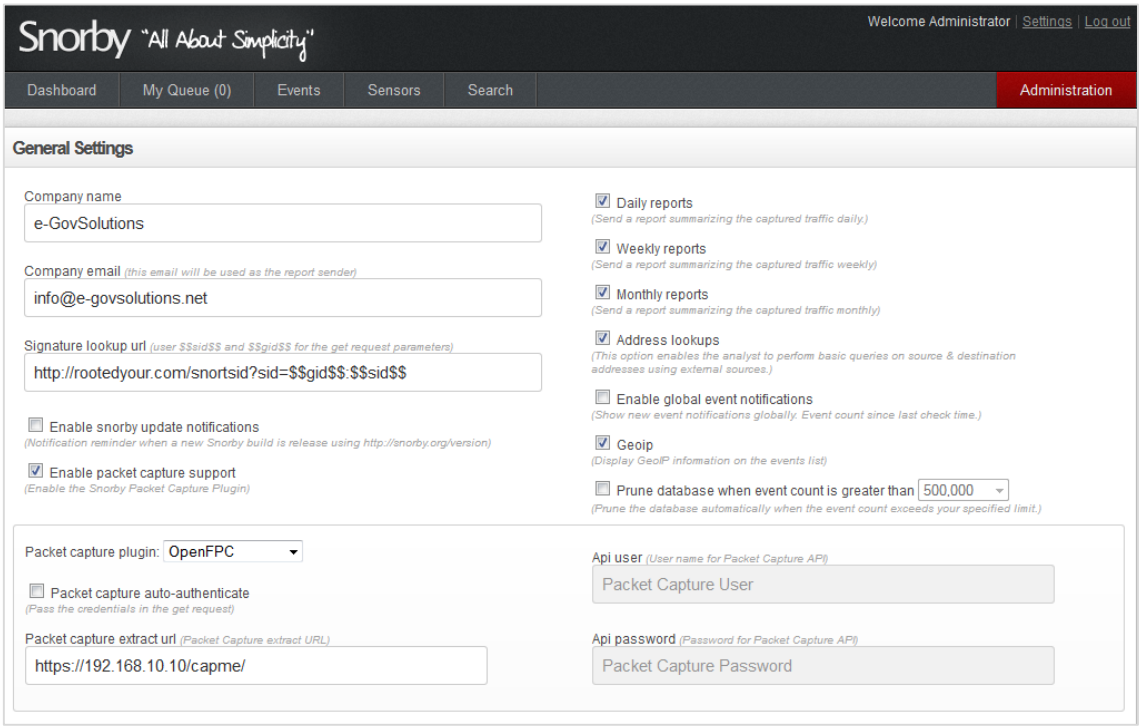


Figura. 3.73. Configuraciones generales de snorby

En la sección de administración de usuarios (Administration → Users) se podrá administrar los usuarios que tienen acceso a la consola de snorby (ver Figura. 3.74.).

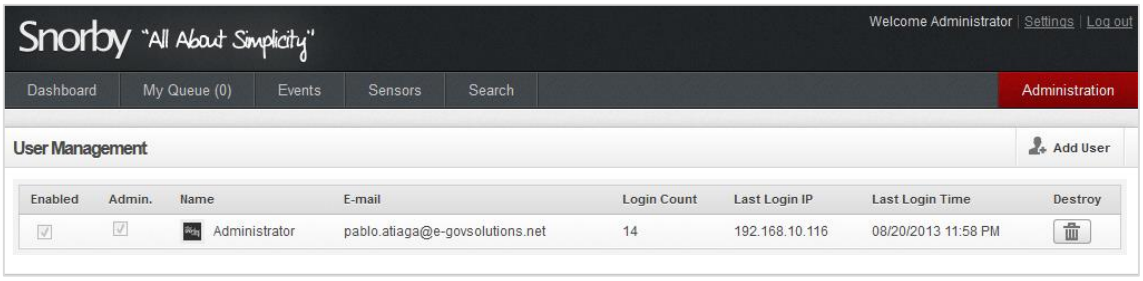


Figura. 3.74. Administración de usuarios de snorby

3.2.3.5. Aplicación de reglas.

Existen dos principales grupos de reglas que se recomiendan aplicarlos dentro de snort.

El primero es el grupo de reglas certificado por el grupo de investigación de vulnerabilidades (Vulnerability Research Team o VRT) de SourceFire, las cuáles pueden ser descargadas como usuario registrado o suscrito. El usuario registrado puede descargar el grupo de reglas de manera gratuita con la desventaja de poder hacerlo 30 días después de que las mismas hayan sido lanzadas, en cambio el usuario suscrito debe pagar un valor anual (dependiendo si es empresarial o para uso personal) y este si puede descargar las reglas el mismo día que son lanzadas. ([35] Sourcefire Inc., 2013)

El segundo grupo es el realizado por Emerging Threats, la cual es una organización de investigación de seguridad cibernética que empuja los límites de detección de amenazas, prevención y neutralización, cuya prioridad es proporcionar una cobertura completa, rápida e innovadora. Este grupo de reglas es posible descargarse de manera gratuita y actualizada, sin embargo hay como bajarse una versión profesional, la cual es pagada y tiene la ventaja de ofrecer soporte y una mayor cobertura de vulnerabilidades y malware. ([36] Emerging Threats Pro, LLC., 2013)

Los archivos de reglas se los puede descargar independientemente, sin embargo en este caso se han colocado todas estas reglas dentro del archivo “downloaded.rules”.

3.2.3.6. Afinamiento de reglas.

En el archivo /etc/nsm/angel-virtual-machine-eth0/threshold.conf es posible realizar un afinamiento de reglas de manera que se puedan eliminar falsos positivos y concentrarse en alertas verdaderas. Esto se hace a través de los identificadores de alerta gen_id y sig_id (gen_id 1, sig_id=0 quiere decir que es aplicable para todas las alertas) de la siguiente manera:

- Para prevenir el exceso de alertas se ha establecido que Snort únicamente dispare una alerta cada 6 minutos en caso de que el mismo host genere la misma repetidamente.

  threshold gen_id 1, sig_id 0, type limit, track by_src, count 1, seconds 360
- Para la supresión de falsos positivos o alertas informativas.

suppress gen_id 1, sig_id 2003410

De esta forma se deben realizar análisis semanales (debido a la actualización de reglas), de manera que se puedan suprimir diferentes reglas que no tengan un gran valor e ir aumentándolas en el archivo threshold.conf (ver Figura. 3.75.)

```
#Only show 1 event per 6 minutes
threshold gen_id 1, sig_id 0, type limit, track by_src, count 1, seconds 360

#ETC POLICY FTP LOGIN SUCCESSFULL
suppress gen_id 1, sig_id 2003410

#GPL WEB_SERVER 403 FORBIDDEN
suppress gen_id 1, sig_id 1201
suppress gen_id 1, sig_id 2101201

#GPL NETBIOS SMB_DS IPC UNICODE SHARE ACCESS
suppress gen_id 1, sig_id 2102466

#ET CHAT GENERAL MSN CHAT ACTIVITY
suppress gen_id 1, sig_id 2009375

#ET CHAT FACEBOOK CHAT
suppress gen_id 1, sig_id 2010785

#ET POLICY Dropbox Client Broadcasting
suppress gen_id 1, sig_id 2012648

#ET POLICY TeamViewer Keep-alive inbound
suppress gen_id 1, sig_id 2008795

#ET CHAT MSN status change
suppress gen_id 1, sig_id 2002192

#ET POLICY Skype User-Agent Detected
suppress gen_id 1, sig_id 2002157

#ET POLICY RDP connection confirm
suppress gen_id 1, sig_id 2001330

#GPL ICMP_INFO PING Cisco Type.x
suppress gen_id 1, sig_id 2100371
```

Figura. 3.75. Archivo threshold.conf

3.2.4. ModSecurity

3.2.4.1. Modos de operación

ModSecurity se puede implementar de dos modos: ([26] Ristic, 2012)

- Embebido

- Puerta de enlace de red

En el modo embebido solo se debe añadir a ModSecurity como un módulo dentro de la infraestructura del servidor web, ya que ModSecurity es un WAF integrable, en este modo no se puede analizar el contenido de los encabezados del servidor. Cuando un módulo es compilado de esta manera, se obtiene como resultado un ejecutable más veloz, aunque su compilación y posterior mantenimiento serán un poco más complicados.

El modo de puerta de enlace de red es el método recomendado ya que así se permite que todo el tráfico pase a través del WAF (ver Fig. 3.76), en este caso ModSecurity se instala como un proxy reverso. Si se instala junto con otros módulos se logrará tener un único punto de vigilancia, anonimato de la red y se podrá inspeccionar la cabecera del servidor de la base de datos. El objetivo es proteger a los servidores Web que se encuentran en la red interna y que prestan servicios a clientes externos. Cuando más servidores internos existen; el concepto de proxy inverso es más útil.

El proxy reverso hace exactamente lo contrario que un proxy de reenvío, ya que se ubica entre un servidor y todos los clientes, por lo que se lo utilizará para todos los servidores web internos.

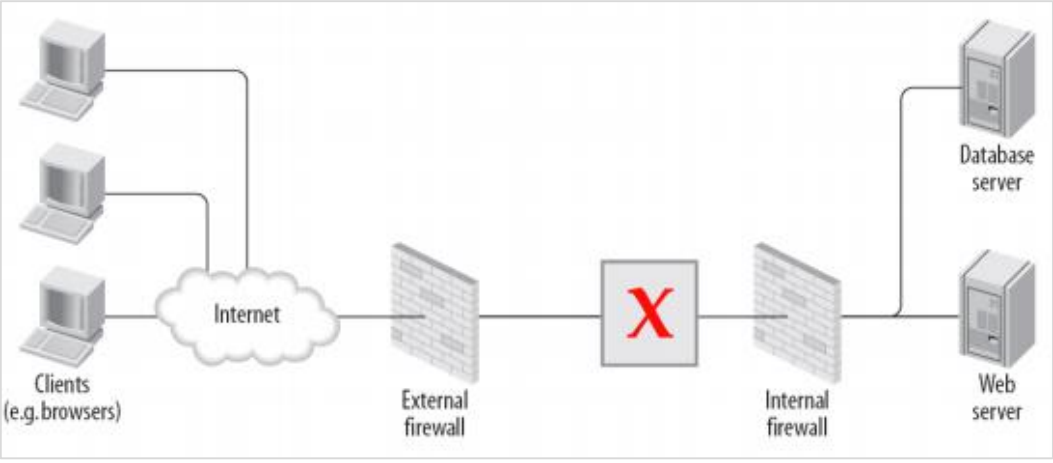


Figura. 3.76. ModSecurity en modo de puerta de enlace de red ([26] Ristic, 2012)

La principal ventaja de utilizar un proxy reverso es que todo el tráfico irá de manera centralizada, donde tendremos un único punto de monitoreo en el cual podemos aplicar otras herramientas para controlar dicho tráfico.

Para este caso se utilizará el modo embebido, es decir instalado en el mismo servidor que la aplicación web.

3.2.4.2. Configuración.

Se inicia con la descarga de ModSecurity desde la página oficial, la versión a descargar será la v.2.7.3 (ver Figura. 3.77.)

Figura 3. 77 Descarga de ModSecurity ([37] Trustwave's SpiderLabs Team, 2013)

Se descomprime el archivo descargado dentro la carpeta donde está ubicado el servidor apache (ver Fig. 3.78.).

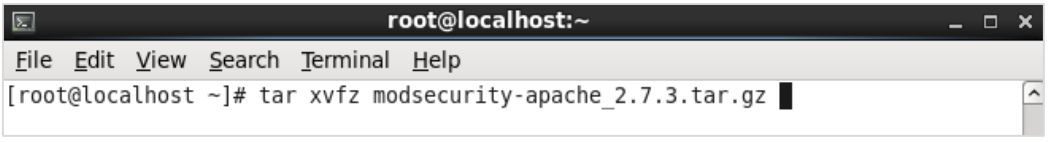


Figura. 3.78. Descompresión del ModSecurity

Es necesario editar el archivo de configuración de apache con las librerías de ModSecurity (ver Figura. 3.79.) para posteriormente realizar la instalación de estos módulos (ver Figura. 3.80.)

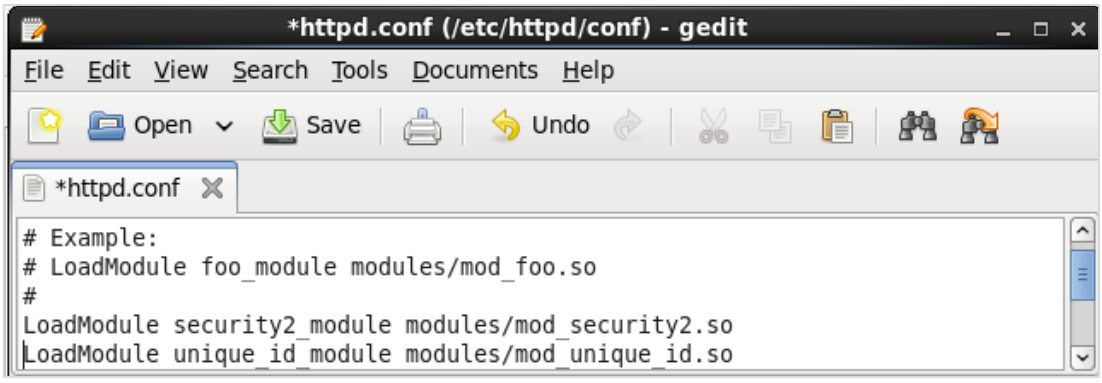


Figura 3. 79 Edición del archivo de configuración de apache con las librerías de ModSecurity

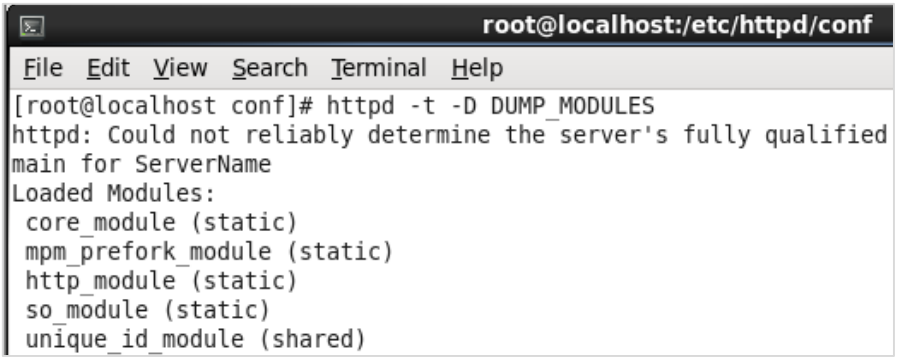


Figura. 3.80. Instalación de los módulos de ModSecurity

Se ejecuta el script de configuración (ver Figura. 3.81.) para posteriormente realizar la compilación de la misma (ver Figura. 3.82.).

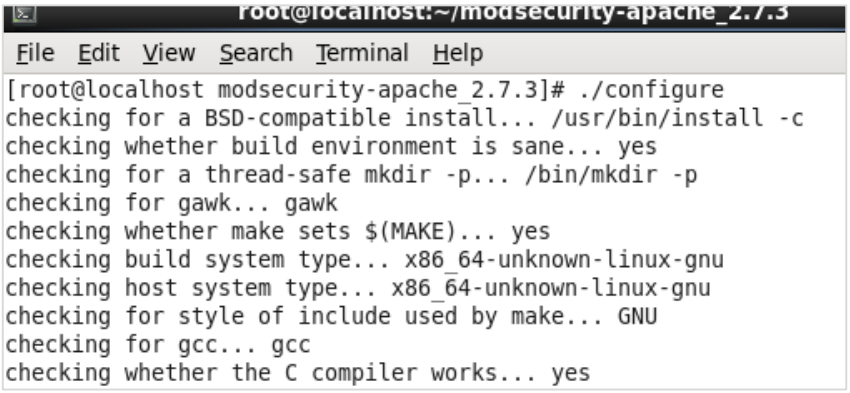


Figura. 3.81. Script de configuración de ModSecurity

Figura. 3.82. Compilación de ModSecurity

Finalmente se comprueba que la instalación haya sido realizada adecuadamente (ver Figura. 3.83.) y se procederá a reiniciar el servidor web (ver Figura. 3.84.).

```
[root@localhost conf]# apachectl configtest
httpd: Could not reliably determine the server's fully qualified domain name
Syntax OK
```

Figura. 3.83. Comprobación de la instalación de ModSecurity

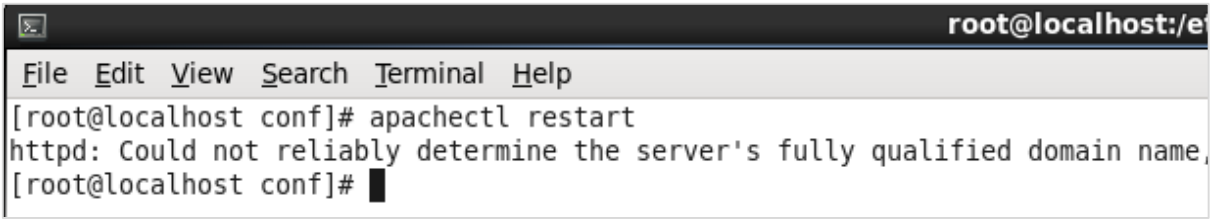


Figura. 3.84. Reinicio del servidor apache posterior a la instalación de ModSecurity

A continuación es posible visualizar y editar el archivo de configuración de ModSecurity para observar, habilitar y deshabilitar reglas para su correcto funcionamiento (ver Figura. 3.85.).

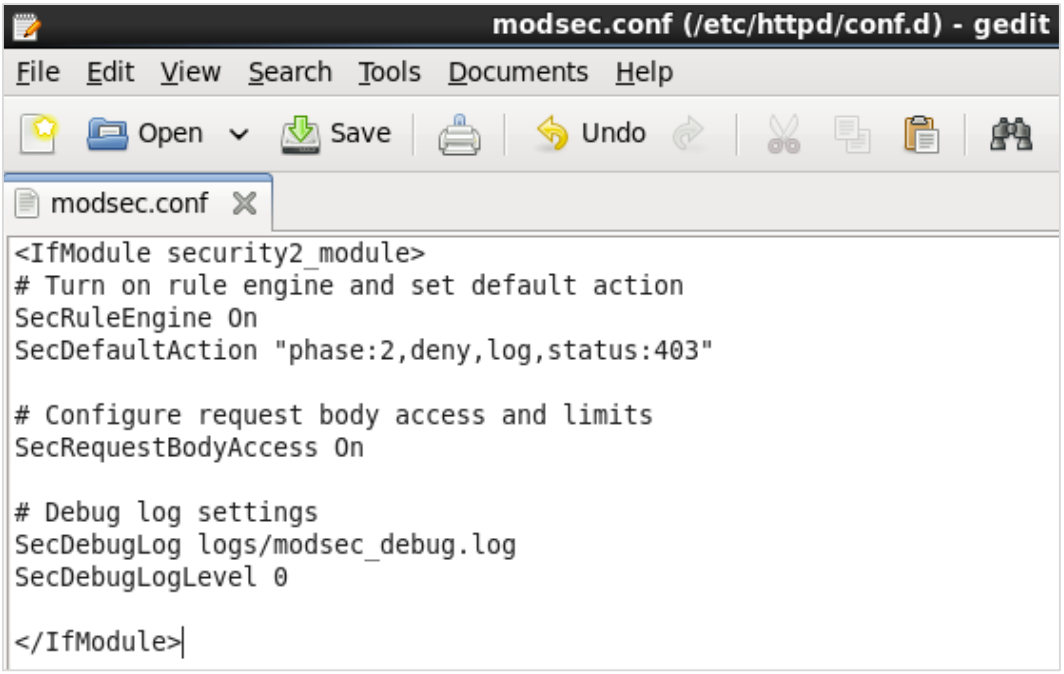


Figura. 3.85. Edición del archivo de configuración de ModSecurity

Para comprobar el correcto funcionamiento de ModSecurity, se sugiere crear una página web con el nombre secret.html y posteriormente crear una regla para bloquear todo el tráfico dirigido a la aplicación web que contenga la palabra secret. Para esto, lo primero es crear el archivo HTML (ver Figura. 3.86.) y comprobar el acceso desde un navegador (ver Figura. 3.87.).

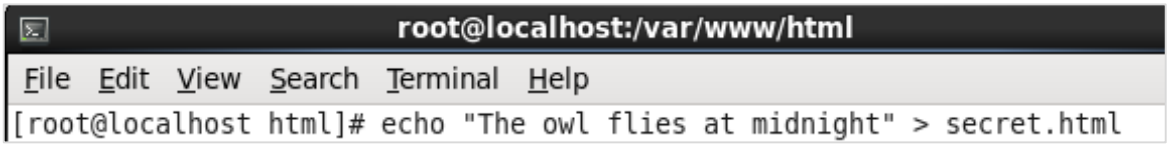


Figura 3. 86 Creación de la página secret.html para comprobar funcionamiento de ModSecurity

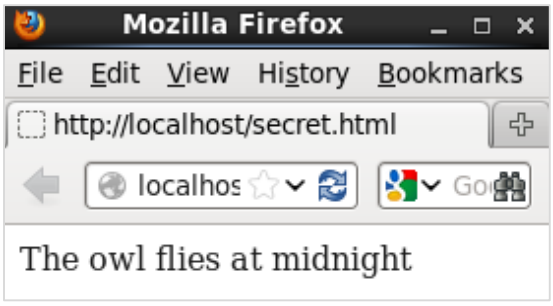


Figura. 3.87. Funcionamiento de la página secret.html para comprobar funcionamiento de ModSecurity

La siguiente prueba consiste en habilitar la regla que denegará el acceso de páginas que contengan la frase secret dentro de las mismas (ver Figura. 3.88.) y comprobar su correcto funcionamiento cuando se intenta ingresar por medio de un navegador (ver Figura. 3.89.).

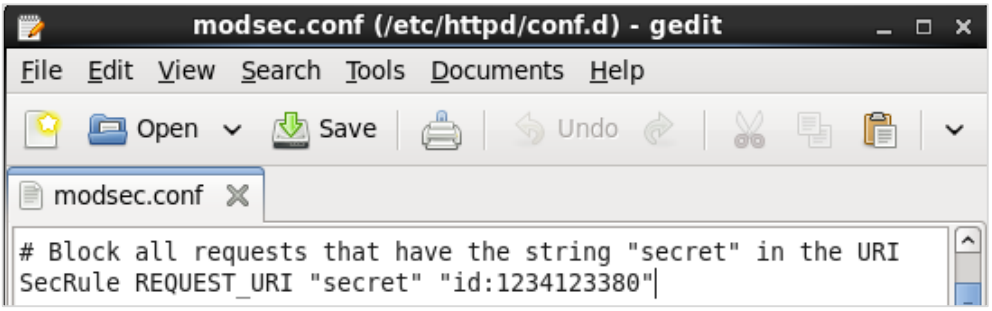


Figura. 3.88. Habilitación de la regla secret para comprobar funcionamiento de ModSecurity

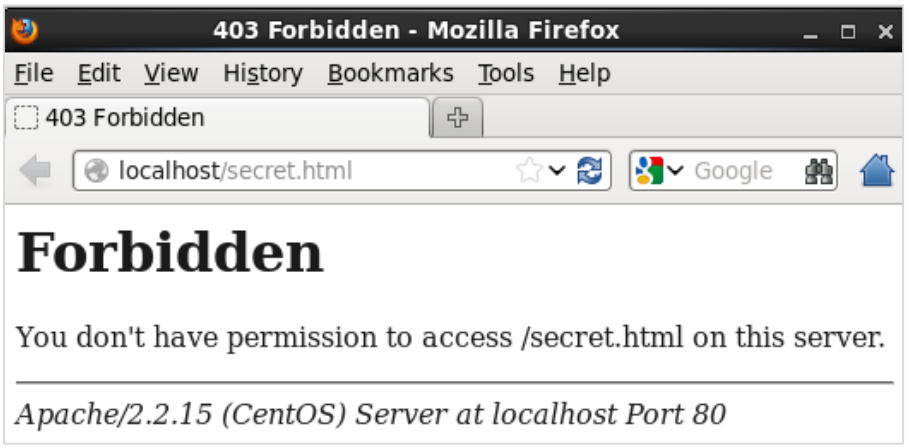


Figura. 3.89. Habilitación de la regla para comprobar funcionamiento de ModSecurity

Como se observa en la imagen anterior, encontramos fácilmente la versión del sistema operativo y de apache con la que se está trabajando, lo cual se convierte en un blanco para los atacantes, pues conociendo estos datos se pueden explotar las vulnerabilidades existentes.

El objetivo es enmascarar el servidor y poner como si se estuviera trabajando con una versión más antigua de apache, para que el atacante piense que se tiene una brecha de seguridad en el servidor.

Si se ingresa desde otra máquina, únicamente se debe anteceder la dirección IP seguido por la página web creada (ver Figura. 3.90.). Además se observa cómo se enmascara el servidor mostrando lo que desee el administrador, en este caso una versión desactualizada de apache.

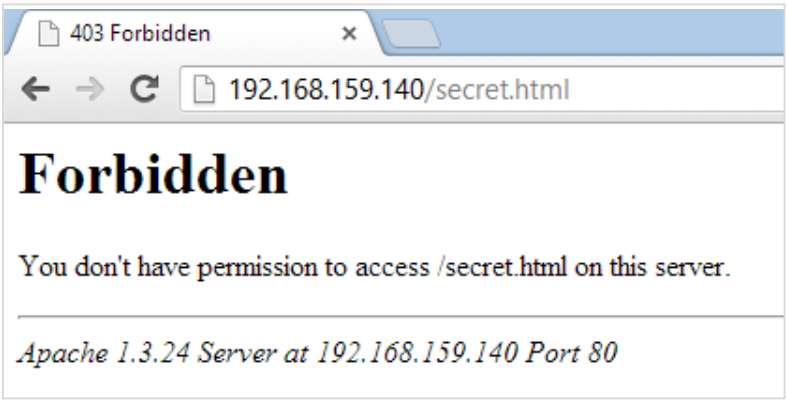


Figura. 3.90. Ingreso externo a página web

Como anteriormente se mencionó ModSecurity es poco útil si no se crean o cargan reglas para su funcionamiento. Por lo cual OWASP, en su página oficial entrega un conjunto de reglas las cuales están disponibles para su descarga gratuita. ([38] OWASP, 2013)

Es necesario descargarlas dentro del directorio de apache donde se creará una carpeta denominada ModSecurity-crs la cual incluirá todas las reglas (ver Figura. 3.91.).

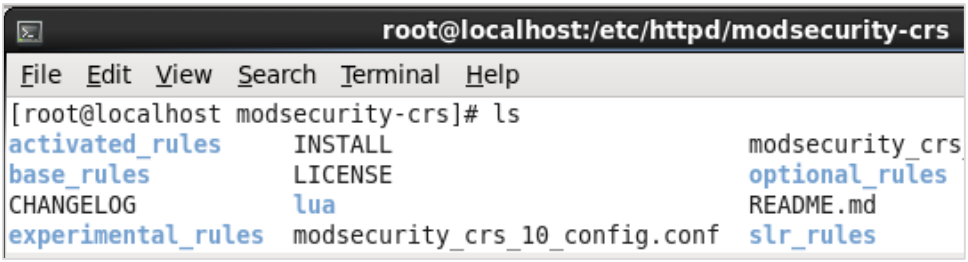


Figura. 3.91. Creación de carpeta para la descarga de reglas de OWASP relacionadas con ModSecurity

Dentro del archivo de configuración de apache, se cargará el módulo necesario para el funcionamiento de las reglas (ver Figura. 3.92.).

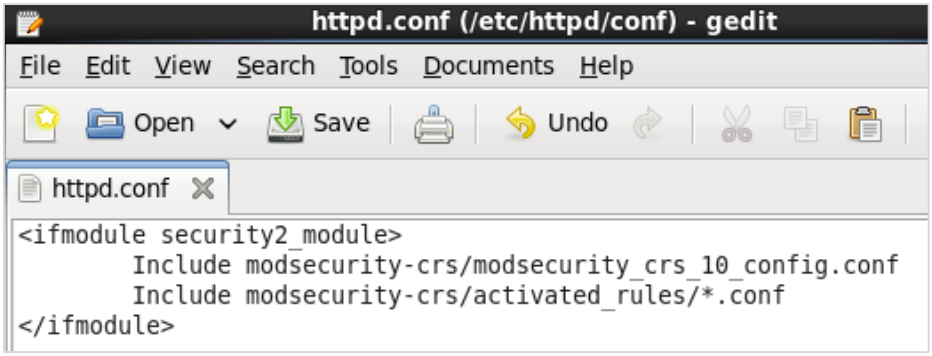


Figura. 3.92. Carga de reglas de OWASP relacionadas con ModSecurity

3.2.4.3. Creación de políticas

La función del motor de reglas de ModSecurity es realizar análisis de los datos recogidos comprobándolos con un contenido malicioso o un contenido previamente creado. Las reglas son directivas que se ubican en el archivo de configuración, con lo cual se decide qué hacer con los datos recibidos.

El lenguaje de reglas es bastante amplio ya que no solo existen reglas previamente definidas sino que también el administrador puede crear su conjunto de reglas restringiendo así los movimientos de su red.

En este punto se estudiará la creación de reglas básicas, y su formato de sintaxis para el posterior uso de las mismas

La principal directiva utilizada para crear reglas es SecRules y esta es su sintaxis: ([25] Mischel, 2009)

SecRule VARIABLES OPERATOR [ACTIONS]

Donde:

VARIABLES.- Especifica los lugares que se visitará durante una transacción HTTP. Se reprocesan datos de las transacciones, por lo que las normas se centrarán en la detección. Las variables se dividen en petición al servidor, variables

de respuesta, banderas de análisis y variables de tiempo. En una sola directiva se pueden utilizar más de una variable utilizando el símbolo pipe (|).

OPERATORS.- Especifica un patrón o palabra clave que va a ser controlada por la variable. Hay cuatro tipos de operadores: cadenas, numéricos, validación y operadores misceláneos. Los operadores siempre inician con el signo arroba (@) y van seguidos por un espacio.

ACTIONS.- Especifica que acción se debe tomar si al evaluar la regla coincide con los parámetros impuestos, es decir es la tarea que efectuará ModSecurity, puede ser un mensaje de error o la acción que se establezca. Existen siete categorías: acciones disruptivas, flujo, metadatos, variable, registro especial y varios.

3.2.5. BotHunter

3.2.5.1. Modos de operación

BotHunter solamente tiene un modo de operación y ese el modo escucha, este no puede tomar acción sobre el tráfico que visualiza debido a su análisis por comportamiento por lo que se lo debe ubicar mediante un puerto SPAN creado en la salida de tráfico hacia internet (ver Figura. 3.93.).

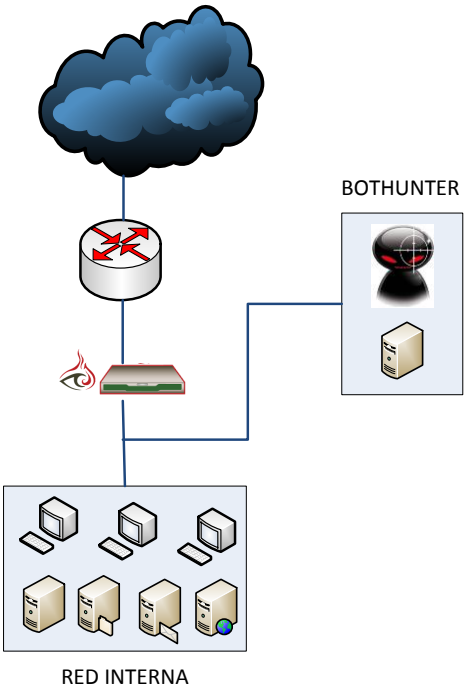


Figura. 3.93. Diagrama físico BotHunter

3.2.5.2. Configuración

Se ingresará a la cuenta en donde se realizó la configuración del sistema, en este caso el usuario se llama cta-bh1 (ver Figura. 3.94.). ([28] Phillip Porras, 2012)

```
Enter the name of the user under which to run the BotHunter software
(default cta-bh -- will be created): cta-bh1
```

Figura. 3.94. Cuenta de BotHunter

Se debe ingresar al modo de configuración mediante el comando “BotHunter configure” y es necesario detener cualquier proceso que se encuentre corriendo en ese momento (ver Figura. 3.95.).

Figura. 3.95. Ingreso al modo de configuración de BotHunter

Posteriormente es posible modificar los parámetros de entrada, para este caso de dejarán los mismos en los valores por defecto (ver Figura. 3.96.).

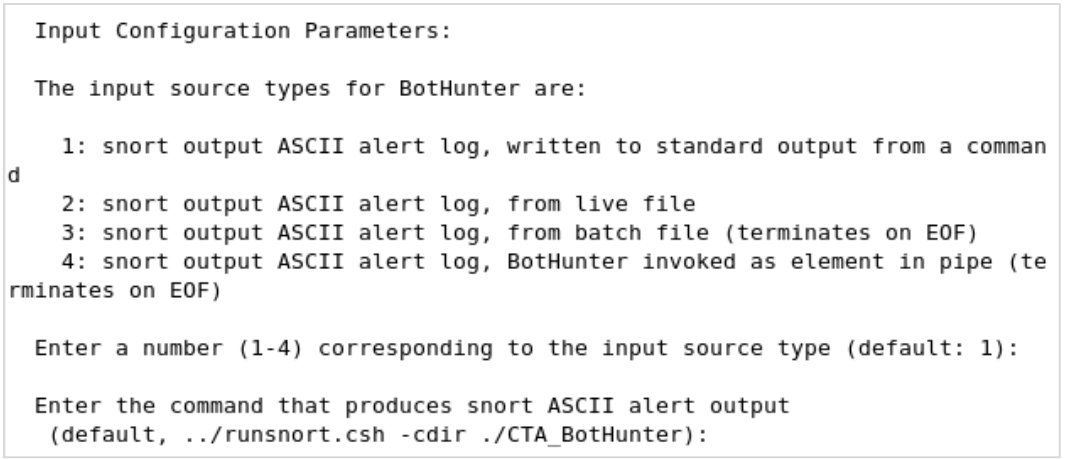


Figura. 3.96. Parámetros de entrada para BotHunter

A continuación se configurarán los parámetros que se modificarán automáticamente en el archivo de configuración de snort.

El primer parámetro configurado será la lista de redes que pertenecen a la red interna (ver Figura. 3.97.).

Figura. 3.97. Red segura para BotHunter

Posteriormente es opcional configurar los servidores SMTP (ver Figura. 3.98.) y DNS (ver Figura. 3.99.), las cuales son variables utilizadas por snort en algunas reglas específicas.

Figura. 3.98. Servidor SMTP

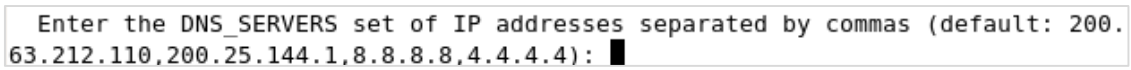


Figura. 3.99. Servidor DNS

Para configurar la interfaz de tráfico, el instalador mostrará cuáles son las interfaces que fueron detectadas, para este caso se escogerá la interfaz eth1 (ver Figura. 3.100.), pues ahí es donde se encuentra configurado el puerto SPAN

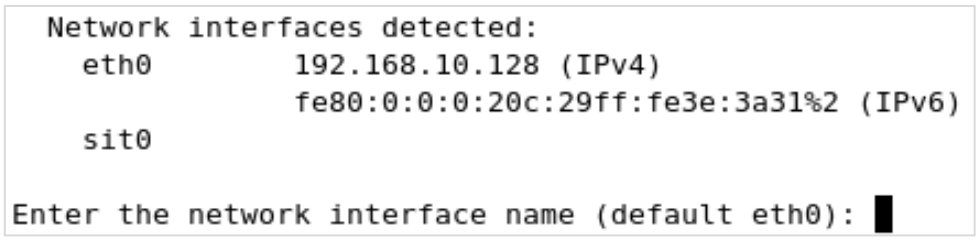


Figura. 3.100. Interface de red

Posteriormente se configurará los parámetros de salida que servirán para la actualización de BotHunter y manejo de logs, configurando inicialmente el método de acceso al repositorio (ver Figura. 3.101.).

```
Output Configuration Parameters:

This version can send the anonymized bot profiles to at most
one repository.

The repository access method can be
   proxyssl -- SSL connection through TOR proxy to repository
   ssl      -- Direct SSL connection to repository
   none     -- No data to a repository

Enter the repository access method (default ssl): ssl
```

Figura. 3.101. Método de acceso al repositorio de BotHunter

Es necesario configurar la dirección IP del repositorio donde se actualizan las firmas y reglas de malware (ver Figura. 3.102.).

```
Cyber-TA BotHunter Repository at SRI Menlo Park is at 130.107.10.11.

Enter the destination repository (default 130.107.10.11):
```

Figura. 3.102. Dirección IP del repositorio de BotHunter

En posible especificar el modo de actualización de las firmas y reglas, el cual se seleccionará como automático (ver Figura. 3.103.).

```
Enter the remote update service mode (default: automatic): automatic
```

Figura. 3.103. Modo de actualización de BotHunter

Opcionalmente se pueden realizar las configuraciones de logs, pero para fines prácticos, los mismos se pueden dejar en sus valores por defectos (Ver Figura. 3.104.).

```
    3) Output parameters:
       Destination repository:              ssl to 130.107.10.11 (Cyber-TA Bot
Hunter Repository at SRI Menlo Park) on port 6282
       Remote update service:               automatic
       Local binary output file:            botProfiles_%dt.bin
         Rotate binary output by interval:  1440 minutes
           Adjust interval alignment by:    localtime
       Local text output file:              botHunterResults_%dt.txt
```

Figura. 3.104. Configuraciones de logs de BotHunter

3.2.6. KFsensor

3.2.6.1. Modos de operación

KFSensor solamente tiene un modo de operación y ese es que sea instalado dentro de la zona de servidores justamente para que simule ser un servidor más del entorno de red. Para este caso se le ubicará como parte de la DMZ (ver Figura. 3.105.). ([29] Keyfocus Ltda., 2013)

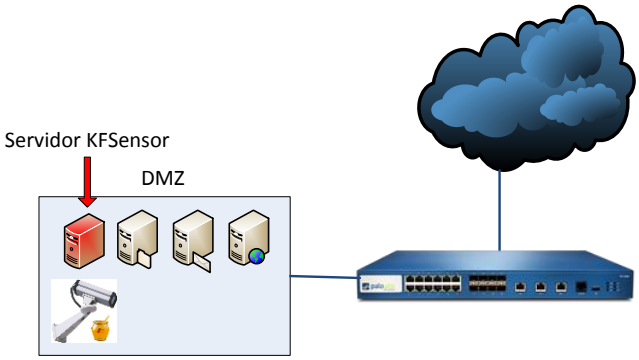


Figura. 3.105. Diagrama físico KFSensor

3.2.6.2. Configuración

Para la configuración, el primer paso que se tiene que indicar la carpeta donde se realizará la instalación (ver Figura. 3.106.)

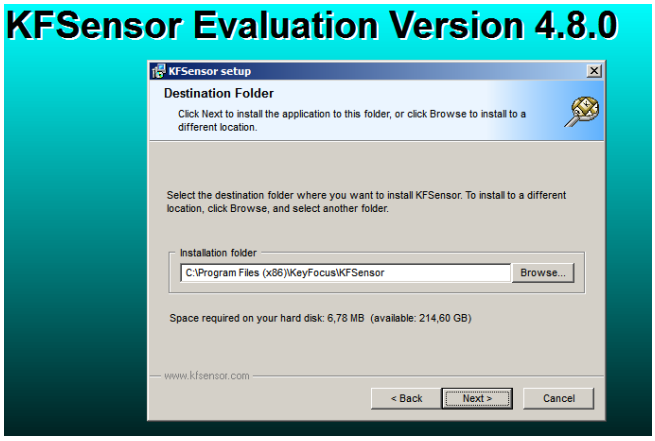


Figura. 3.106. Carpeta de instalación de KFSensor

KFSensor puede detectar ataques en diferentes puertos, es necesario indicar las clases de puertos a ser utilizados en los diferentes escenarios (ver Figura. 3.107.).

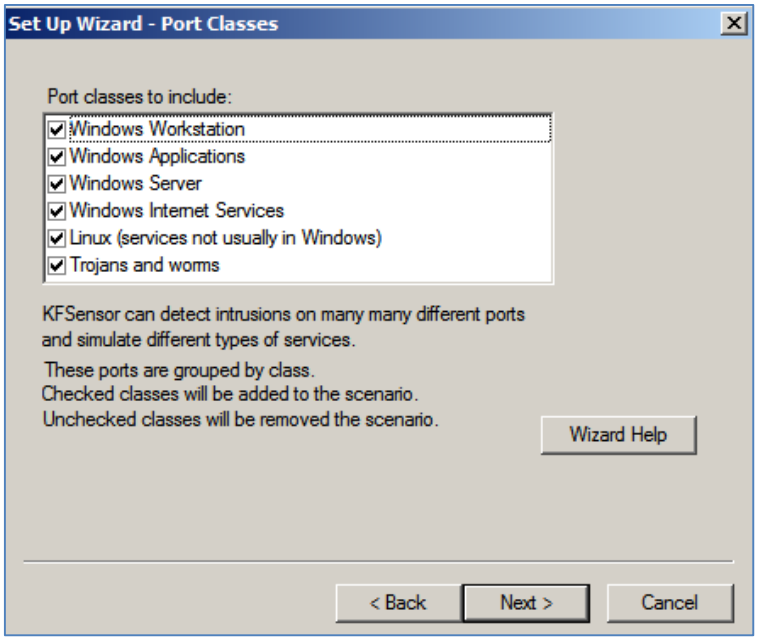


Figura. 3.107. Clases de puertos a ser utilizados en KFSensor

Al igual que cualquier servidor, es posible configurar el nombre del dominio (ver Figura. 3.108.); el mismo que sirve para ser identificado en cada uno de los servicios y además en el escenario respectivo.

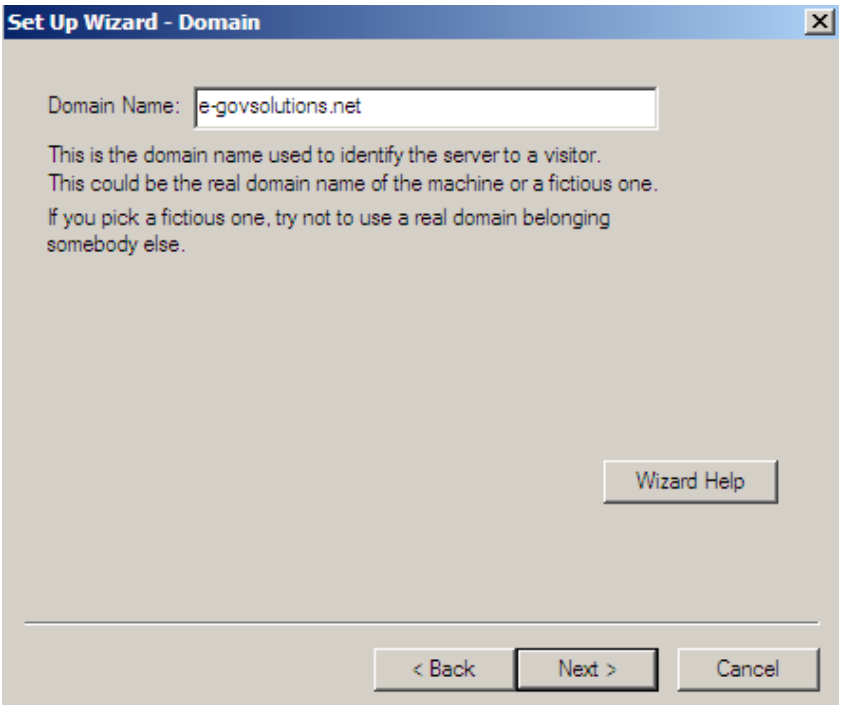


Figura. 3.108. Dominio señuelo de KFSensor

A continuación se debe configurar las siguientes opciones (ver Figura. 3.109.):

- Denial of Service: permite especificar el máximo de eventos antes de bloquear el acceso por parte de la dirección IP atacante.
- Port Activity: permite especificar durante cuánto tiempo un puerto/servicio muestra una actividad y un evento generado.
- Proxy Emulation: para controlar si los servicios de KFSensor pueden conectarse hacia servidores externos.
- Network Protocol Analyzer: permite configurar la captura de tráfico en formato .pcap.

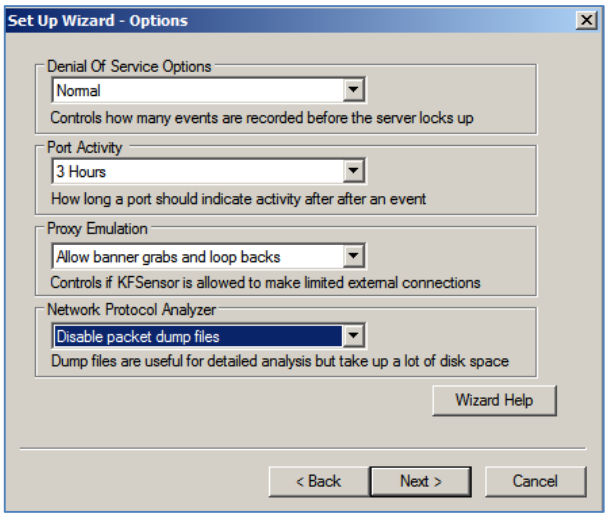


Figura. 3.109. Configuración de opciones de KFSensor

Es necesario realizar la configuración de las interfaces que se utilizarán para montar los servicios simulados (ver Figura. 3.110.).

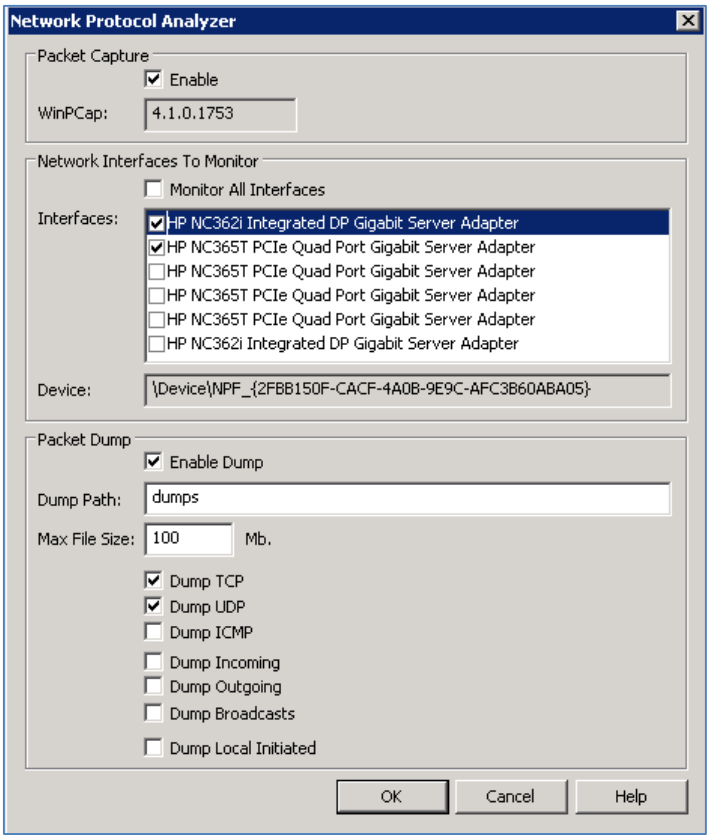


Figura. 3.110. Configuración de interfaces de KFSensor

A continuación se realizará la configuración para el almacenamiento de los eventos en la base de datos MySQL (ver Figura. 3.111.)

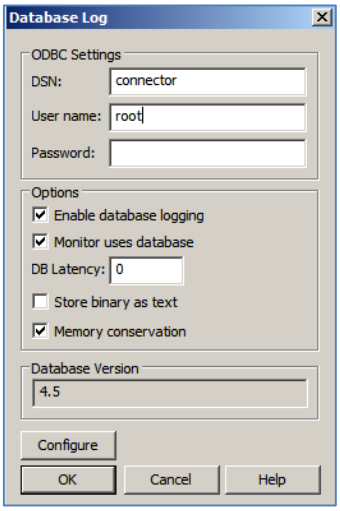


Figura. 3.111. Configuración de la base de datos de MySQL

Así también cabe recalcar que para elegir el guardado de eventos en las tablas se lo realizará en: kflog o kflogt respectivamente y con la dependencia de si guardar en la primera o segunda tabla seleccionando o no la opción ¨Store binary and text¨ de Settings -> Log Database. En este caso se guardará la información en la base de datos en la tabla kflogt: (ver Figura. 3.112.)

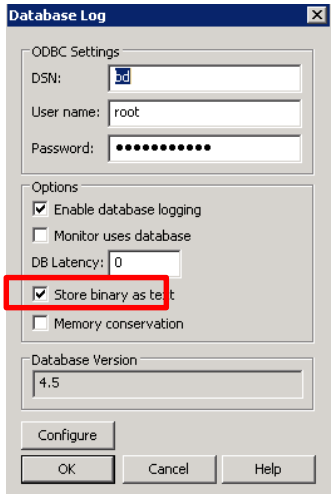


Figura. 3.112. Almacenamiento en la base de datos de KFSensor

Posteriormente se mostrará los escenarios creados (ver Figura. 3.113.) y se editará la configuración de los mismo (ver Figura. 3.114.). Los escenarios contendrán todos los servicios simulados que deseamos montar sobre el servidor honeypot.

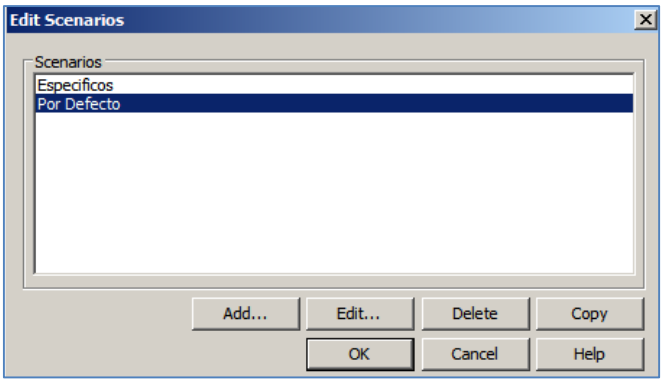


Figura. 3.113. Escenarios creados en KFSensor

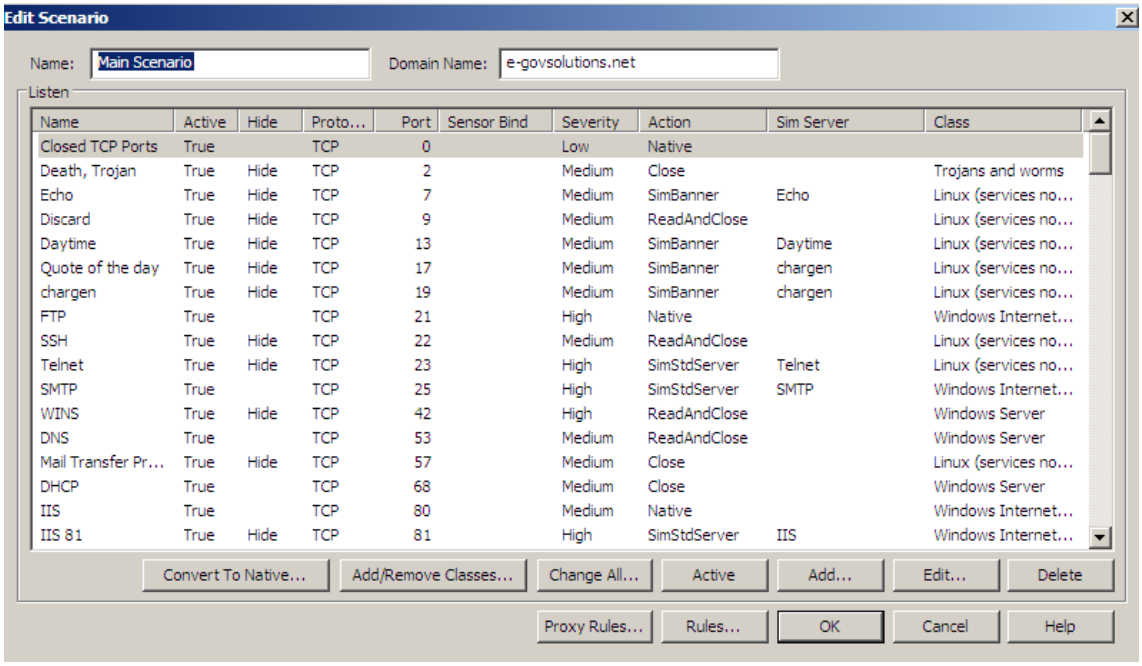


Figura. 3.114. Configuración de escenarios en KFSensor

A continuación y a modo de ejemplo, se muestra la configuración para el servicio FTP (ver Figura. 3.115.) simulado por KFsensor así como una descripción de los campos:

- Name: Nombre del servicio.
- Icon: Etiqueta gráfica para el servicio.
- Class: Etiqueta descriptiva del servicio.
- Protocol: Protocolo del servicio.
- Port: Número del servicio.
- Bind address: interfaz de ¨escucha¨ para el servicio.
- Action: Tipo de simulación para el servicio requerido.

- Severity: Severidad para cuando exista un posible cambio o interacción contra el servicio.
- Time Out: Tiempo para de cerrado de conexión del servicio.
- Sim Name: Lista de servicios simulados por el que KFsensor según el tipo de ¨Action¨ (Sim Banner, Sim Std Server).
- Visitors DOS attack Limit:
    - Max connections per IP: Número máximo de conexiones por IP.
    - Action on max connections per IP: Acción a tomar por número máximo de conexiones por IP (Lock Out/Ignore).

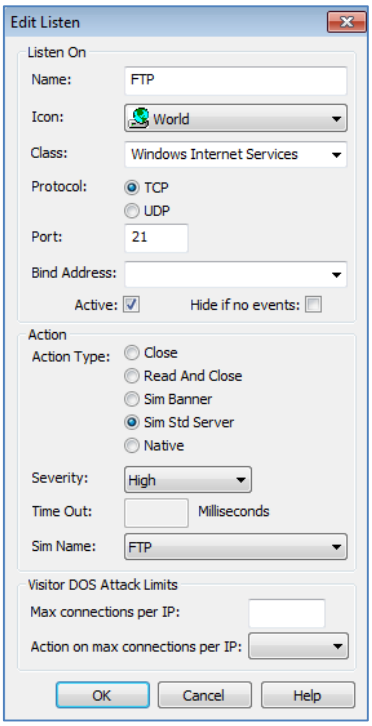


Figura. 3.115. Configuración de servicio FTP en KFSensor

3.2.6.3. Montaje de servicios.

En la Tabla. 3.4. se mostrará el escenario con los servicios/puertos simulados. ([29] Keyfocus Ltda., 2013)

#	SERVER	PORT	DESCRIPTION
1	CMD Command console	4444	The Command console Sim Std Server emulates the Windows command shell, otherwise known as a DOS box
2	DHCP	67	The Dynamic Host Configuration Protocol (DHCP) is a protocol which allows for the automatic configuration of networks. Its typical use is to assign dynamic IP address to computers on a network.
3	FTP	21	File Transfer Protocol
4	HTTP	80	An HTTP server is another name for a web server
5	MySql	3306	The MySql service
6	NBT Name Service	137	Windows File and print sharing
7	NBT Datagram Service	138	Windows File and print sharing
8	NBT Session Service	139	Windows File and print sharing
9	NBT SMB	445	Windows File and print sharing
10	POP3	110	Post Office Protocol. A POP3 server is used to store email messages, which can be retrieved using email applications like Microsoft Outlook.
11	Relay		A Relay server is used to allow visitors to access a service running on another machine
12	SMTP	25	Simple Mail Transfer Protocol. A SMTP server is used to accept incoming email messages.
13	E SOCKS	1080	A SOCKS proxy server is used to relay all types of TCP and UDP traffic through a proxy server.
14	SQL Server	1433	The main MS SQL Server service

15	SQL UDP Server	1434	The MS SQL Server UDP service
16	Telnet	23	A Telnet server is used to allow visitors to open a remote console on the server machine
17	Terminal Server	3389	Terminal Server is a Microsoft application that allows remote users to log on to a server
18	VNC	5900	VNC is a cross platform remote control application

Tabla. 3.4. Servicios montados en el servidor de KFSensor

3.3. HARDENING DE SERVIDORES

Todas las empresas poseen por lo menos un servidor, el cual es considerado como un activo crítico, ya que puede poseer información sensible, bases de datos, servidores de correo con comunicaciones internas o información de clientes (tarjetas de crédito, números de cuenta) que son de tipo confidencial y no deberían ser expuestos por ningún motivo, lamentablemente la mayoría de las aplicaciones no protegen esta información como se necesita por lo cual es necesario fortalecer las seguridades de los servidores, esto es lo que se denomina hardening de los sistemas, de manera que se garantice la protección de las aplicaciones, el software y la información.

El Hardening es una estrategia que sirve para defender los sistemas contra ataques, removiendo programas vulnerables y cerrando brechas de seguridad, restringiendo así el acceso indebido a los servidores.

Este proceso sigue algunos pasos para ser completado exitosamente, primeramente se encuentra la evaluación de los sistemas, a partir de esto se podrá encontrar las falencias y desarrollar procedimientos para asegurar los recursos más sensibles de la red. Cabe recalcar que estos procedimientos son personalizados, y serán realizados según las características de la red, del tipo de negocio de la empresa y deberá ser actualizado según la evolución de los ataques, además es

importante que este procedimiento sea automatizado para facilitar su implementación y posterior estudio.

En la web existen documentos que pueden ayudar a realizar el hardening de servidores y estaciones de trabajo basándose en los diferentes servicios que pueden estar activos en los sistemas, sin embargo la empresa CIS (Center for Internet Security) tiene las listas de verificación más reconocidas a nivel mudial para una gran variedad de servicios y sistemas operativos, las mismas que se pueden descargar gratuitamente desde el link oficial: http://benchmarks.cisecurity.org. (ver Figura. 3.116.)

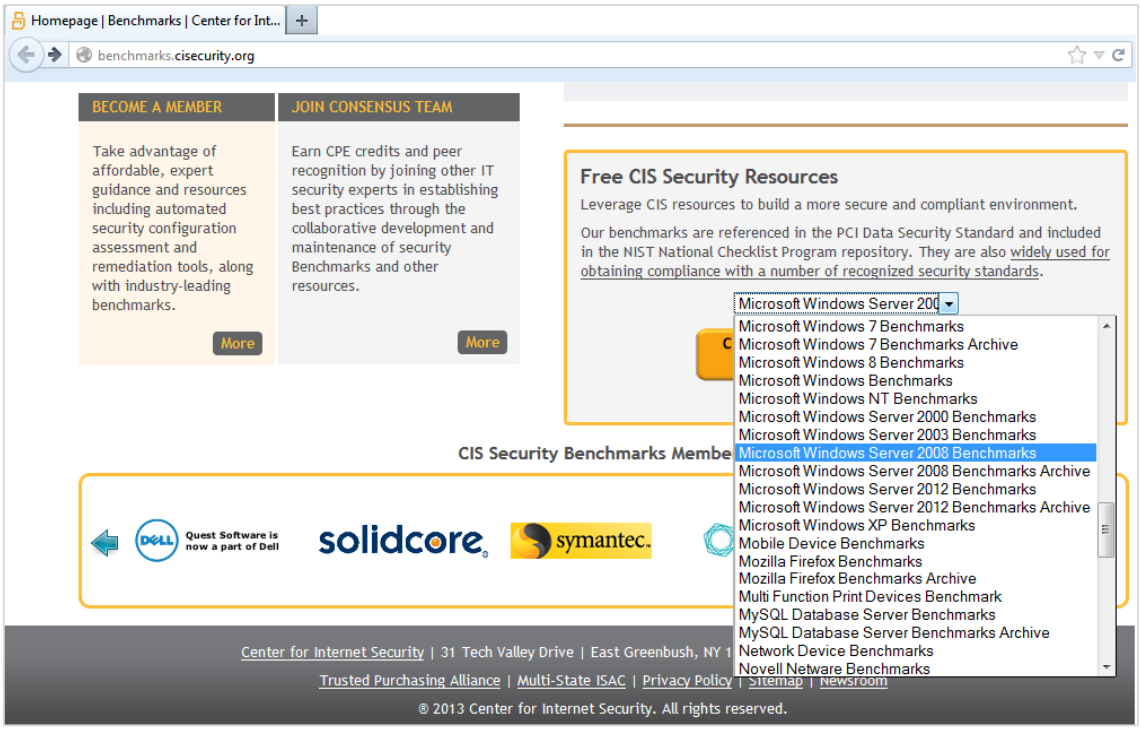


Figura. 3.116. Listas de verificación para hardening de servicios y sistemas operativos. ([39] Center for Internet Security, 2013)

3.4. ANÁLISIS DE VULNERABILIDADES

Cada vez los atacantes se enfocan en buscar vulnerabilidades en servicios, aplicaciones y sistemas operativos de manera que posteriormente se pueda crear un exploit para poder acceder a los diferentes sistemas y así obtener información. Estas vulnerabilidades están en constante crecimientos y aparecen diariamente

sobre todo en las aplicaciones (Facebook, twitter, whatsapp, dropbox, etc.) y sistemas operativos (Windows) más utilizados (ver Figura. 3.117.).

jueves, 4 de abril de 2013

15:55:00

Nueva vulnerabilidad en Facebook permite control de cuentas

Share 110 Twittear 85 +1 4

<Hacking> The Hacker News facebook </Hacked Again >

Nir Goldshlager ya había expuesto dos graves defectos en Facebook OAuth. La primera fue permitía hackear una cuenta de Facebook, sin que el usuario instale ninguna aplicación en su cuenta y la segunda mostraba diferentes maneras para eludir la protección de expresiones regulares en Facebook OAuth.

Ahora, Nir ilustra sobre un nuevo ataque que demuestra lo que sucede cuando se instala una aplicación en la cuenta de la víctima y cómo se la puede manipular. Según el hacker, si la víctima tiene una aplicación instalada como Skype o Dropbox, es capaz de tomar el control de sus cuentas.

Para esto, un atacante sólo necesita encontrar una vulnerabilidad de redirección URL o un Cross Site Scripting en el dominio del propietario de la aplicación de Facebook, como por ejemplo en Skype Facebook App. Además hay que tener en cuenta que los programas de recompensas *(Bounty Programs)* no consideran esto como una vulnerabilidad.

Figura. 3.117. Noticia de una nueva vulnerabilidad descubierta para Facebook ([40] Borghello, 2013)

Las organizaciones deben realizar un análisis de vulnerabilidades constantemente a servidores, dispositivos finales, elementos de seguridad y aplicaciones de manera que se puedan identificar y remediar las brechas de seguridad encontradas de manera que se pueda evitar el ingreso de software malicioso a la red.

A través del uso de herramientas, procesos o personal capacitado se puede ayudar a corregir las deficiencias, ya que no es adecuado únicamente basarse en los métodos de protección convencionales.

El análisis de vulnerabilidades se lo realiza siguiendo los siguientes pasos (ver Figura. 3.118.): ([41] Qualys Inc., 2013)

- Descubrimiento.- Identificación de los activos que forman parte de la red, localizando los activos, sistema operativo y todos los servicios que están activos en el sistema.
- Priorización.- Toda organización posee activos que son de mayor importancia que otros ya sea por la información que albergan o por cualesquiera que sean las funciones que este cumpla, por lo cual se debe priorizar cuáles serán los activos que necesitan ser analizados.
- Evaluación.- Es necesario determinar cuáles serán los niveles de riesgo en los cuales se va a enfocar la corrección de errores, esto se basa en la criticidad de los activos y la importancia de los mismos, y se determinará por el administrador de la red. Se debe realizar una evaluación de las vulnerabilidades de forma periódica y programada.
- Informe.- Se basa en medir los riesgos hallados durante el análisis y entregar un reporte con las vulnerabilidades encontradas, esto va a asociado con las políticas de seguridad de la empresa respecto a los activos.
- Remediación.- Reparar las vulnerabilidades encontradas, de acuerdo al riesgo que estas implican en la organización, la remediación se la realiza según como se priorice los activos.
- Verificación.- Se realiza una nueva auditoría para determinar que las vulnerabilidades han sido eliminadas.

Figura. 3.118. Ciclo de análisis de vulnerabilidades

3.5. HERRAMIENTAS PARA ANÁLISIS DE VULNERABILIDADES

Para realizar el análisis de vulnerabilidades se debe tomar en cuenta como primer punto si se va a utilizar una arquitectura de código abierto o un software propietario.

Uno de los software más utilizados para el análisis de vulnerabilidades es el programa Nessus, el cual trabaja sobre la plataforma Linux/Unix, tiene su versión de código abierto, y posee una base de datos de patrones de ataque, que son las que son enviadas a la máquina objetivo con el fin de detectar si esta tiene vulnerabilidades que podrían ser atacadas.

Además se tienen programas comerciales que utilizan a Nessus como su motor de análisis, entre estos se encuentra Catbird para Linux y MBSA para Windows, estos programas se diferencian de Nessus ya que añaden características adicionales como son la generación de reportes, gestión centralizada de las vulnerabilidades, monitoreo de red interna y externa incluyendo los accesos inalámbricos, etc. Por lo cual es decisión de las empresas escoger cual será el

método que utilizarán para realizar el análisis de vulnerabilidades dependiendo del nivel de profundidad que necesiten.

3.6. ESCÁNER DE VULNERABILIDADES QUALYS

3.6.1. Introducción

Existen muchos motivos para la existencia de vulnerabilidades, pero lo más importante es conocer que las vulnerabilidades no se podrán eliminar de manera automática, por el contrario se requiere de una gestión que ayudará detectarlas, eliminarlas y controlarlas, esta herramienta es Qualys, la cual realiza todas estas tareas de maneras especializada y realizando un flujo de trabajo que ayudará a eliminar los riesgos que podrán ser explotados.

Qualys es un escáner de vulnerabilidades, el cual juega un papel vital en la seguridad de la red y en el cumplimiento de reglas dentro de una organización. En la industria de la seguridad los analistas están de acuerdo con que la seguridad en la red debe cumplir con varios requerimientos a través del uso de diferentes herramientas. Un analizador de vulnerabilidades puede detectar todos los problemas que el antivirus y firewall dejan escapar, por lo tanto no está para reemplazar a ninguna herramienta sino para complementarla.

El analizador de vulnerabilidades Qualys trabaja de manera proactiva, ya que al realizar un escaneo de los equipos de la red, de manera casi continua, estarán constantemente actualizados sobre las nuevas vulnerabilidades que son introducidas por los proveedores de software, así como de las buenas prácticas que se deberán manejar internamente por el personal, lo ideal sería poder realizar un sistema de seguridad automatizada para garantizar el cumplimiento de políticas y normativas dentro de la organización.

Qualys realiza una gestión completa de las vulnerabilidades, empezando con el descubrimiento de la red para conocer todos los activos que están conectados a la misma, realiza un escaneo, reporta los datos encontrados, informa acerca de la

remediación y finalmente se recomienda realizar un escaneo para verificar que las vulnerabilidades fueron mitigadas. Este proceso debe ser continuo, ya que cualquier cambio de políticas o de configuraciones de la red implica inevitablemente la realización de un nuevo escaneo, además aunque no se realicen cambios en la red diariamente se descubren nuevas vulnerabilidades que puede poner en riesgo la seguridad en la organización.

Por medio de QualysGuard las pequeñas y grandes organizaciones, hacen efectivo el manejo de sus vulnerabilidades por ser un proceso automatizado, manteniendo el control de su red al generar reportes centralizados, verificando la remediación de las vulnerabilidades encontradas, además indicará los diferentes niveles de riesgo que tendrá cada vulnerabilidad para que de esta manera el administrador de la red identifique cuáles serán los casos en los cuales se centrará y cuáles serán aquellos que deberán descartarse según el impacto que tengan los mismos dentro de la red.

3.6.2. Modos de operación

Qualys puede funcionar de tres modos principales: ([41] Qualys Inc., 2013)

- Escaneo externo
- Escaneo interno por medio de un equipo
- Escaneo interno por medio de una máquina virtual

El escaneo externo se lo realiza con equipos ubicado en Estados Unidos que permiten realizar un análisis de las direcciones IP públicas de la empresa desde el internet, como lo haría un atacante en la primera fase.

Para escaneos internos, Qualys ofrece hacerlo desde un equipo instalado en la red interna o desde una máquina virtual dentro de uno de los computadores o servidores de la misma red. Estos escaneos servirán para visualizar las vulnerabilidades evitando los bloqueos que pueden hacer distintos dispositivos de seguridad o probar el nivel de protección de los elementos de seguridad ubicados en la red interna.

En este caso se utilizará un equipo virtual instalado dentro de la red interna (ver Figura. 3.119.).

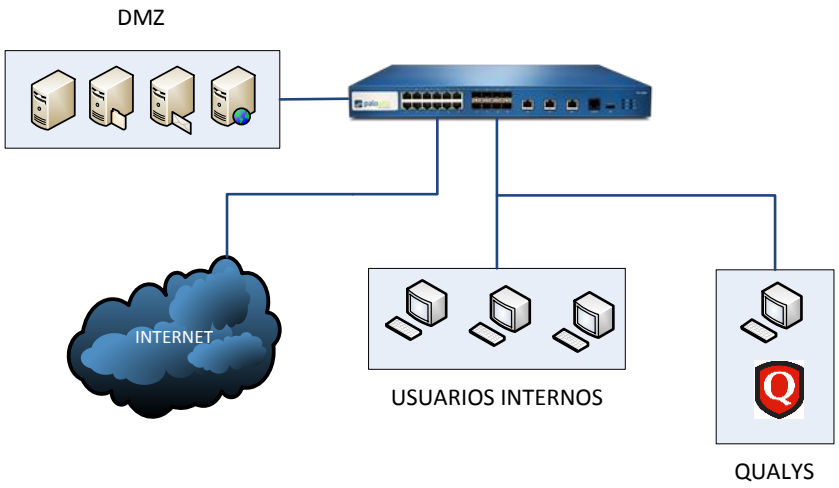


Figura. 3.119. Diagrama físico Qualys

3.6.3. Funcionamiento interno

Para realizar la gestión de vulnerabilidades se utiliza el módulo VM (Vulnerability Management), con esta aplicación se automatiza el ciclo de vida de la auditoría de la red, para realizar dicha auditoría se deben cumplir cuatro pasos que permitirán realizar un análisis exhaustivo de toda la organización: ([41] Qualys Inc., 2013)

- Mapeo de la red
- Escaneo de vulnerabilidades
- Reporte de Vulnerabilidades
- Remediación

Para iniciar es necesario crear un “Network Map Profile” que indica la parte de la red a la cual se va a realizar el descubrimiento, que indica cuales son todos los activos que están conectados a la red. Para realizar el primer escaneo se accede a Maps en la sección Scans y posteriormente se realiza un New Map (ver Figura. 3.120.).

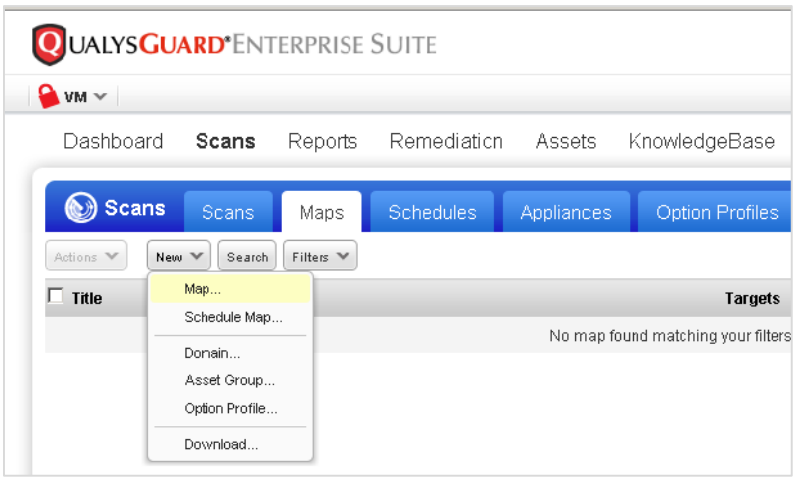


Figura. 3.120. Crear un nuevo mapeo en Qualys

Al dar clic en esta opción aparecerá un pop-up que nos permitirá darle un nombre, seleccionar un perfil, un scanner y escoger el dominio, posterior a la configuración es posible lanzar el mapeo de la red (ver Figura. 3.121.).

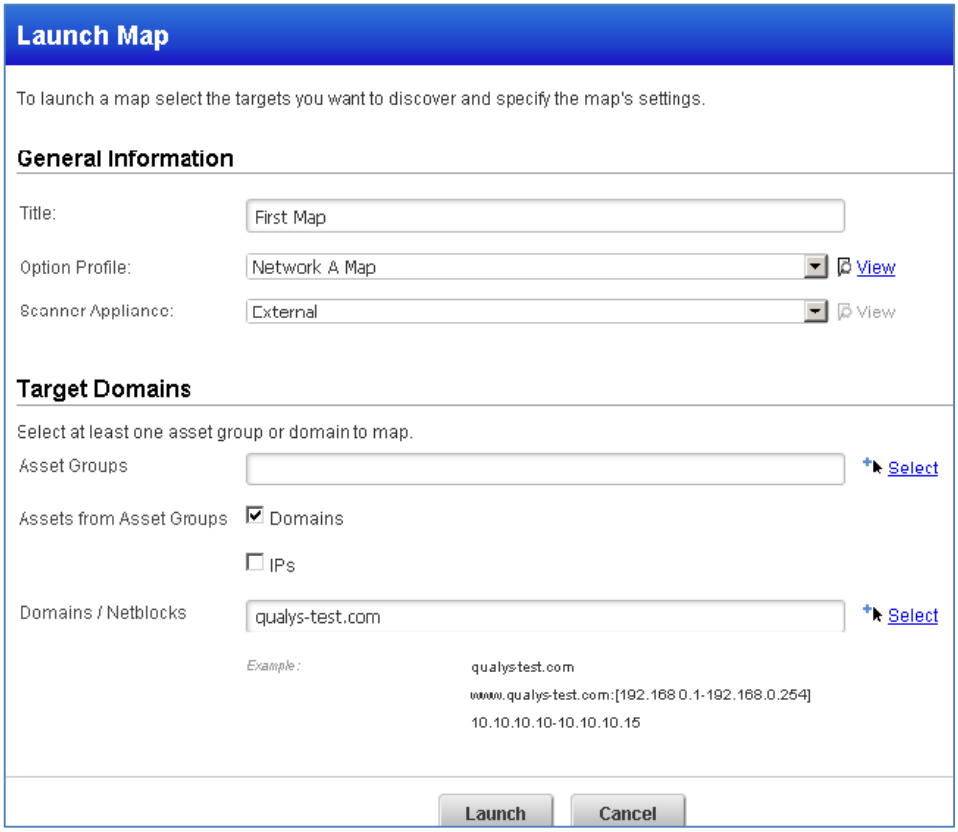


Figura. 3.121. Mapeo de la red con Qualys

Una vez finalizado el mapeo (ver Figura. 3.122.) se enviará un reporte detallado al mail que fue configurado para recibir las notificaciones.

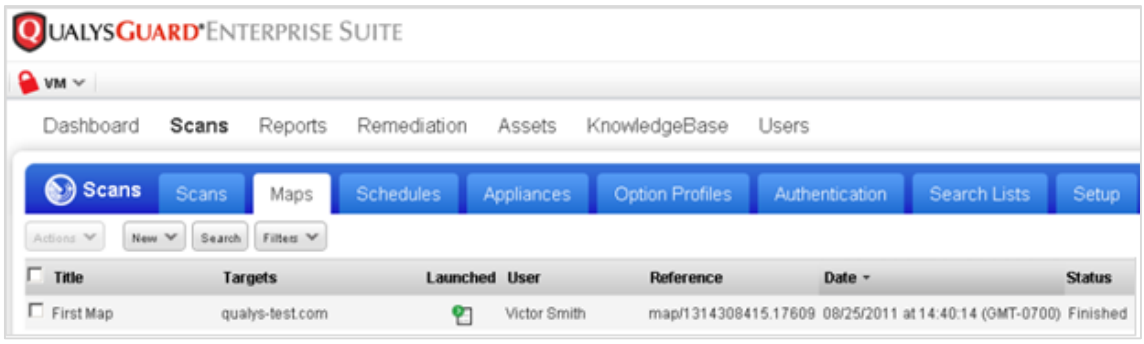


Figura. 3.122. Mapeo finalizado en Qualys

El resultado de mapeo será obtenido en un archivo HTML, para que pueda ser exportado o para generar un reporte, también existe la opción de observar en modo gráfico el descubrimiento total de la red (ver Figura. 3.123.)

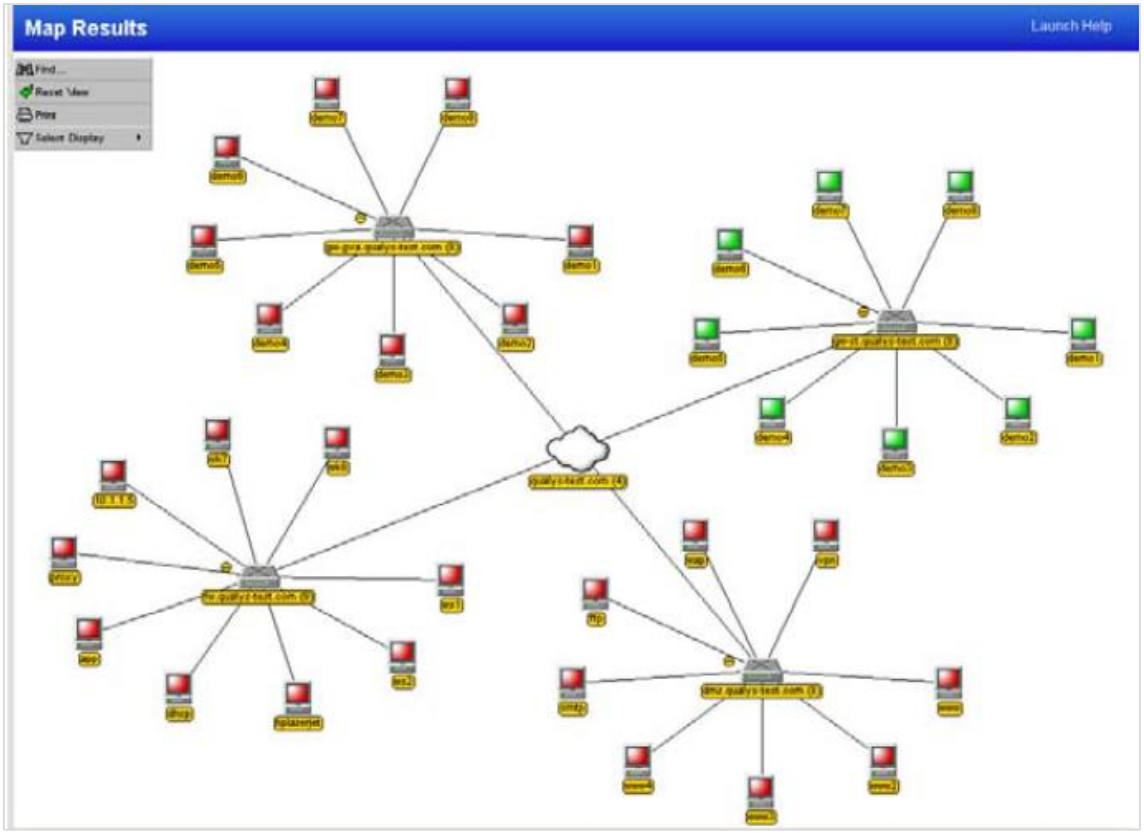


Figura. 3.123. Resultado del mapeo en Qualys

Al dar clic sobre cualquiera de los host es posible observar una pequeña descripción del mismo (ver Figura. 3.124.).

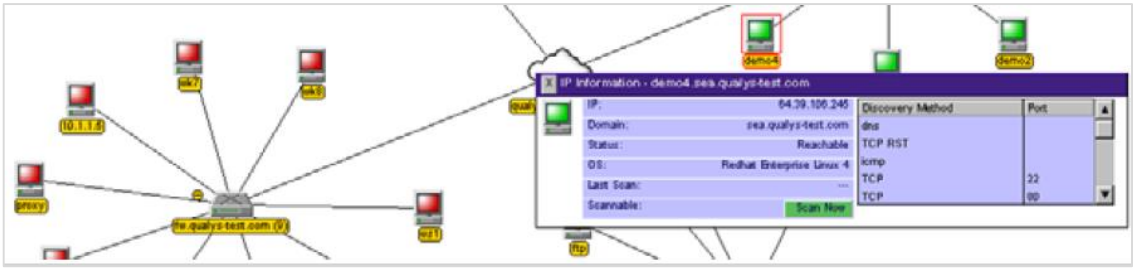


Figura 3.124. Detalle de host en el mapeo de una red con Qualys

Así como en el mapeo, en el escaneo también se deben crear perfiles. Para crear un nuevo perfil se debe ir a Scans > Option Profiles y posteriormente New > Option Profile (ver Figura. 3.125.). Se pueden crear perfiles personalizados, indicando el sistema operativo, los puertos que se desea analizar, la profundidad con la cual se realizará el escaneo, host que se deseen excluir, si se realizará autenticación, etc. Se debe tomar en cuenta que se pueden crear perfiles desde cero, modificar perfiles existentes o utilizar formatos predeterminados según cual sea la necesidad del administrador de la red.

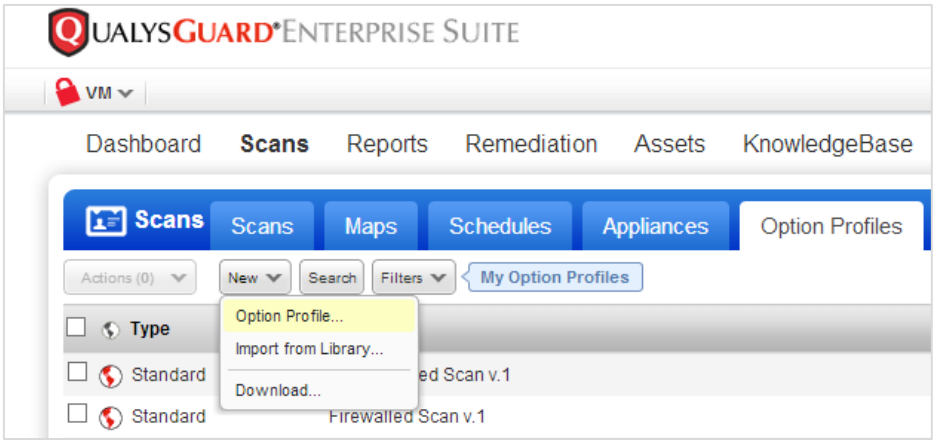


Figura. 3.125. Creación de un perfil para un escaneo en Qualys

Una de las opciones más interesantes es el escaneo con credenciales, en esta opción se entrega el usuario y la contraseña a Qualys de manera que el análisis sea mucho más intenso, y sobre todo para que con la autorización del administrador se pueda ingresar al sistema completamente. Además se deberá indicar el tipo de sistema operativo que va a ser escaneado (ver Figura. 3.126.) para que Qualys busque dentro de las credenciales que fueron entregadas para este sistema operativo.

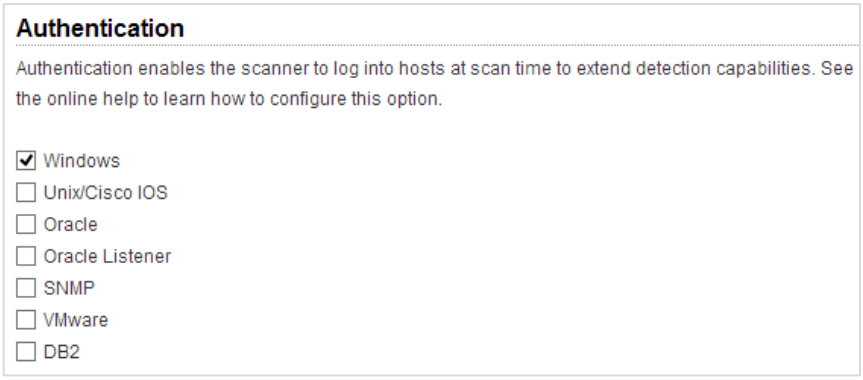


Figura. 3.126. Configurar escaneo con autenticación en Qualys

Para realizar el primer escaneo se accede a Scans > New Scan. Al darc clic en launch se ejecutará el escáner al host definido anteriormente utilizando el perfil antes creado (ver Figura. 3.127.).

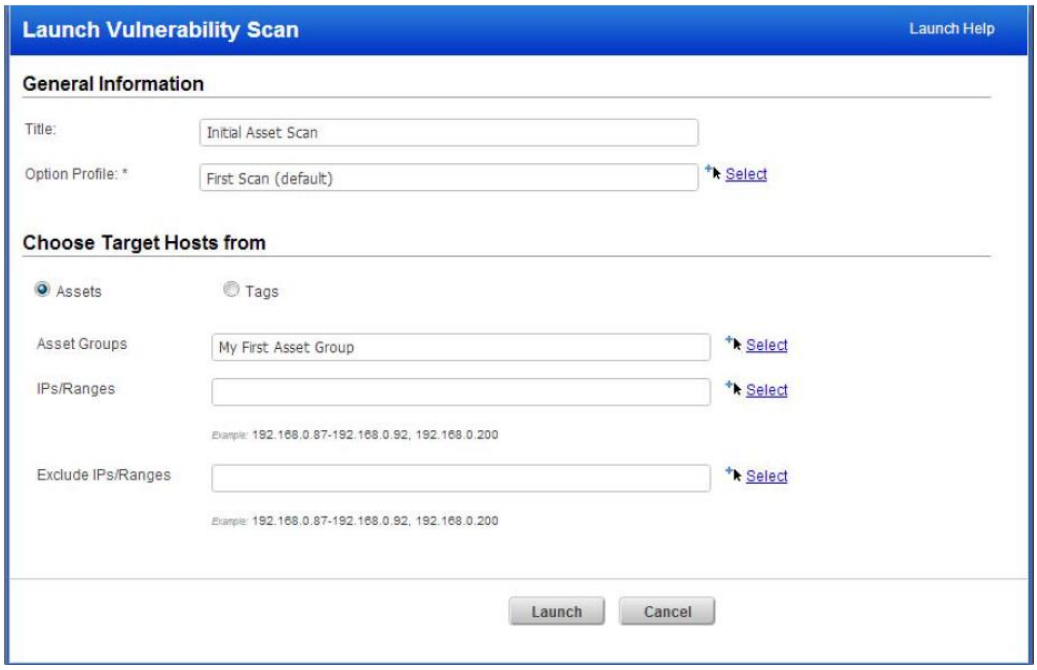


Figura. 3.127. Realizar escaneo de vulnerabilidades con Qualys

Mientras se corre un escaneo, este puede ser detenido, pausado o reanudado (ver Figura. 3.128.) y dependiendo del host, el escaneo dura aproximadamente una hora

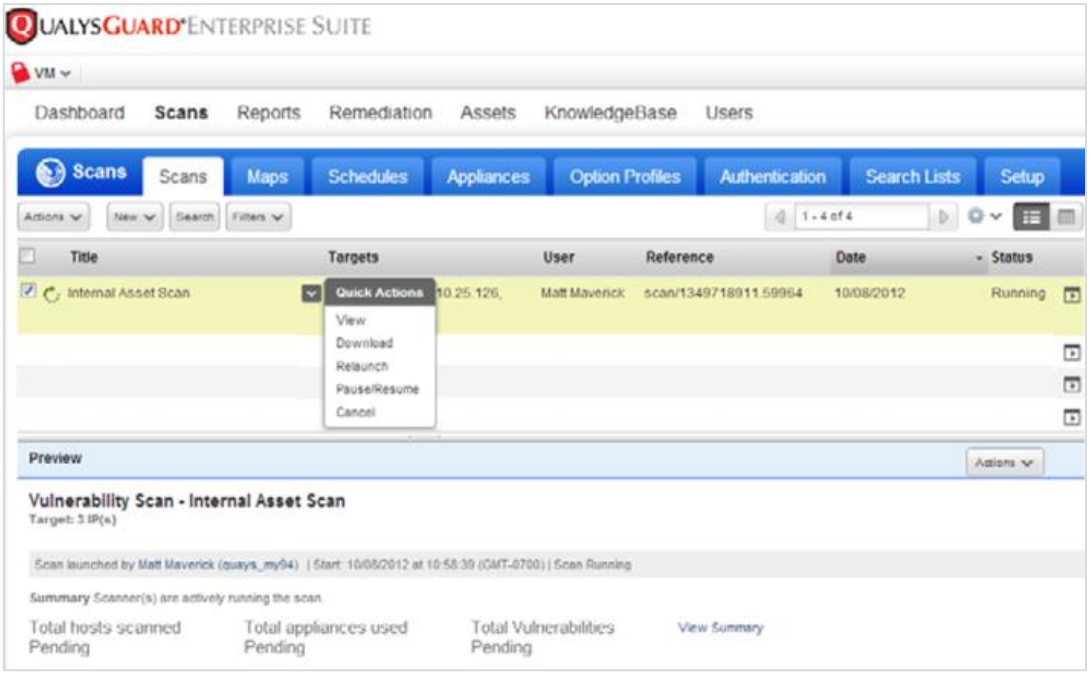


Figura. 3.128. Escaneo en proceso en Qualys

Cuando haya finalizado el escaneo se mostrará un botón en verde y que ya se puede acceder a los resultados con tan solo dar un clic (ver Figura. 3.129.).

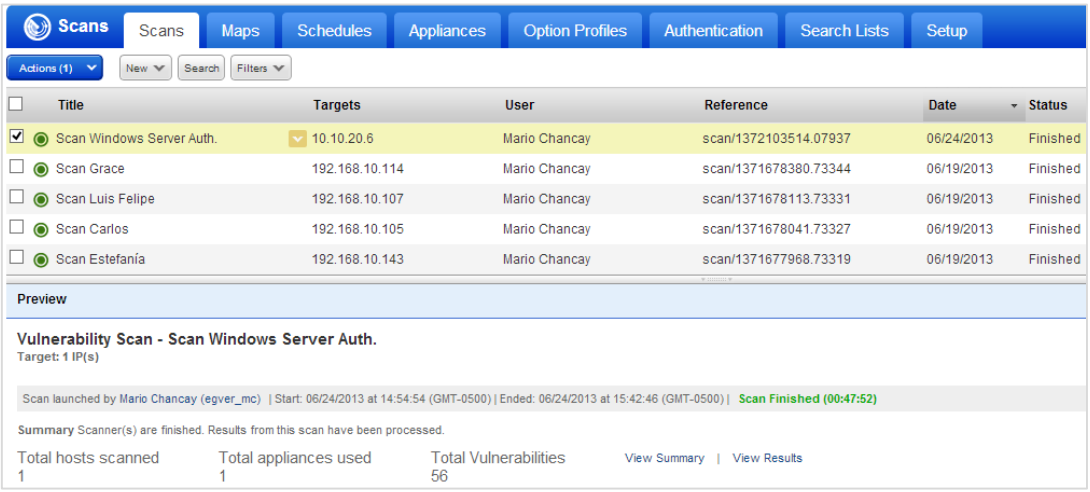
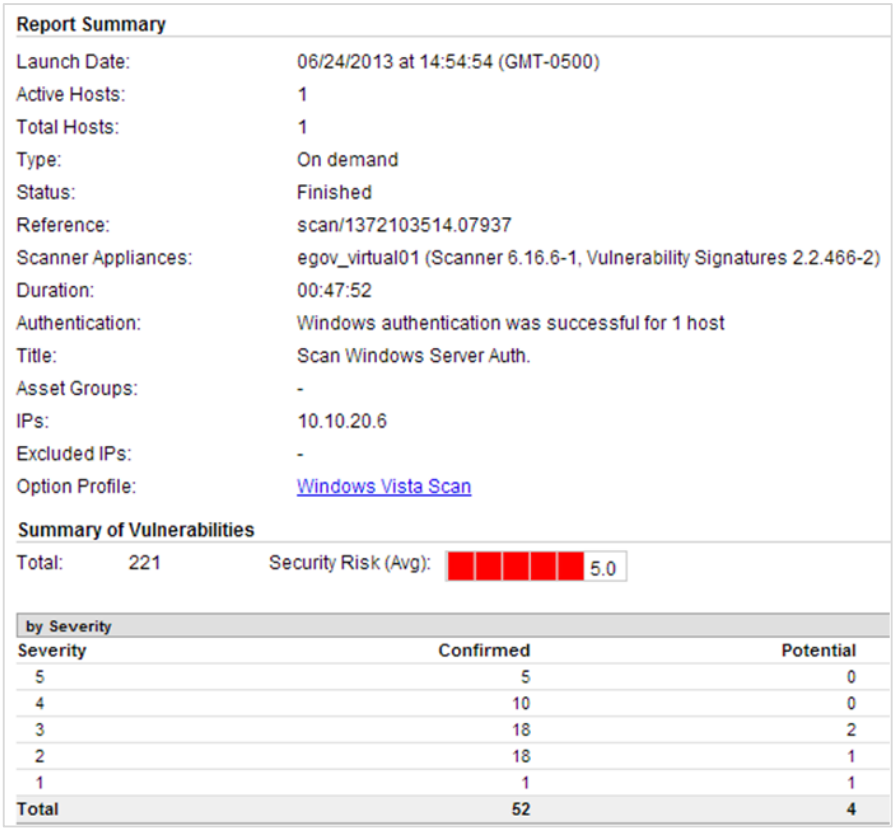


Figura. 3.129. Escaneo finalizado con Qualys

Al dar clic en “view results” se desplegará el resultado obtenido, donde se mostrará el host, si se realizó el escaneo con autenticación, con qué perfil se realizó el escaneo, además la cantidad de vulnerabilidades encontradas y el promedio de riesgo según la cantidad de vulnerabilidades y el nivel de criticidad de las mismas (ver Figura. 2.130.).



Report Summary

Launch Date:	06/24/2013 at 14:54:54 (GMT-0500)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1372103514.07937
Scanner Appliances:	egov_virtual01 (Scanner 6.16.6-1, Vulnerability Signatures 2.2.466-2)
Duration:	00:47:52
Authentication:	Windows authentication was successful for 1 host
Title:	Scan Windows Server Auth.
Asset Groups:	-
IPs:	10.10.20.6
Excluded IPs:	-
Option Profile:	Windows Vista Scan

Summary of Vulnerabilities

Total: 221 Security Risk (Avg): 5.0

by Severity

Severity	Confirmed	Potential
5	5	0
4	10	0
3	18	2
2	18	1
1	1	1
Total	52	4

Figura. 3.130. Ejemplo resumen de reporte con Qualys

En el reporte también se puede mostrar una descripción más detallada de las vulnerabilidades, entre estos está un breve resumen de la vulnerabilidad, cual es el impacto que tiene la misma sobre el sistema, si existe algún exploit para atacar, y la solución para eliminar o mitigar su existencia (ver Figura. 3.131.).

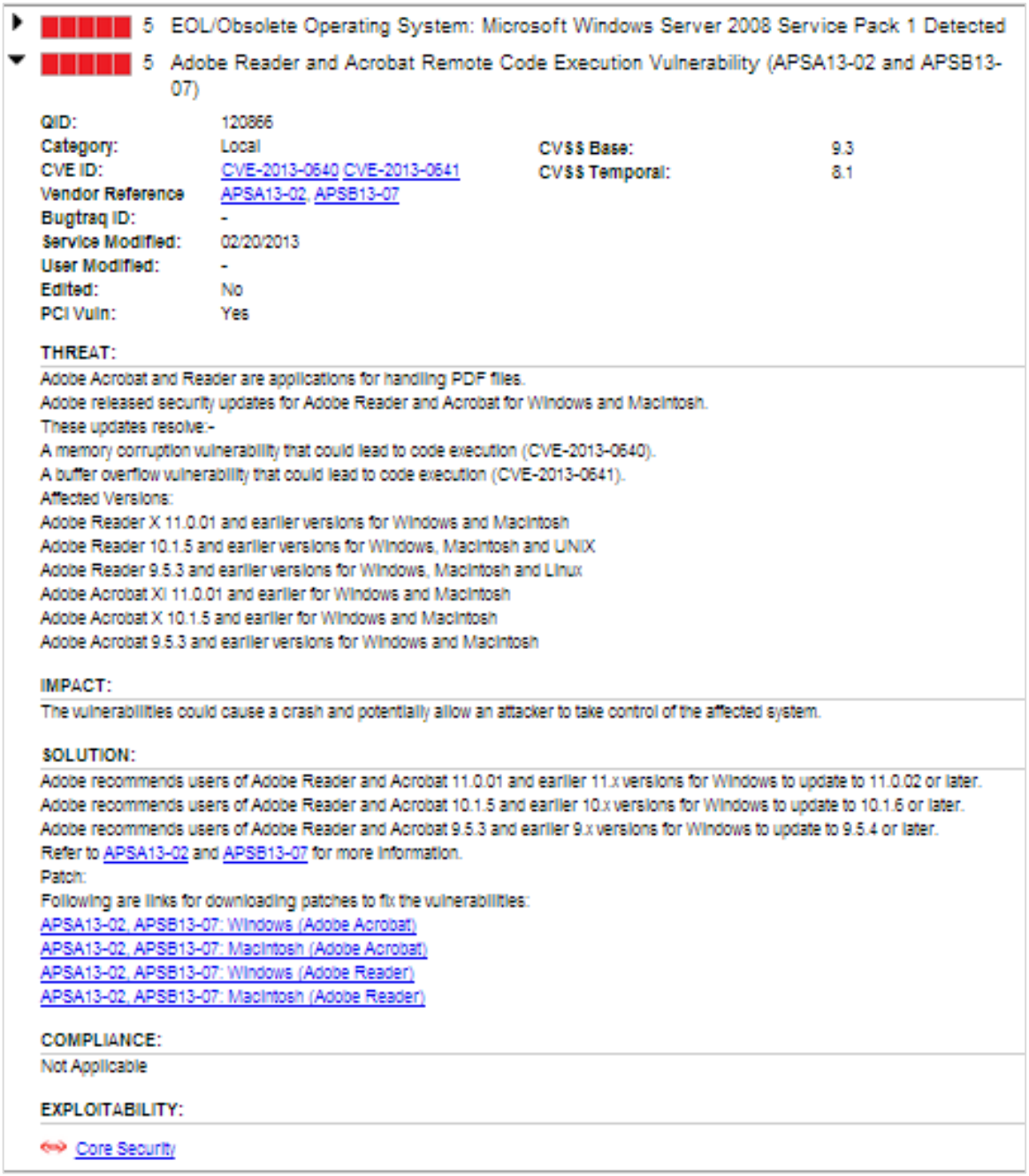


Figura. 3.131. Vulnerabilidad explotable encontrada con Qualys

En el Dashboard se observa de manera gráfica y resumida los resultados obtenidos, así como la totalidad de todos los escáneres realizados, y el top 10 de vulnerabilidades halladas (ver Figura. 3.132.).

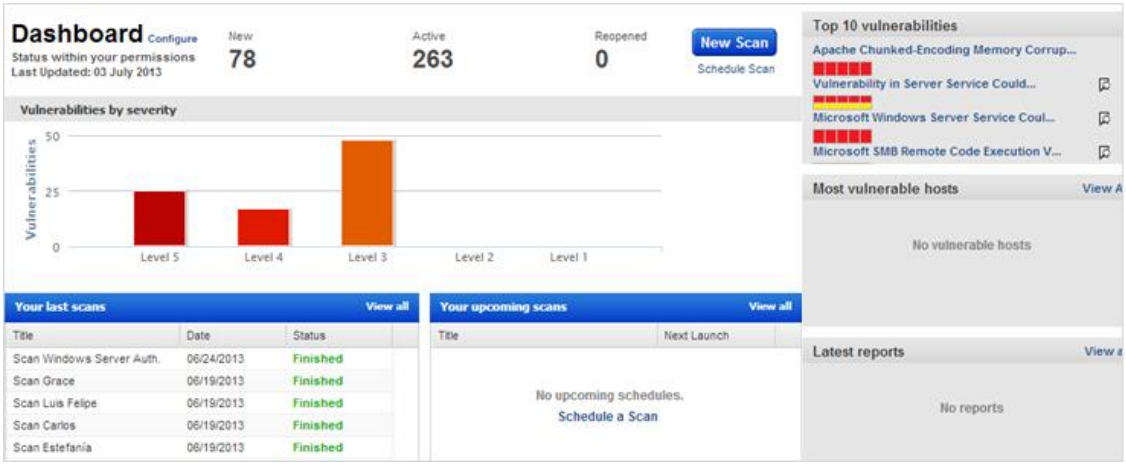


Figura. 3.132. Dashboard de Qualys

Una de las principales características que distingue a Qualys de otros analizadores de vulnerabilidades es la capacidad que tiene el mismo en la creación de reportes, su flexibilidad para personalizar los reportes es un gran diferenciador ante sus competidores.

La mayoría de analizadores de vulnerabilidades no permite crear reportes, y en caso de que puedan hacerse, estos vienen predefinidos por el fabricante de manera que el usuario solo podrá acoplarse a los modelos existentes.

Los reportes de Qualys tienen los siguientes componentes:

- Activos de la red, que pueden ser IPs o grupos de activos que participaron en el análisis.
- Gráficos donde se muestran los resultados de la red y el estado de seguridad del sistema.
- Resumen del análisis realizado a la red.
- Información acerca de las vulnerabilidades descubiertas.
- Filtrado que permite personalizar la forma en que serán mostrados los resultados.

Existe una opción en Qualys que permite que los resultados de los análisis puedan ser compartidos, el administrador de la red podrá escoger el grupo de usuarios que podrán tener acceso a los resultados de una análisis, tener conocimiento de la iniciación de un escaneo o realizar la descarga completa de los

resultados para su posterior estudio. Estos reportes podrán ser descargados en formato PDF o HTML y serán enviados vía mail a los usuarios habilitados.

Los reportes pueden ser creados según la necesidad del administrador (ver Figura. 3.133.).

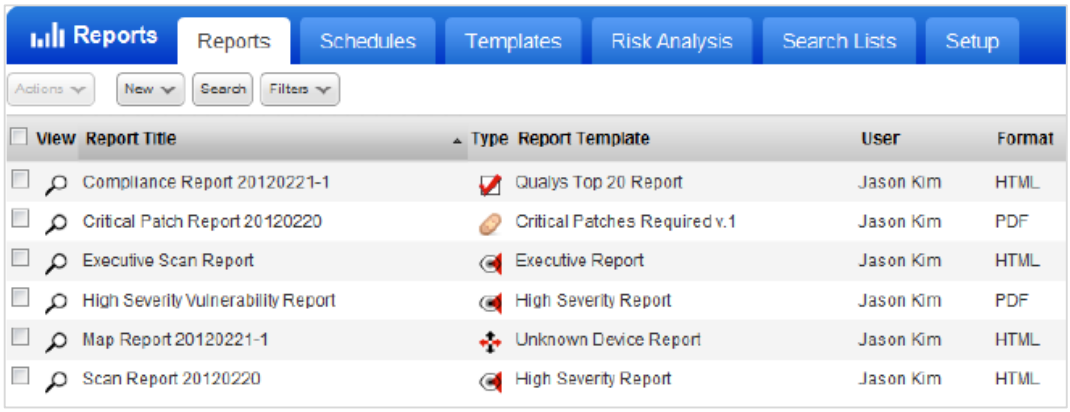


Figura. 3.133. Reportes creados en Qualys

Cuando se ejecuta un reporte este realiza en segundo plano, por lo cual se puede ejecutar cualquier otra acción a la par sin necesidad de detener la ejecución del mismo. Al finalizar el reporte un mail será enviado con un resumen de los resultados para que el usuario decida qué hacer con el mismo.

Para realizar un reporte, se accede al área de Reports > New, en donde se escogerá el tipo de reporte que se desea ejecutar (ver Figura. 3.134.).

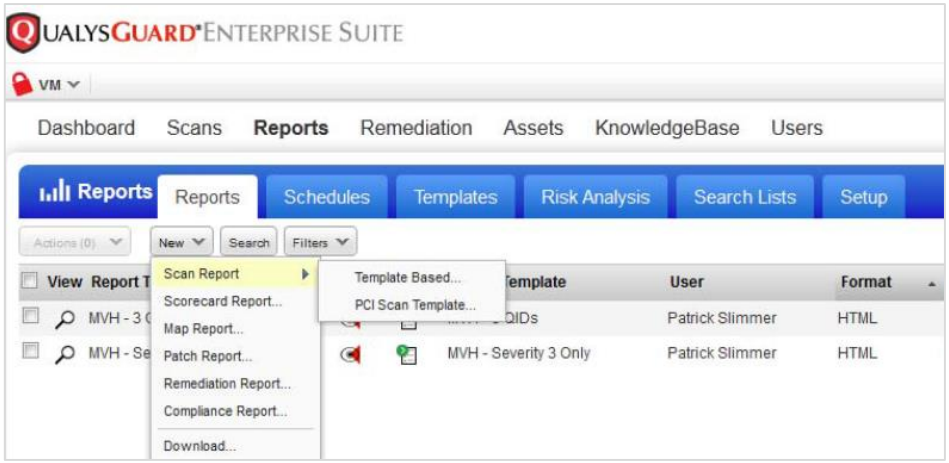


Figura. 3.134. Creación de un nuevo reporte en Qualys

Al escoger la opción Template Based se desplegarán una serie de opciones como se muestra en la siguiente figura, en donde el usuario escogerá la más apropiada según sus necesidades, Qualys ofrece una gran variedad de opciones que serán muy útiles al momento de empezar a manejar la herramienta (ver Figura. 3.135.).

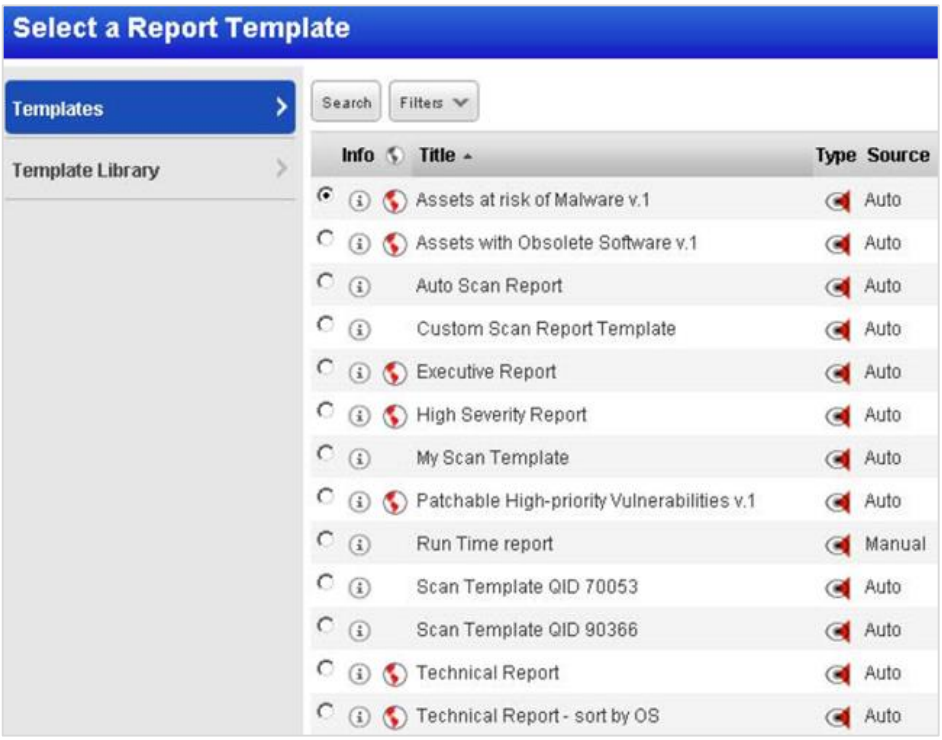


Figura. 3.135. Plantillas para la creación de un reporte en Qualys

Una vez que se ha realizado un escaneo total de la red, la actividad final consiste en remediar o eliminar las vulnerabilidades encontradas.

3.6.4. Configuración

Se procede a la creación de un nuevo escáner virtual que es con el cual se va a trabajar, para lo cual se accede a Scans > Appliances > New > Virtual Scanner Appliance (ver Figura. 3.136.)

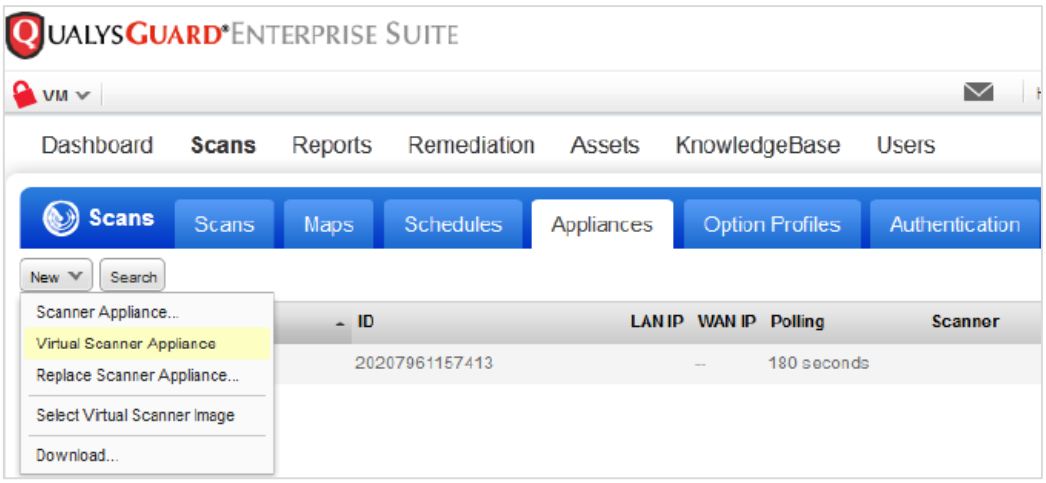


Figura. 3.136. Configuración de un nuevo escáner de Qualys

Ingresar un nombre para el escáner virtual, al realizarlo Qualys entregará un código de activación y un link desde el cual será posible descargar una máquina virtual para ejecutarla en un ambiente virtualizado, en este caso se escogerá la que corresponde a VMWare. Inicialmente la máquina se encuentra desactivada, mostrando la versión del escáner que está funcionando y la versión del motor de firmas (ver Figura. 3.137.).

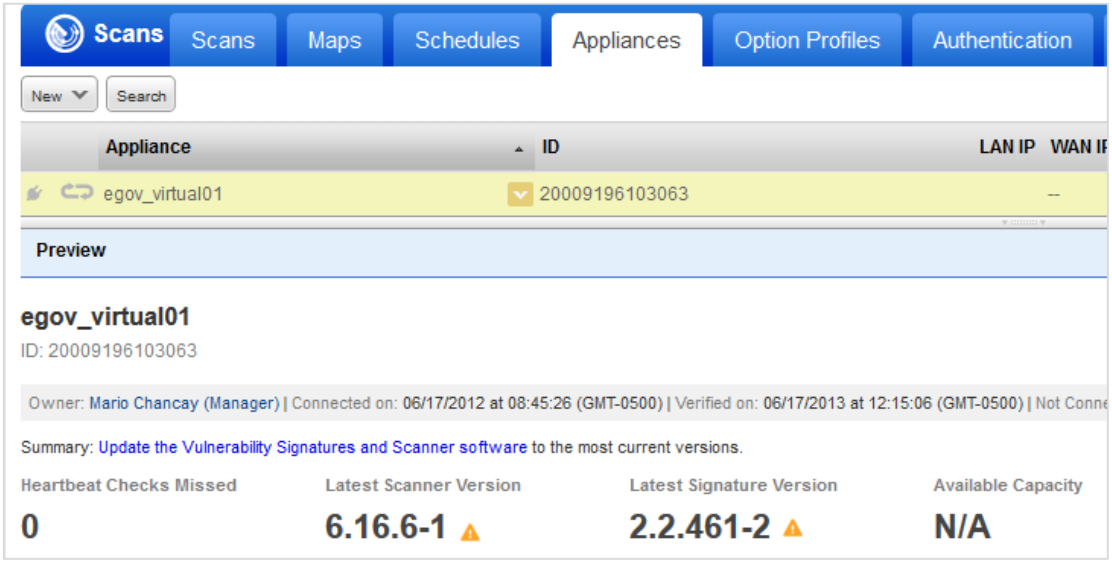


Figura. 3.137. Creación de escáner virtual en Qualys

Una vez descargada la máquina virtual, se procederá a abrirla en VMWare, y se ingresará toda la configuración necesaria, empezando por el código de activación con el cual se descargarán todos los paquetes necesarios para su correcto funcionamiento (ver Figura. 3.138.).

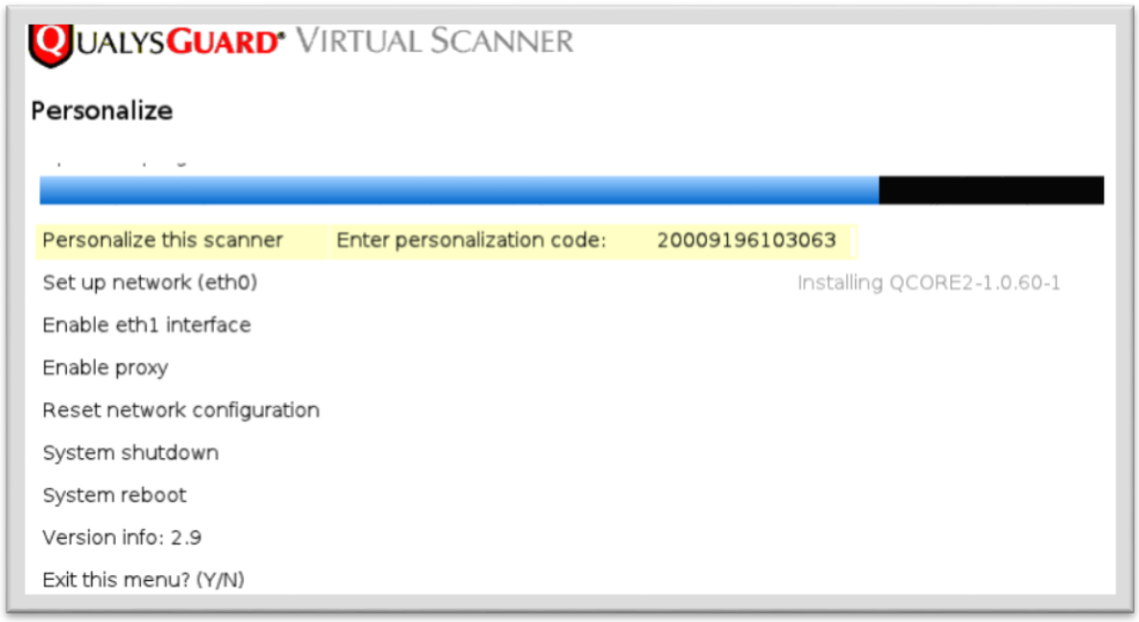


Figura. 3.138. Configuración de escáner virtual de Qualys

Una vez finalizada la configuración adicional se procederá a realizar la configuración de la red según los requerimientos (ver Figura. 3.139.).

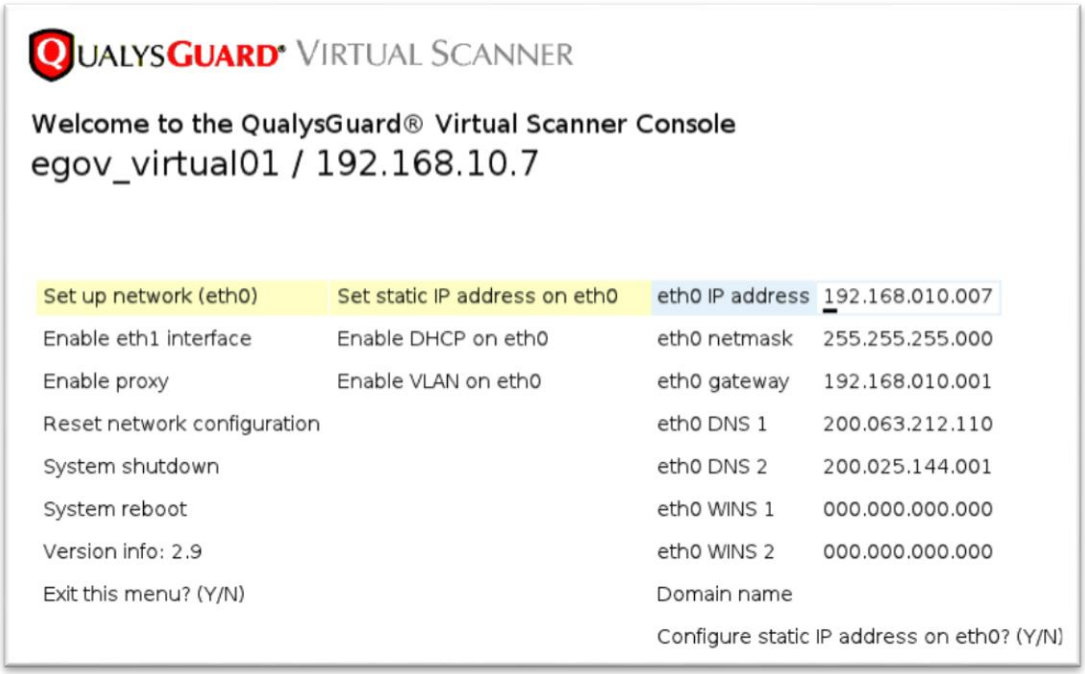


Figura. 3.139. Configuraciones de red de escáner virtual de Qualys

Posteriormente es necesario ingresar a la página de QualysGuard que es la plataforma en la nube, para verificar que la máquina ya se encuentra activa y lista

para ser utilizada. El ícono en botón verde indicará que el escáner virtual está listo para empezar a funcionar (ver Figura. 3.140.).

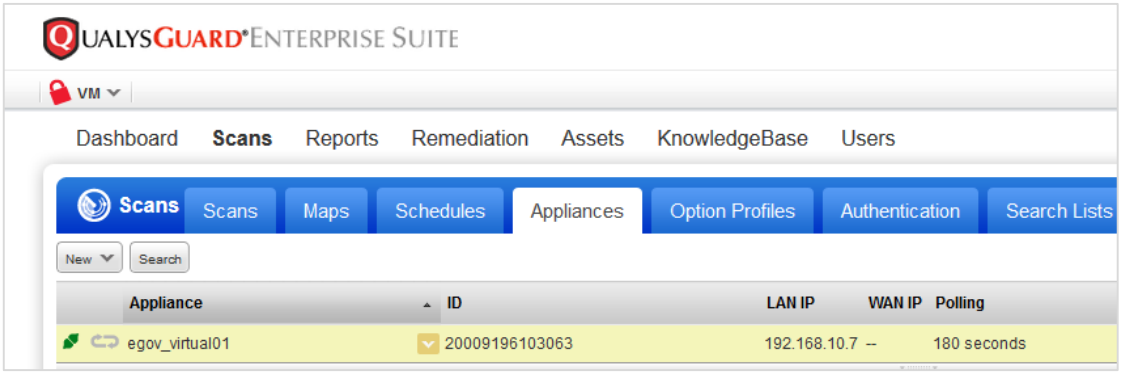


Figura. 3.140. Escáner virtual de Qualys activado

3.6.5. Ventajas y desventajas

Ventajas

- Interfaz de usuario amigable
- Reportes flexibles y totalmente personalizables en diferentes formatos.
- Realiza un análisis más profundo que herramientas open source.
- Se pueden usar filtros según las necesidades del usuario.
- Entrega un resumen detallado de las vulnerabilidades.

Desventajas

- Herramienta Costosa.
- Basada en web.

3.7. VULNERABILIDADES DENTRO DE SERVIDORES WEB

Los primeros ataques que se realizaron a la red, estuvieron relacionados con fallas en los protocolos TCP/IP, cuando estas vulnerabilidades fueron descubiertas y remediadas, los ataques se re direccionaron hacia las capas de aplicaciones y específicamente a la web.

En los últimos tiempos los ataques a los servidores web se han convertido en un gran atractivo para los hackers, ya que hoy en día la gran mayoría de empresas tiene por lo menos una página web, a partir de esta se buscan errores de configuración en los sistemas, los cuales son más comunes de lo que se espera, con lo que se deja al servidor web disponible y vulnerable ante cualquier ataque.

Cuando se realiza un ataque a un sitio web, este se caracteriza por ser bastante vistoso, en cuestión de minutos se logra poner al descubierto todas las vulnerabilidades que se encontraron, y como las páginas web son públicas y se encuentran colgadas en la red a nivel mundial, no tarda mucho en que todos los hackers conozcan de los problemas de dicho sitio, aprovechando esta oportunidad para colocar dentro del sitio publicidad sobre ellos mismos, logrando así que la reputación de la empresa decaiga mientras que el hacker ganará popularidad dentro de la comunidad de hackers.

La principal causa de los ataques a los servidores web se da por una configuración inapropiada o por errores de diseño. Cuando las organizaciones son grandes así mismo lo son sus servidores, los cuales son más complejos pues dan servicios como alta disponibilidad, balanceo de carga, etc. ocasionando que sean servidores más difíciles de administrar. Por el contrario si la empresa es pequeña normalmente utiliza servidores web sencillos, mismos que no requieren mucha administración, además su instalación es más simple dejando al administrador la posibilidad de realizar una configuración por default, ocasionando que la seguridad sea mínima, dejando abiertas brechas que permitirán a los hackers ingresar de manera remota al servidor y modificar contenidos de manera no autorizada.

Los protocolos que son utilizados para la transferencia de páginas web son HTTP y HTTPS, a través de los cuales es posible realizar la comunicación hacia y desde Internet, uno de los usos más frecuentes es la transmisión de páginas web que permite al usuario interactuar con los servicios ofrecidos en línea.

Como los ataque iniciales se realizaron a servidores web, las organizaciones se esforzaron en encontrar métodos para protegerlos y a partir de esto los ataque se enfocaron en las aplicaciones web las mismas que se definen como las

interfaces a las cuales se puede acceder desde el navegador, es por esto que las seguridades en todos los servicios de Internet deben darse tanto en la etapa de diseño como en la de desarrollo.

Al realizar un escaneo con cualquiera de las herramientas que se encuentran disponibles para este fin, se van a mostrar gran cantidad de las vulnerabilidades del sistema, lo cual permitirá reforzar las seguridades del sistema, además existen medidas adicionales que se deberán considerar al implementar un servidor web, entre los cuales está eliminar ficheros, privilegios de usuario, entre otros.

Las vulnerabilidades de aplicaciones (ver Figura. 3.141.) web pueden ser las siguientes:

- Vulnerabilidades del servidor web, en la actualidad es muy complicado encontrar este tipo de vulnerabilidad ya que las organizaciones han reforzado las protecciones de los servidores.
- Manipulación de URL, se realizan modificaciones de parámetros de la URL con el objetivo de modificar el comportamiento usual del sitio web.
- Aprovechar las vulnerabilidades de los sistemas de identificación de usuarios y errores de autenticación.
- Inyección de código HTML y secuencia de comandos entre sitios
- Inyección SQL en campos no validados.

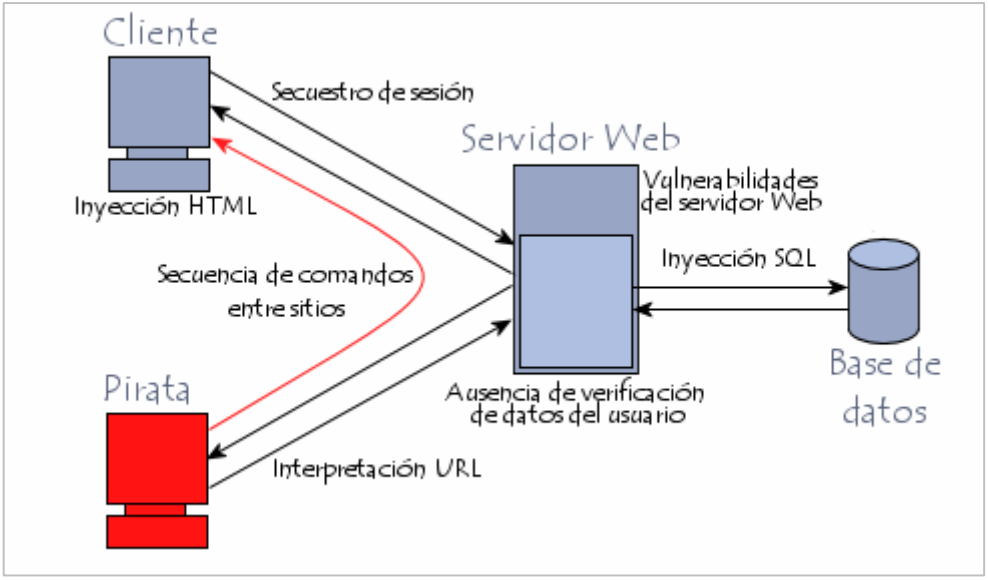


Figura. 3.141. Tipos de vulnerabilidades en aplicaciones web ([42] Kioskea, 2013)

La mayoría de los ataques realizados a servidores web se deben a la negligencia de los desarrolladores, quienes no validan correctamente cada uno de los campos de ingreso de datos de los usuarios.

Un ataque a una aplicación web es totalmente dañino, ya que afecta a la imagen y prestigio de la empresa, se modifica de manera negativa la presentación del sitio web, se puede ingresar o modificar datos de los usuarios, y puede existir intrusión en el servidor web.

3.8. ESCÁNER DE VULNERABILIDADES WEB (QUALYS GUARD WAS)

3.8.1. Introducción

Esta herramienta permite a las organizaciones evaluar y seguir las vulnerabilidades de las aplicaciones web. ([43] Qualys Inc., 2013)
Por medio del WAS (Web Application Scanner) se puede realizar:

- Escaneo de aplicaciones web en busca de vulnerabilidades.
- Identificar como se manejan los datos confidenciales.
- Crear listas blancas para evitar falsos positivos.

- Entregar reportes con prácticas a seguir, lista detallada de vulnerabilidades, etc.

Qualys WAS se caracteriza por realizar una detección completa de las vulnerabilidades de aplicaciones web, basándose en una de las más prestigiosas aplicaciones que es OWASP la cual realiza el top 10 de las vulnerabilidades web más comunes.

3.8.2. Configuración

Seleccionar el módulo de Web Application Scanning v1 (ver Figura. 3.142.)

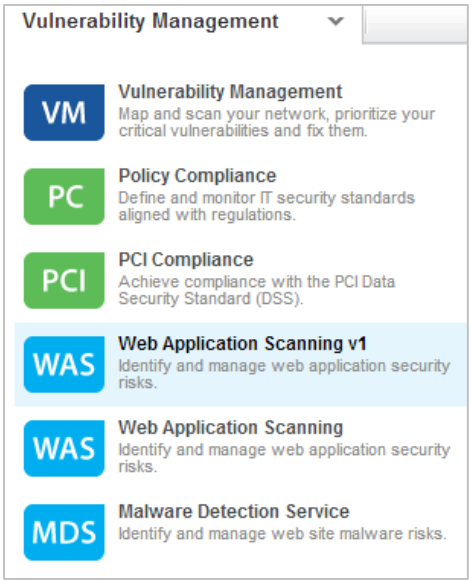


Figura 3. 142 Módulo Qualys WAS

Par empezar con el escaneo, es necesario añadir el servidor web que va a ser analizado (ver Figura. 3.143.).

Figura. 3.143. Ingreso de Aplicación Web en Qualys WAS

A continuación se realiza un análisis de vulnerabilidades (ver Figura. 3.144.), chequeando toda la información en busca de vulnerabilidades como Cross Site Scripting (XSS), SQL Injection, etc.

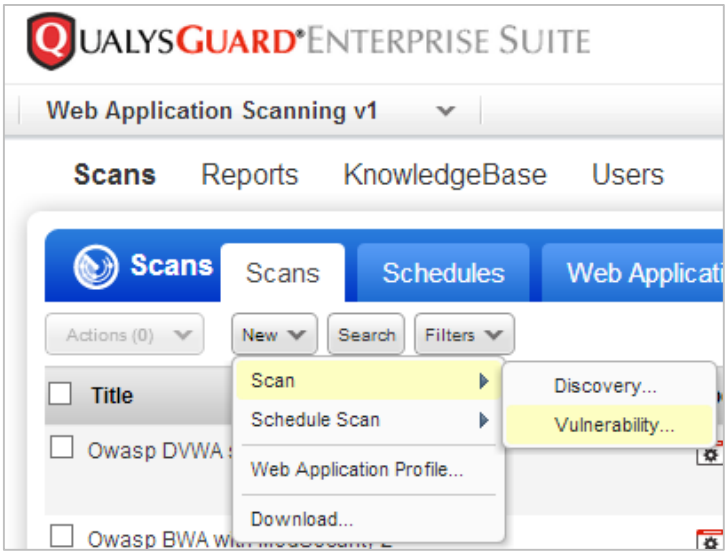


Figura. 3.144. Análisis de vulnerabilidades con Qualys WAS

Al realizar un escaneo de vulnerabilidades, se escoge la aplicación web a la cual se le realizará el escaneo, además se pueden escoger las configuraciones como el perfil y autenticación que son las credenciales con las cuales Qualys podrá tener mayor acceso (ver Figura. 3.145.).

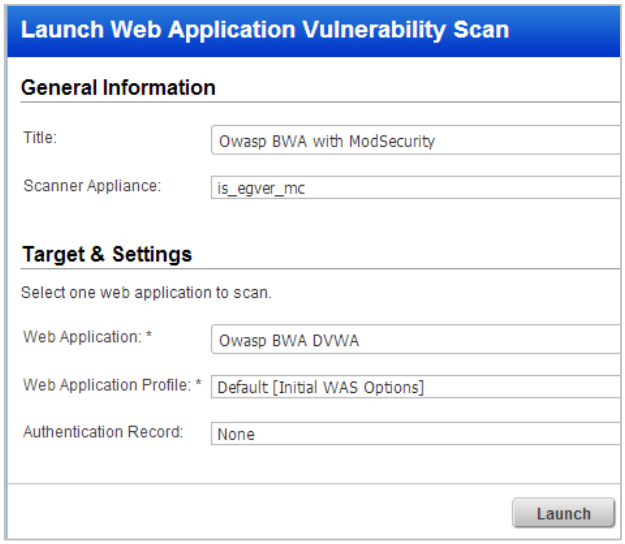


Figura. 3.145. Ejecución de Escaneo con Qualys WAS

Cuando el escaneo ha finalizado se verá el estado del mismo, el host analizado, la duración del escaneo, etc. (ver Figura. 3.146.), además se podrá realizar la descarga del reporte en el formato deseado para su posterior análisis (ver Figura. 3.147.).

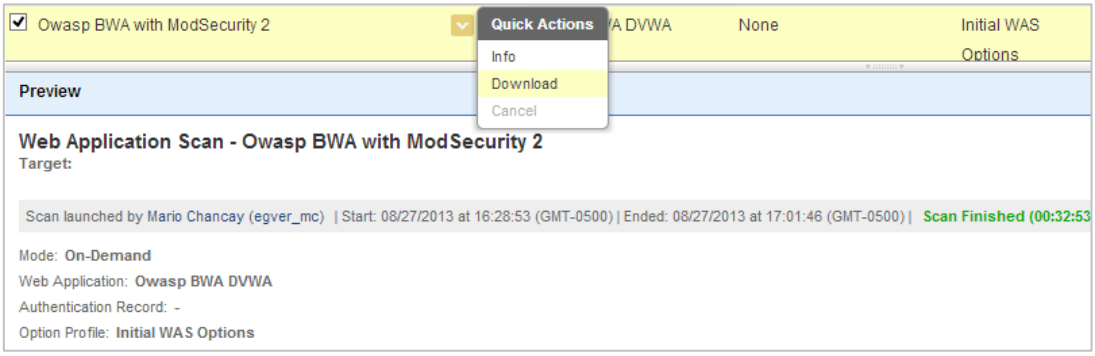


Figura. 3.146. Finalización de Escaneo con Qualys WAS

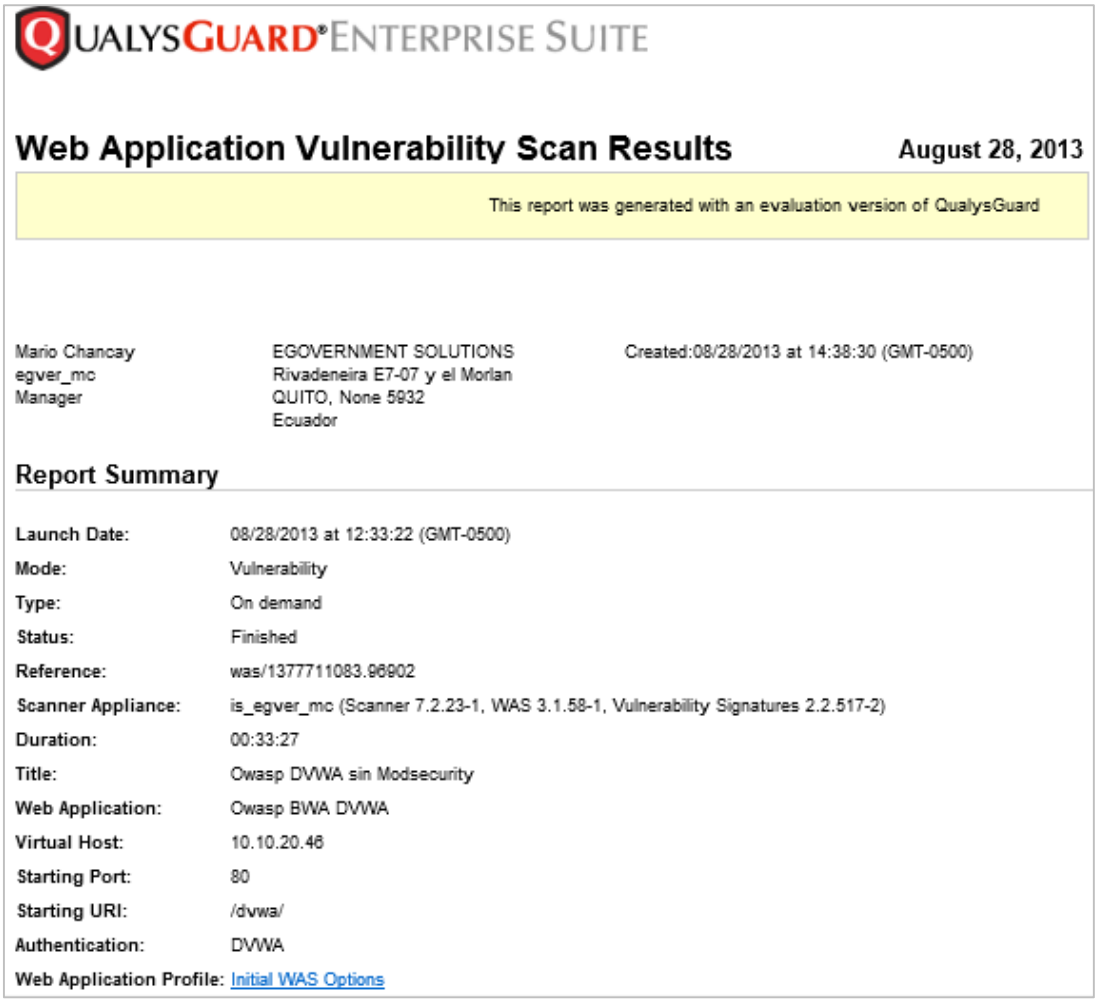


Figura. 3.147. Reporte de Qualys WAS

Finalmente se observará en el reporte las vulnerabilidades encontradas, para que de esta manera se pueda ver el grado de riesgo de la vulnerabilidad, el malware que está asociado a esta vulnerabilidad, el impacto de la misma y uno de los puntos más importantes es saber si es explotable (ver Figura. 3.148.).

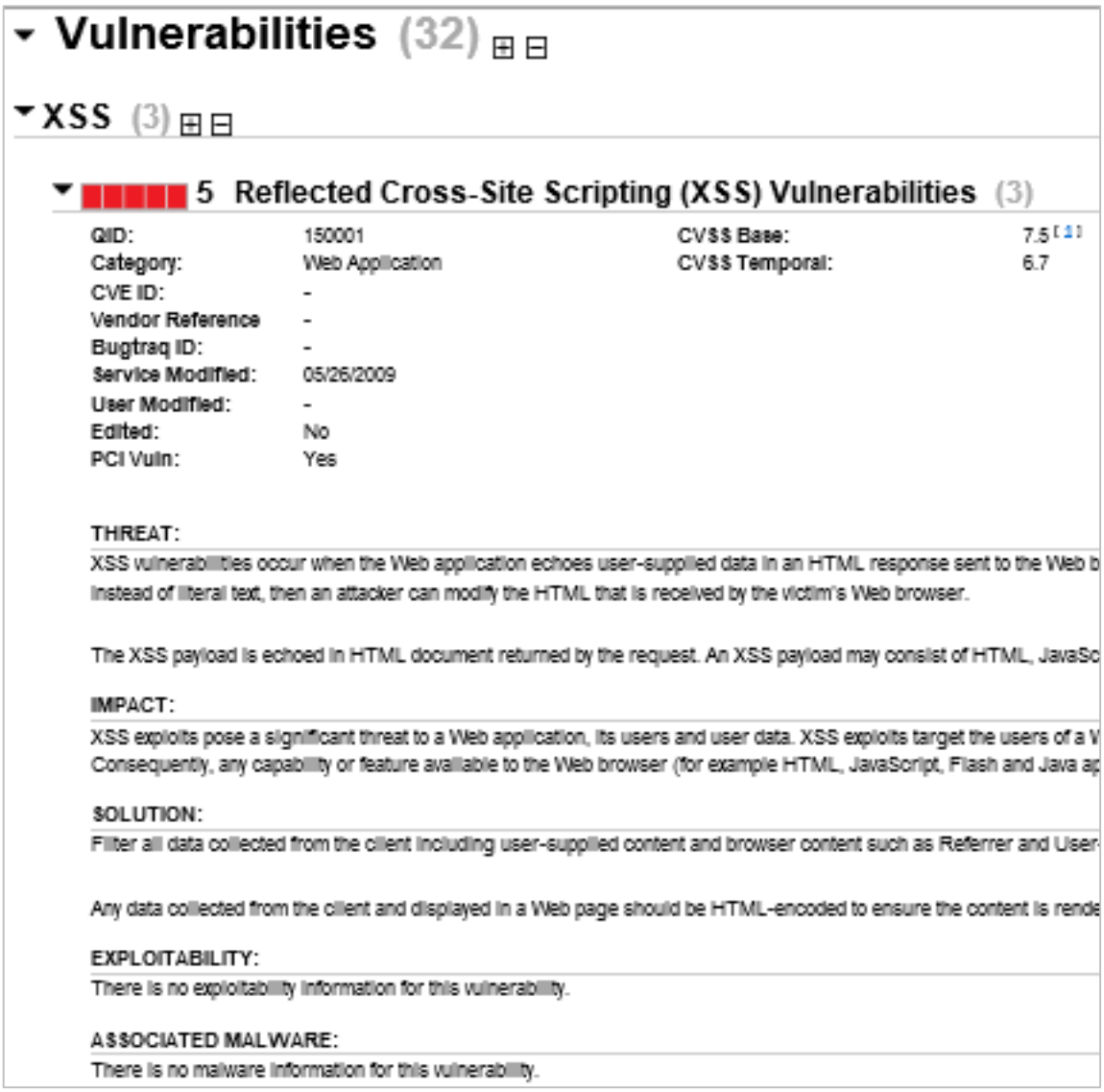


Figura. 3.148. Reporte Detallado de Qualys WAS

3.8.3. Ventajas y desventajas

Ventajas

- Interfaz de usuario amigable
- Reportes flexibles y totalmente personalizables en diferentes formatos.
- Escaneos de aplicaciones web que contienen JavaScript y flash.

- Realiza un análisis más profundo que herramientas open source.

Desventajas

- Herramienta Costosa.
- Basada en web.

CAPÍTULO IV

SEGURIDAD EN ESTACIONES DE TRABAJO Y FACTOR HUMANO

4.1. INTRODUCCIÓN

La seguridad en los dispositivos finales es tan importantes como la de la zona perimetral, las razones principales son las siguientes:

- Para proteger a los dispositivos de propagaciones y ataques laterales, es decir que provengan de la red interna.
- Brindar protección contra ejecución de archivos en dispositivos fijos y móviles.
- Proteger a los dispositivos del ingreso de archivos maliciosos por medio de elementos ejecutables.

Las soluciones que se proveen para este tipo son las más comunes y las que principalmente se sugieren para un entorno personal, además del empresarial.

En este ámbito de la seguridad informática, este es el campo en el que más competidores se encuentran, debido al bajo costo y al alto target que tienen estos productos (dispositivos móviles y fijos tanto empresariales como personales). (ver Figura. 4.1.).

Figura. 4.1. Ejemplos de empresas que brindan seguridad para dispositivos finales

4.2. EL FACTOR HUMANO DENTRO DE LA SEGURIDAD DE LA RED

"Una cadena es tan fuerte como su eslabón más débil" ([44] Reid, 1700), en ámbito de seguridad es necesario proteger todos los "eslabones" del mismo y por lo general el más débil es el factor humano, debido a la falta de conocimiento de la variedad de ataques cibernéticos y técnicas que se utilizan para los mismos.

Por otro lado también es influyente la creciente cantidad de datos personales y empresariales que se encuentran actualmente en la "nube", hay suficiente información que puede aprovechar un atacante para realizar su cometido en redes sociales, en sitios de almacenamiento (dropbox, 4shared, skydrive, etc.) y en correos electrónicos.

Para esto es necesario que todas las personas que forman parte de la empresa tengan un conocimiento de las amenazas actuales y como las mismas pueden ser un riesgo para la empresa y su información.

Hay que tomar en cuenta que cualquier persona puede ser una amenaza para la empresa, sobre todo las que no suelen tener un amplio conocimiento informático como son desde las personas operativas (guardia, secretaria) hasta la parte

gerencial que precisamente suele ser la más atacada debido a la cantidad de información y privilegios que posee dentro de la red, es decir en algunas empresas el gerente tiene muchas más libertades de navegación, además de poseer datos extremadamente sensibles como contraseñas, información de empleados, datos de cuenta, etc.

4.3. INGENIERÍA SOCIAL

La ingeniería social, en términos informáticos, es el arte o la manipulación para que la gente ejecute diferentes acciones y así obtener información confidencial, acceso o privilegios a los dispositivos informáticos. ([12] Pazmiño, 2012)

Los atacantes informáticos se valen de numerosas técnicas, utilizando como su principal herramienta los correos electrónicos, redes sociales, chats, internet en general y los dispositivos extraíbles.

Las características de un atacante son las siguientes: ([12] Pazmiño, 2012)

- Se mostrará amigable con el objetivo
- Buscará ganarse la confianza del objetivo
- Suelen ser personas jóvenes
- Buscarán las afinidades del objetivo a fin de llegar al punto afectivo del mismo

Dependiendo del valor de la información que se está buscando, el tiempo puede ser indiferente he incluso el mismo puede llegar a demorar años.

Los ataques basados en redes sociales generalmente son dirigidos a gente entre 12 y 27 años, en el que se concentrará en obtener amistad en función de juegos y grupos afines a los gustos del objetivo, buscando información personal como ausencia o presencia de adultos en la casa, dirección, lugares frecuentados, situación económica, etc. ([12] Pazmiño, 2012)

Tanto en chat como en redes sociales, los ataques son dirigidos generalmente a relaciones personales (amor y amistad) buscando la extorsión del objetivo, en los cuales se crean perfiles falsos para obtener cualquier tipo de información.

Los dispositivos extraíbles son utilizados para la ejecución de archivos maliciosos sobretodo aprovechando la reproducción automática configurada en la mayoría de dispositivos finales.

Por correo electrónico, es muy común el vulnerar el interés del objetivo en ganar dinero fácil, para este casó es muy común los ataques de phishing, los cuales consisten en simular correos y páginas electrónicas de organizaciones o entidades financieras, buscando que el objetivo haga clic en links que parecen verdaderos y así obtener números de tarjetas de crédito, contraseñas, información personal o incluso transferencia de dinero a cuentas falsas.

Pueden existir varias técnicas ingeniosas dentro de estos correos, por ejemplo los mismos suelen tener un aviso de haber ganado la lotería y el correo tiene documentos adjuntos, además de un mensaje completo que detalla el procedimiento para retirar el dinero (ver Figura. 4.2.).

Figura. 4.2. Ejemplo de correo malicioso con mensaje de haber ganado la lotería

Ataques un poco más avanzados pueden mandar correos electrónicos sabiendo la entidad financiera en la que el objetivo ti abierta una cuenta y mandar un correo con un formato casi exacto al de la entidad financiera solicitando ingresar a un link para actualización de datos donde el mismo suele tener un nombre muy similar que parece real (ver Figura. 4.3.).

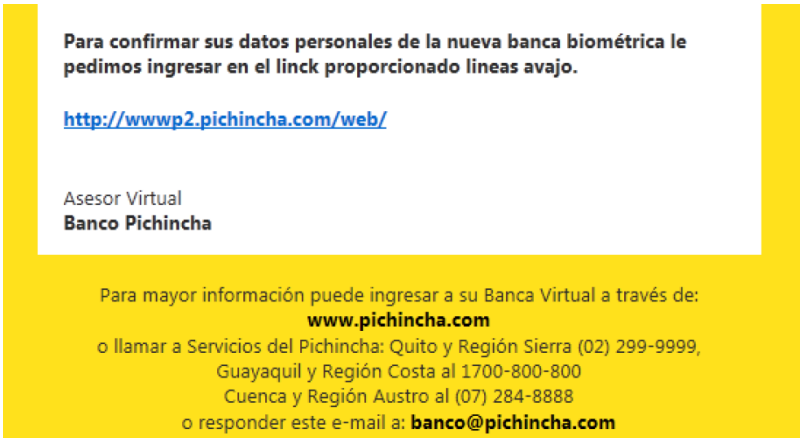


Figura. 4.3 Ejemplo de correo malicio de una entidad financiera con un link ficticio

La mejor defensa para estos tipos de ataques consiste en:

- Estar informados.
- Validar la direcciones a las que se conecta (posicionando el ratón sobre el link sin dar clic en el mismo o investigándola en sitios de filtrado de url como www.virustotal.com o www.urlvoid.com).
- Evitar el ingreso de información en sitios que no sean de entera confianza.
- Validar que los sitios que deban estar cifrados, lo estén (conexiones https).
- Compartir con el resto de gente y comunidad los ataques encontrados.

4.4. INTERNET SECURITY

4.4.1. Introducción

Todas las empresas que proveen soluciones para dispositivos finales suelen presentar una variedad de productos dividido en dos principales categorías:

- Hogar y empresas pequeñas
- Empresas medianas y grandes

Para hogar y empresas pequeñas se ofrecen productos que son administrados dentro del dispositivo del usuario final y tienen un coste muy accesible, en cambio las soluciones para empresa medianas y grandes tiene una consola de administración por la cual se configuran todos los dispositivos empresariales y además suelen tener características de protección reemplazando a seguridades perimetrales como filtrado URL, control de aplicaciones, etc.

Para este caso se utilizará una solución para hogar y empresas pequeñas ya que se busca una protección local, además que la cantidad de usuarios no justifica la inversión y administración que requiere una soluciona para empresas medianas y grandes.

El producto más completo para hogar y empresas pequeñas se suele llamar Internet Security independientemente de la marca. Existen varias marcas pioneras que han demostrado continuidad y liderato, las cuales son:

- Kaspersky
- Symantec
- McAfee
- Trend Micro
- Sophos

Estas cinco empresas han sido las líderes por dos años consecutivos en el cuadrante mágico de Gartner para seguridad de dispositivos finales (ver Figura. 4.4.).

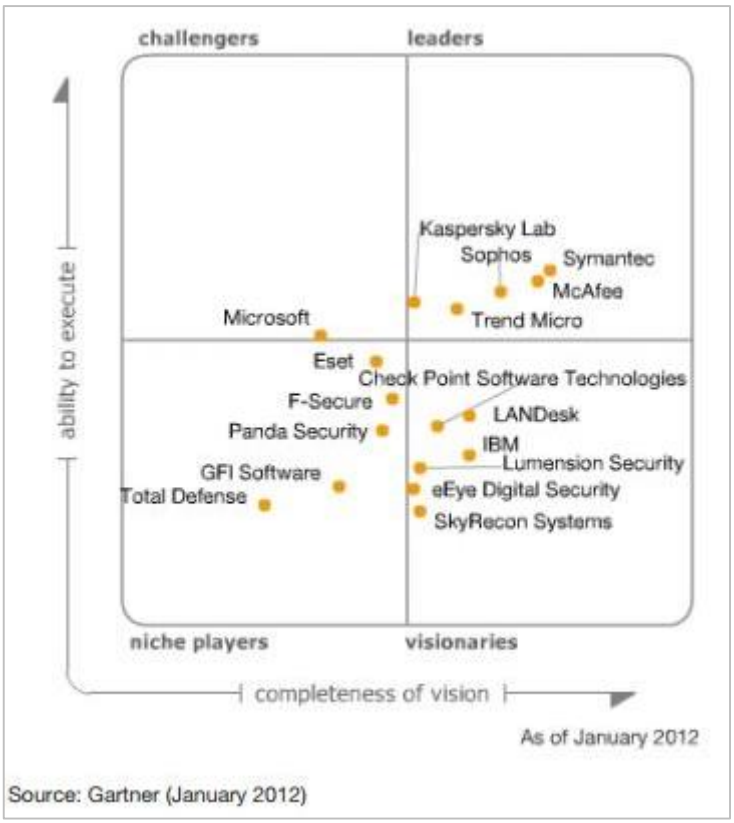


Figura. 4.4. Cuadrante de Gartner para seguridad de dispositivos móviles de enero de 2012 ([45] Gartner, 2012)

Es una difícil tarea decidir cuál de estos cinco productos es el mejor ya que entre los mismos se han dividido diferentes premios reconocidos internacionalmente por lo que se considera que se debe buscar un producto que se adapte a las necesidades específicas de cada empresa.

Para este proyecto se ha seleccionado como producto a Kaspersky Internet Security debido a la constancia de la empresa y ser un producto de impacto mínimo en el rendimiento del dispositivo final y alto nivel de protección. Prueba de esto es haber ganado sido elegido como la mejor protección antivirus dentro del reporte realizado por los laboratorios tecnológicos Dennis (www.DennisTechnologyLabs.com) entre abril y junio del 2013 (ver Figura. 4.5.).

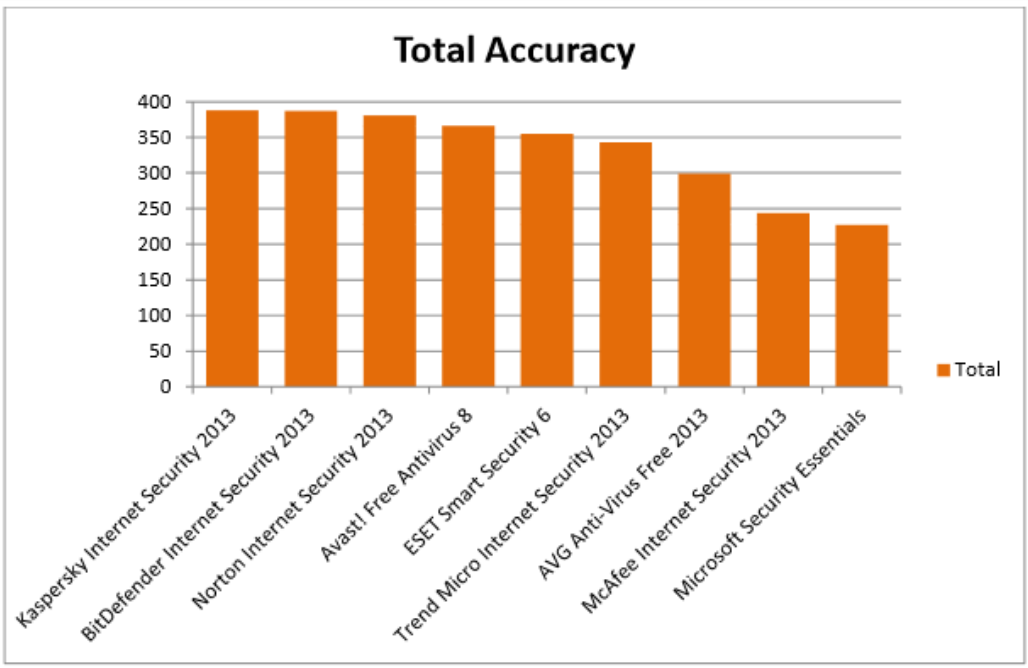
Figura. 4.5. Kasperky elegido como la mejor protección antivirus dentro del reporte de los laboratorios Dennis ([46] Kaspersky Lab, 2013)

Este informe tiene como objetivo comparar la eficacia de los productos anti-malware proporcionados por empresas de seguridad conocidos. Los productos se exponen a las amenazas de Internet que se viven durante el periodo de prueba. Esta exposición se llevó a cabo de una manera realista, lo que refleja estrechamente la experiencia de un cliente. Estos resultados reflejan lo que habría pasado si un usuario estaba usando uno de los productos y visitó un sitio web infectado. ([47] Dennis Technology Labs, 2013)

Los productos probados fueron los siguientes:

- AVG Anti-Virus Free 2013
- Avast! Free Antivirus 8
- BitDefender Internet Security 2013
- ESET Smart Security 6
- Kaspersky Internet Security 2013
- McAfee Internet Security 2013
- Microsoft Security Essentials
- Norton Internet Security 2013
- Trend Micro Internet Security 2013

El resultado del reporte fue que Kasperky Internet Security 2013 obtuvo 388 de 400 puntos posibles, siendo este el mejor puntaje de los productos probados (ver Figura. 4.6.).



The total accuracy ratings take into account successes and failures with both malware and legitimate applications.

TOTAL ACCURACY RATINGS

Product	Total Accuracy Rating	Percentage	Award
Kaspersky Internet Security 2013	388	97%	AAA
BitDefender Internet Security 2013	386.8	97%	AAA
Norton Internet Security 2013	381	95%	AAA
Avast! Free Antivirus 8	366.25	92%	AA
ESET Smart Security 6	354.95	89%	A
Trend Micro Internet Security 2013	343	86%	A
AVG Anti-Virus Free 2013	299	75%	C
McAfee Internet Security 2013	243.9	61%	-
Microsoft Security Essentials	227	57%	-

Figura. 4.6. Reporte realizado por los laboratorios Dennis entre abril y junio de 2013 ([47] Dennis Technology Labs, 2013)

4.4.2. Características

Kaspersky Internet Security se especializa en la protección de los dispositivos finales y en todo el vector de ataque que puede venir asociado con el mismo. Las características principales son las siguientes: ([48] Kaspersky Lab, 2013)

- Protección contra virus y amenazas de Internet.- Al combinar funcionalidad basada en la nube y poderosas tecnologías de seguridad que se ejecutan en la estación de trabajo, Kaspersky Internet Security 2013 proporciona

defensas más eficaces contra las amenazas cada vez más complejas de hoy.

- Detecta amenazas nuevas y emergentes.- La solución Kaspersky Security Network, basada en la nube, recopila la información de millones de sistemas de usuarios alrededor del mundo como ayuda para actualizar la base de datos con los virus y ataques de malware más recientes. Las posibles amenazas se monitorean y se analizan en tiempo real.
- Identifica sitios web sospechosos y sitios web de phishing.- Las tecnologías anti-phishing detectan proactivamente URL fraudulentos y usan información en tiempo real, desde la nube. La característica URL Advisor también agrega etiquetas con códigos de colores a todos los enlaces web con el fin de advertir sobre el nivel de peligro de un enlace y de las páginas subsiguientes.
- Brinda mayor seguridad para compras y actividades bancarias en línea.- Kaspersky Internet Security ha incluido siempre capas adicionales de seguridad que ayudan a proteger su información durante las transacciones en línea. Safe Money comprueba automáticamente que el sitio web que se está visitando es seguro y además es posible abrirlo en un modo especial y protegido para mantener a salvo la información confidencial.
- Protege la privacidad e identidad digital.- Kaspersky Internet Security 2013 ofrece una amplia gama de tecnologías para proteger su privacidad y su identidad, incluidas dos características de seguridad únicas para el ingreso de información personal en línea:
    - Secure Keyboard es una nueva tecnología de Kaspersky que se activa automáticamente cada vez que abre el sitio web de un banco, un sitio web de pagos o que ingresa una contraseña en cualquier página web, esto para asegurarse de que los keyloggers no tengan acceso a la información que se ingresa con el teclado físico.
    - La característica Virtual Keyboard mejorada de Kaspersky permite usar clics del mouse para ingresar la información bancaria, de modo que las teclas que presiona no puedan ser rastreadas ni robadas por keyloggers, hackers o ladrones de identidad.
- Impide que el malware aproveche las vulnerabilidades de la estación de trabajo.- Si en el dispositivo final existen vulnerabilidades de aplicaciones o

del sistema que no se han actualizado con las correcciones más recientes, además de buscar vulnerabilidades, Kaspersky Internet Security 2013 analiza y controla las acciones de programas que las tienen de modo, que no puedan provocar daños.

4.4.3. Antivirus

La principal característica de un Internet Security es que es un antivirus con beneficios adicionales. El antivirus ayudará a proteger los dispositivos finales de los ataques conocidos y todo lo que sea capaz de descubrir el laboratorio interno de Kaspersky mediante la información que pueden proveer sus usuarios alrededor del mundo.

En la Tabla. 4.1 se puede visualizar claramente cuáles son las diferencias

Comparación	Internet Security 2013	Antivirus 2013
Protección híbrida La protección híbrida combina el poder de la nube las avanzadas tecnologías que residen en la estación de trabajo a fin de brindar una respuesta más rápida y efectiva ante las complejas amenazas de la actualidad		

Reacción rápida y detección anticipada de software malicioso Las nuevas tecnologías de Kaspersky con capaces de proteger gracias a los datos en tiempo real provenientes de la nube. Además, tiene la posibilidad de conectarse con millones de usuarios que participan en Kaspersky Security Network en todo el mundo.		
Prevención automática contra exploits Incluso si la estación de trabajo y las aplicaciones en ejecución no se han actualizado con las últimas correcciones, Kaspersky puede impedir el aprovechamiento de vulnerabilidades.		
Mejor protección anti-phishing Un nuevo motor anti-phishing mejora las defensas contra las acciones que realizan estafadores de Internet para obtener acceso a información confidencial.		
Safe Money Kaspersky Internet Security siempre ha brindado protección para las transacciones en línea y, en su versión más reciente, cada vez que intenta iniciar sesión en un banco en línea, un sitio web de un sistema de pagos o un sitio de comercio electrónico comprueba automáticamente que el sitio web que se está visitando es seguro y además es posible abrirlo en un modo especial y protegido para mantener a salvo la información confidencial.		

Firewall Bidirecional El firewall bidireccional proporciona un perímetro seguro alrededor del equipo para evitar que la infiltración por puertos desconocidos.		
Módulo antispam El módulo anti-spam nuevo y mejorado proporciona un filtro más confiable de mensajes no deseados, además de informes optimizados sobre el spam detectado.		

Tabla. 4.1. Comparación entre Internet Security y antivirus de Kaspersky ([48] Kaspersky Lab, 2013)

4.4.4. Funcionamiento interno

El núcleo de un Internet Security es su antivirus, ya que es la parte que más análisis y procesamiento va a realizar.

Un antivirus para dispositivo final es un software que se instala en la estación de trabajo y es capaz de realizar análisis bajo demanda o programada en busca de software malicioso. Esta es una solución basada en firmas, que realiza análisis de diversos tipos de información y en caso de que se encuentre un archivo infectado procede, de ser posible a desinfectarlo (ver Figura. 4.7.).

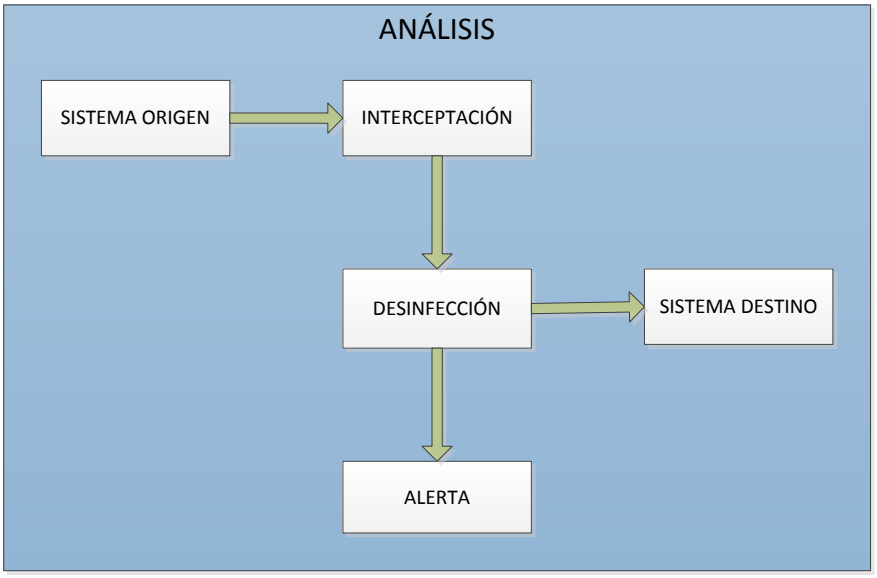


Figura. 4.7. Funcionamiento interno de un antivirus

Lo más importante de un antivirus es la calidad del laboratorio que tiene y la cantidad de información que puede recibir de todos sus clientes y colaboradores alrededor del mundo, porque de esta manera puede comprender más rápidamente nuevos ataques que aparezcan, poder identificarlos y de esta manera realizar la creación de una firma para así poder actualizar y proteger a todos sus sistemas alrededor del mundo.

Es por esto que es muy importante tener siempre actualizado el antivirus para poder recibir la información suficiente y firmas que nos provee el laboratorio de investigación, en este caso, de Kaspersky.

4.4.5. Configuración

Una vez que ha sido correctamente instalado el software dentro del dispositivo final, es necesario realizar un análisis y posteriormente se observará una pantalla que indica el correcto estado de la aplicación (ver Figura. 4.8.).

Figura. 4.8. Estatus de Kaspersky Internet Security 2013

Este es un software que viene pre configurado por defecto, por lo que, a menos que se desee, no hay que realizar configuraciones adicionales y únicamente es necesario verificar que todas las características del Internet Security se encuentren habilitadas (ver Figura. 4.9.).

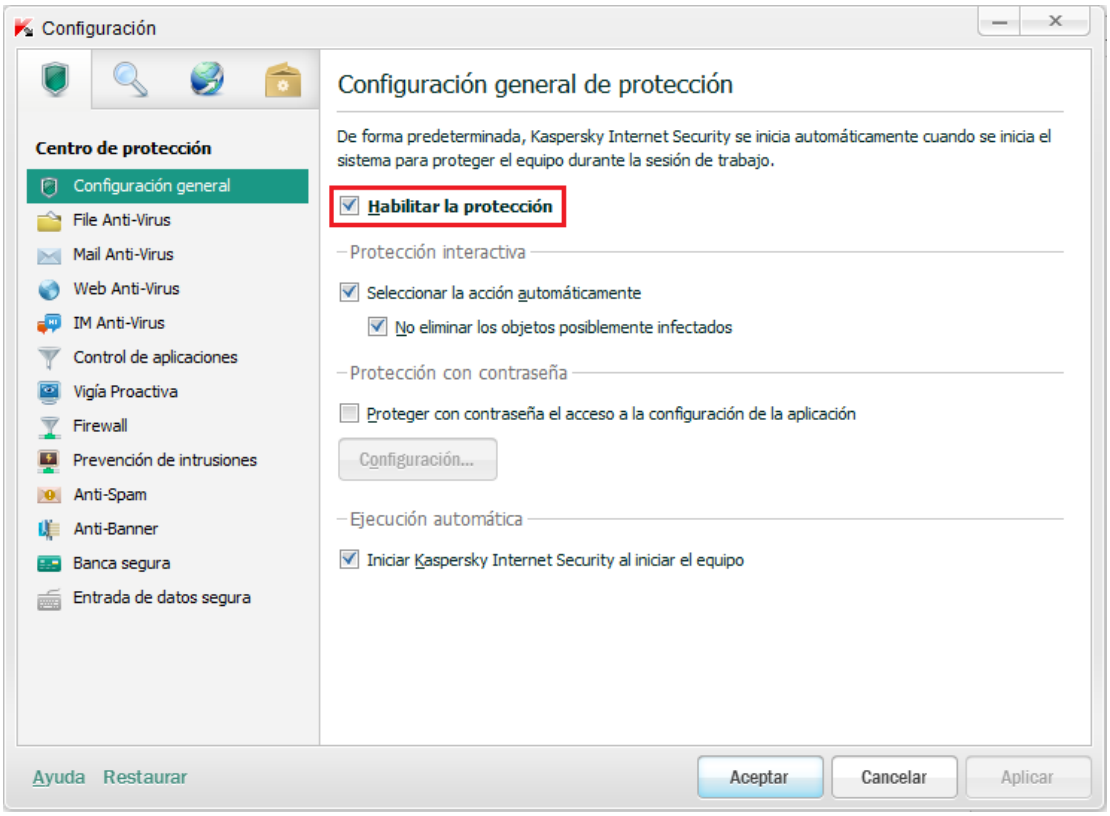


Figura. 4.9. Configuración de Kaspersky Internet Security 2013

4.4.6. Interpretación de resultados

Debido a que esta herramienta es para uso de expertos y no expertos en temas de seguridad informática, la interpretación de resultados es sumamente sencilla. Para demostrar esto se va a realizar la descarga de un archivo del sitio www.eicar.org, el cuál es un proyecto que permite comprobar el correcto funcionamiento de cualquier sistema antivirus sin realizar la descarga de un archivo malicioso real.

La generación de la alerta es la que mostrará la información del malware detectado, sin embargo lo más importante es la acción ya que esta nos indicará si fue bloqueado o no el intento de infección (ver Figura. 4.10.).

Figura. 4.10. Bloqueo de intento de infección con el archivo eicar

De la misma forma dentro de la consola se podrá visualizar la acción y el tipo de evento detectado (ver Figura. 4.11.).

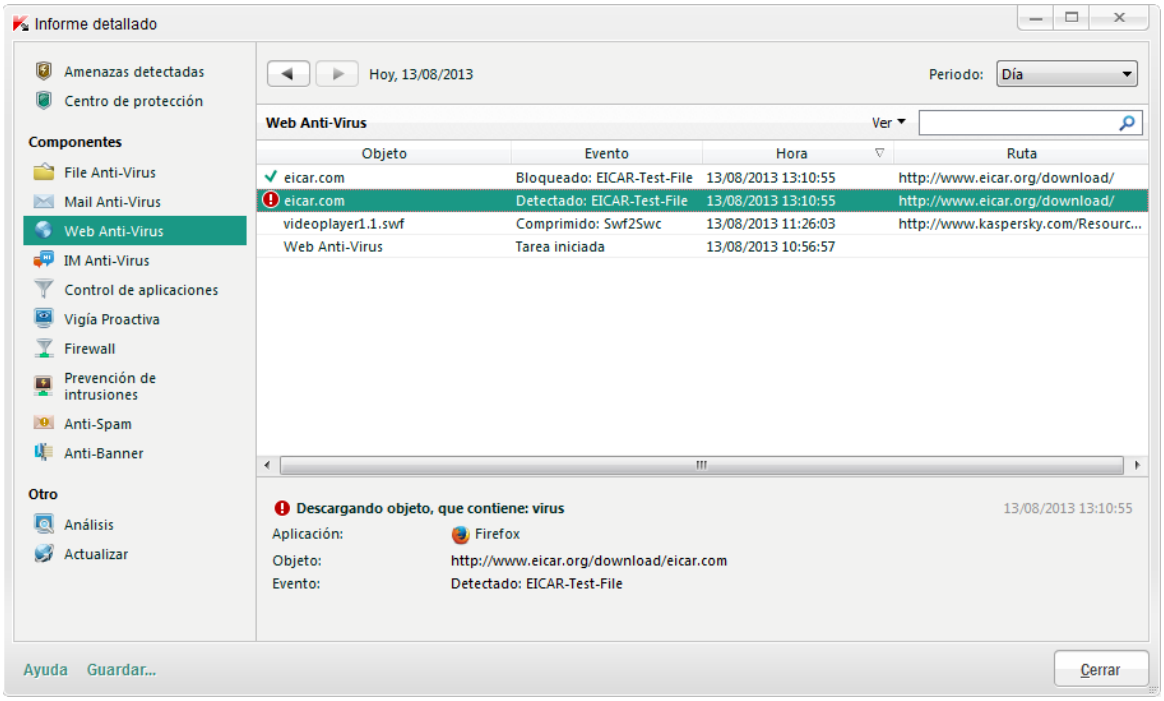


Figura 4. 11 Visualización dentro de la consola de intento de infección con el archivo eicar

4.4.7. Ventajas y desventajas

Ventajas

- Se enfoca en archivos maliciosos a nivel de dispositivo final.
- Los laboratorios sofisticados y la ayuda en tiempo real de colaboradores y clientes proveen una respuesta ágil en caso de nuevas amenazas descubiertas.
- Costo muy bajo.
- Afectación mínima en el rendimiento de la estación de trabajo.
- Provee protecciones adicionales al momento de ingresar información confidencial por medio de tráfico web.

Desventajas

- Es basado en firmas.
- Es incapaz de detectar un ataque sin una firma de por medio.
- No puede descifrar tráfico.

4.5. ACTUALIZACIÓN DE PARCHES (SECUNIA PSI)

Los cambios que se realizan constantemente a los programas con el fin de actualizarlos, modificarlos, aumentar su funcionalidad o corregir errores, son denominados parches, los mismos que son útiles para evitar que existan vulnerabilidades en el sistema al tener programas desactualizados.

Los parches son desarrollados por las mismas empresas creadoras de los programas o sistemas operativos con el fin de remediar posibles errores, los parches pueden crearse para el código fuente, para archivos binarios de un programa o hasta para sistemas operativos completos dependiendo de las necesidades.

4.5.1. Introducción

Secunia PSI (Secunia Personal Software Inspector) es un software gratuito que ayuda a identificar vulnerabilidades que se encuentran presentes en el sistema y que no pertenecen a Microsoft, cuando los programas se encuentran desactualizados pueden dejar al sistema abierto ante cualquier ataque.

Secunia PSI se encarga de verificar que los programas instalados estén actualizados, para evitar así vulnerabilidades que podrían ser aprovechadas para realizar ataques.

La finalidad de esta herramienta no es analizar la configuración del sistema operativo, para saber si está desprotegido, o conocer si las configuraciones son adecuadas, el objetivo de Secunia PSI es encontrar agujeros en los programas instalados. ([49] Secunia, 2013)

4.5.2. Configuración

Una vez descargada e instalada la última versión de Secunia PSI, se procede a realizar un escaneo completo del equipo, para verificar el estado de los programas (ver Figura. 4.12.).

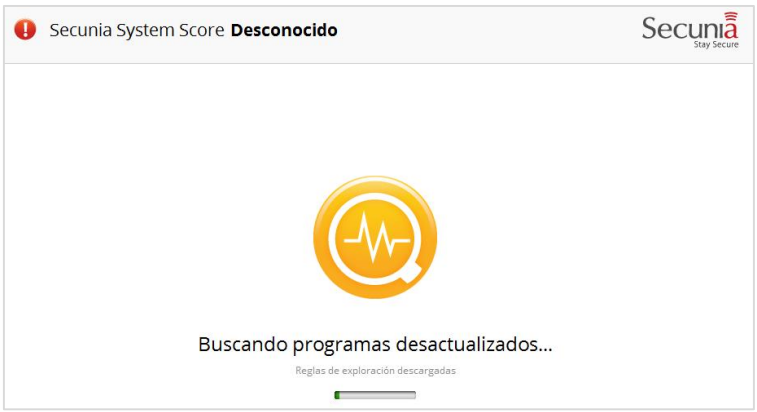


Figura. 4.12. Búsqueda de programas desactualizados con Secunia PSI

En caso de encontrar programas que se encuentran desactualizados, la herramienta buscará el parche necesario, y según las configuraciones del usuario

podrá descargar e instalar ya sea de manera automática o manual todos los parches que sean necesarios para dejar el programa trabajando con la última versión del mismo (ver Figura. 4.13.).

Figura. 4.13. Programas desactualizados detectados por Secunia PSI

4.5.3. Ventajas y desventajas

Ventajas

- No se necesita actualizar manualmente los programas instalados en el equipo, pues Secunia PSI lo hace de manera automática.
- Tiene gran cantidad de programas en su base de datos para mantenerlos actualizados.
- Es gratuito

Desventajas

- Consume recursos del sistema.
- Contiene algunos bugs al intentar la descarga de actualizaciones automáticas.

4.6. CAPACITACIÓN DEL FACTOR HUMANO

La mejor forma de prevenir que el factor humano sea el eslabón más débil en la cadena de seguridad es capacitándolo y manteniéndole informado de los avances tecnológicos concernientes con el tema de los ataques cibernéticos.

Lo ideal es realizar una capacitación inicial de ocho horas con todo el personal nuevo (o que no haya sido capacitado) para asegurar que todos tengan una noción base de la importancia de la seguridad de la información y como protegerse. La capacitación debe comprender los siguientes temas:

- Importancia de la seguridad de la información
    - ¿Qué es la información?
    - ¿Qué es información confidencial?
    - ¿Dónde está la información confidencial?
    - ¿Por qué es necesario proteger la información?

- Ataques cibernéticos
    - ¿Qué son los ataques cibernéticos?
    - ¿Cómo aparecieron los ataques cibernéticos?
    - ¿Qué buscan los atacantes?
    - ¿A quiénes pueden afectar los ataques cibernéticos?
    - ¿De qué formas pueden afectar los ataques cibernéticos?
    - ¿Qué tan protegidos estamos?

- Ingeniería social
    - ¿Qué es la ingeniería social?
    - ¿Cuál es la psicología del atacante?
    - ¿Cuál es la psicología del ataque?
    - ¿Cómo se identifica un ataque?

- Remediaciones
    - ¿Cómo nos protegemos de los ataques cibernéticos?
    - ¿Qué debo hacer si me encuentro con algo sospechoso?

- ¿Qué debo hacer si estoy siendo atacado o sé que alguien está siendo atacado?
- ¿Con quién puedo hablar de estos temas?
- ¿Cómo le protejo a mi comunidad?

Posterior a está capacitación es necesario realizar sesiones cortas permanentes, aproximadamente cada dos meses. Estas sesiones pueden ser de una o dos horas y el objetivo de las mismas debe ser una charla con moderador que permita conocer los cambios que han existido desde la última reunión y que le gente pueda contar sus experiencias reales.

4.7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE UNA EMPRESA

Las políticas de seguridad de la información son un documento de alto nivel establecido por la gerencia y el departamento de seguridad de la información en el que se debe expresar el compromiso de la empresa acerca de la protección de su información y la de sus empleados. ([50] Microsoft, 2011)

Este documento debe tener definiciones básicas para que todo el que lo lea comprenda el significado de cada término y sobretodo que es lo que entiende la empresa como seguridad de la información.

Los pasos a seguir serán los siguientes:

Paso 1: Crear las política de seguridad.- Son normas que dirigirán al usuario a utilizar de manera responsable y consiente los recursos empresariales y evitar su uso indebido que podría ocasionar serios problemas en los activos de una empresa. Las políticas son documentos que contienen los lineamientos a seguir por cada uno de los trabajadores donde se definirán las normas, responsabilidades, funciones, etc. Una política de seguridad debe encontrarse totalmente definida, donde se indicará quienes son los responsables de cada área, indicando los roles de cada empleado. Este documento debe encontrarse firmado por cada uno de los

empleados, donde constarán las sanciones respectivas por el incumplimiento de las normas.

Paso 2: Protección de equipos de escritorio y portátiles.-

- Instalación de antivirus.- Todos los equipos tanto portátiles como de escritorio, deberán tener instalado un software antivirus, el cual debe ser actualizado constantemente, y realizar análisis a los equipos periódicamente.
- Actualizar el Software.- Es necesario que todos los equipos se encuentren actualizados, pues cuando un software se encuentra desactualizado es el blanco perfecto para ataques.
- Configuración del Firewall.- restringir los usuarios, tráfico y contenido que tienen acceso a la red.
- Anti Spam.- los trabajadores deben tener claro que al recibir correo electrónico de remitentes desconocidos, estos mail pueden encontrarse infectados con virus, por lo cual se debe implementar la política de eliminar dichos correos sin abrirlos, aparte de esto todo ordenador debe tener instalado filtros de correo para evitar la entrada de spam.
- Utilizar software legal.- Al utilizar programas que no son originales se puede correr el riesgo de que se ejecuten acciones legales contra la empresa, además el software legal garantiza su buen funcionamiento y tiene soporte en caso de errores.
- Realizar una navegación segura.- para que la navegación por internet no traiga problemas de seguridad a la organización es importante cumplir con ciertas normas como acceder únicamente a sitios de confianza, analizar con el antivirus las descargas realizadas, no ingresar a la web desde servidores, descargar programas únicamente desde sitios oficiales, no permitir pop-ups en el navegador, utilizar navegadores sin privilegios para acceder a internet evitando así cambios en el sistema, al acceder a sitios seguros asegurarse que sea una conexión https.

Paso 3: Protección de la red.- Ya sea que la organización tenga una conexión cableada o inalámbrica, es necesario cuidar los siguientes puntos:

- Utilizar constraseñas seguras.- indicar a los empleados la importancia de una constraseña segura, estableciendo como parámetros a seguir una longitud mínima, combinación de letras mayúsculas, minúsculas, números y símbolos, y estableciendo un tiempo en el cual se debe realizar el cambio de la misma.
- Modificar las claves de acceso a la red Wifi periódicamente.
- Configurar el firewall para definir qué comunicaciones van a ser permitidas y cuales denegadas dentro de la red.

Paso 4: Proteger los servidores.-

- Establecer comunicaciones seguras con los clientes a través de certificados del servidor, de manera que la información viajará encriptada utilizando tecnología SSL y así se evite que pueda ser vista por terceras personas.
- Mantener los servidores en una sala adecuada donde mantengan una buena ventilación y con un cableado adecuado para evitar que los mismo puedan ser desconectados por error.

Paso 5: Mantener la información protegida.-

- Realizar copias de seguridad de datos importantes para la organización, normalmente se utiliza para este fin unidades extraíbles.
- Definir los privilegios que va a tener cada usuario, es decir solo ciertos usuarios tendrán acceso al usuario administrador, de esta manera se evitará que usuarios comunes puedan realizar cambios en el sistema sin autorización.
- Cifrar la información más sensible para garantizar la confidencialidad e integridad de los datos dentro de la red, para esto se puede usar el sistema de archivos cifrados EFS para cifrar carpetas y archivos confidenciales.
- Para evitar que los equipos se apaguen de manera inesperada al ocurrir un corte de la energía eléctrica o al existir sobre voltajes es recomendable el uso de equipos de alimentación ininterrumpida.

Paso 6: Proteger las aplicaciones y los recursos.-

- Instalar los últimos Service Packs de la base de datos, y las actualizaciones más recientes para mejorar la seguridad de los equipos.
- Aislar el servidor y realizar periódicamente copias de seguridad del mismo.
- Utilizar un Firewall de Aplicaciones Web para proteger a la organización de ataques específicos contra aplicaciones Web.
- Realizar auditorías para identificar vulnerabilidades en las aplicaciones web.

Paso 7: Gestionar las actualizaciones.-

- Se pueden implementar desde el servidor la revisión de actualizaciones para equipos portátiles de la organización, de manera que se verifique que las actualizaciones se realicen de forma oportuna sin correr el riesgo de que los usuarios se olviden.
- Limitar las capacidades de los usuarios para instalar programas no autorizados, ejecutar programas desde unidades extraíbles o descargar programas de internet.
- Por medio de un equipo administrador realizar un monitoreo de todo el sistema para detectar si ha existido algún cambio o un acceso no autorizado.

Paso 8: Proteger dispositivos móviles.-

Todos los trabajadores deben conocer la importancia de proteger sus dispositivos móviles y a la vez conocer los riesgos que pueden acarrear un mal uso de los mismos.

- Utilizar claves para bloquear los dispositivos móviles.
- No aceptar conexiones de dispositivos desconocidos evitando así transferencias de información no deseada.
- Ignorar mensajes que inciten a realizar descargas o accesos a sitios peligrosos.
- Realizar acceso a Bluetooth por medio de pin.
- Instalar y mantener actualizado un antivirus para dispositivos móviles.
- No descargar software de sitios poco fiables, siempre realizarlo de la página oficial.

- Bloquear la tarjeta SIM en caso de pérdida del teléfono móvil para evitar acceso a datos confidenciales.

Paso 9: Proteger información personal.-

- Cuando se necesite compartir información con terceros, es necesario firmar un acuerdo de confidencialidad, y entregar únicamente la información necesaria, para que en caso de que alguna de las partes rompa dicha confidencialidad se haga responsable por el mal uso de esta información según lo estipulado en el contrato

CAPÍTULO V

EVALUACIÓN DEL SISTEMA INTEGRAL DE SEGURIDAD PROPUESTO

5.1. INTRODUCCIÓN

Las distintas metodologías para análisis de seguridad son las siguientes (ver Figura. 5.1.): ([51] Herzog, 2010)

- Vulnerability Scanning: se refiere generalmente a los chequeos automatizados para encontrar vulnerabilidades conocidas en un sistema o los sistemas de una red.
- Security Scanning: se refiere generalmente a escaneos de vulnerabilidad que incluyen verificación manual de falsos positivos, identificación de debilidades en la red y análisis profesional personalizado.
- Penetration Testing: se refiere generalmente a un proyecto orientado a un objetivo en el cual el objetivo es el trofeo e incluye la obtención de acceso privilegiado a través de condiciones pre-establecidas.
- Risk Assesment: se refiere generalmente a un análisis de seguridad a través de entrevistas e investigación de mediano nivel, la cual incluye justificaciones del negocio, legales y justificaciones específicas a la industria.
- Security Auditing: se refiere generalmente a una inspección de seguridad privilegiada del sistema operativo y las aplicaciones de un sistema o de varios sistemas en varias redes.
- Ethical Hacking: se refiere generalmente a un test de penetración en el cual el objetivo es descubrir trofeos en la red dentro de un tiempo límite del proyecto.

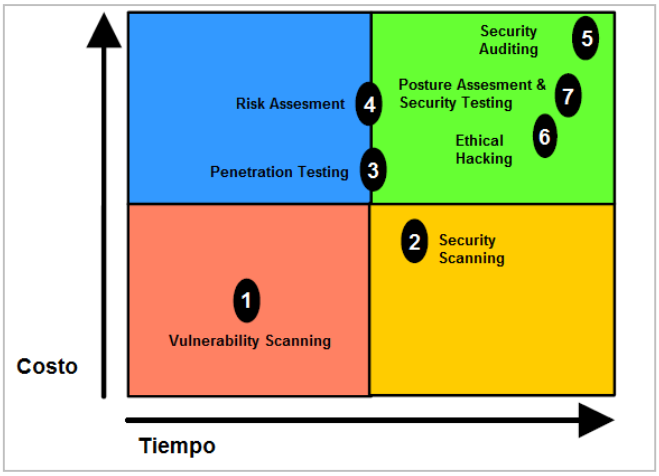


Figura. 5.1. Tipos de metodologías de análisis de seguridad basados en tiempo y costo ([51] Herzog, 2010)

El sistema integral propuesto consiste en la protección de los enlaces de la red de área de campus (Palo Alto Networks), protección del enlace de internet (FireEye y Palo Alto Networks), sistema de detección de intrusos para el enlace de internet (Snort), sistema de detección de botnets por comportamiento (BotHunter), protección de la DMZ (Palo Alto Networks y KFSensor), protección de las aplicaciones web (Palo Alto Networks y ModSecurity) y protección de estaciones finales (Kaspersky y Secunia PSI). A partir de este momento se realizarán pruebas para analizar las respuestas de los diferentes equipos de seguridad.

Las pruebas a realizar son las siguientes:

- Test de penetración desde una de las sedes simuladas a la DMZ
- Test de penetración desde una de las sedes simuladas a una aplicación WEB
- Descarga de diferentes tipos de archivos maliciosos conocidos
- Descarga de un archivo malicioso de día cero
- Infección de un host para análisis de comportamiento con los sensores

5.2. SIMULACIÓN DE ATAQUES

Al utilizar una herramienta líder en el mercado como QualysGuard complementada con herramientas de código abierto BackTrack, se consigue un test de penetración más completo, automatizado y preciso logrando una reducción de

falsos positivos y negativos significativa, lo que permite al cliente reducir el tiempo de interpretación y remediación de las vulnerabilidades, minimizando el riesgo de un posible ataque.

Dentro de las metodologías usadas se cuenta con: Mapeo, Enumeración, Descubrimiento y análisis de vulnerabilidades, etc.

Las pruebas a ejecutar son las siguientes:

- Identificación de Sistemas Operativos, se identifican los sistemas operativos y la versión de los mismos, en busca de información relevante para un atacante.
- Identificación de Servicios, se identifican los servicios y la versión de los mismos, en busca de información relevante para un atacante.
- Escaneo de Puertos, se realiza la identificación activa de los puertos visibles de forma pública, se identifican en ellos la versión de servicio, identificación del mismo, versión y vulnerabilidades.
- Análisis de Vulnerabilidades, se realizan baterías de pruebas tanto a la infraestructura pública de la organización como a las aplicaciones web publicadas. Para identificar claramente vulnerabilidades y problemas de configuración que puedan significar riesgos importantes en la organización.
- Identificación de Información, se identifica la información de valor para un atacante y que puede representar un riesgo para la organización.

Durante la ejecución de las pruebas, se utilizará como marco de trabajo los pasos 1 al 4 descritos en el Open Source Security Testing Methodology (ver Figura. 5.2.). Estos pasos comprenden lo siguiente: ([51] Herzog, 2010)

- Information Gathering: consiste en recopilar toda la información acerca del objetivo a través de medios técnicos y no técnicos.
- Network Mapping: a continuación se debe obtener una “huella” de los dispositivos que se identificaron en el paso anterior. En las actividades se encuentra :
    - Determinar los equipos activos
    - Exploración de puertos y servicios

- Mapeo del perímetro de la red
- Identificar los servicios críticos
- Identificar los sistema operativos y servicios

- Vulnerability Identification: en este punto se detectarán los puntos débiles que son explotables al realizar las siguientes actividades :
  - Identificar servicios vulnerables utilizando los banners de cada servicio
  - Ejecutar una exploración de vulnerabilidades
  - Verificar falsos positivos y negativos
  - Enumerar los vulnerabilidades descubiertas
  - Estimar el probable impacto
  - Identificar las vías de ataque y los escenarios de explotación

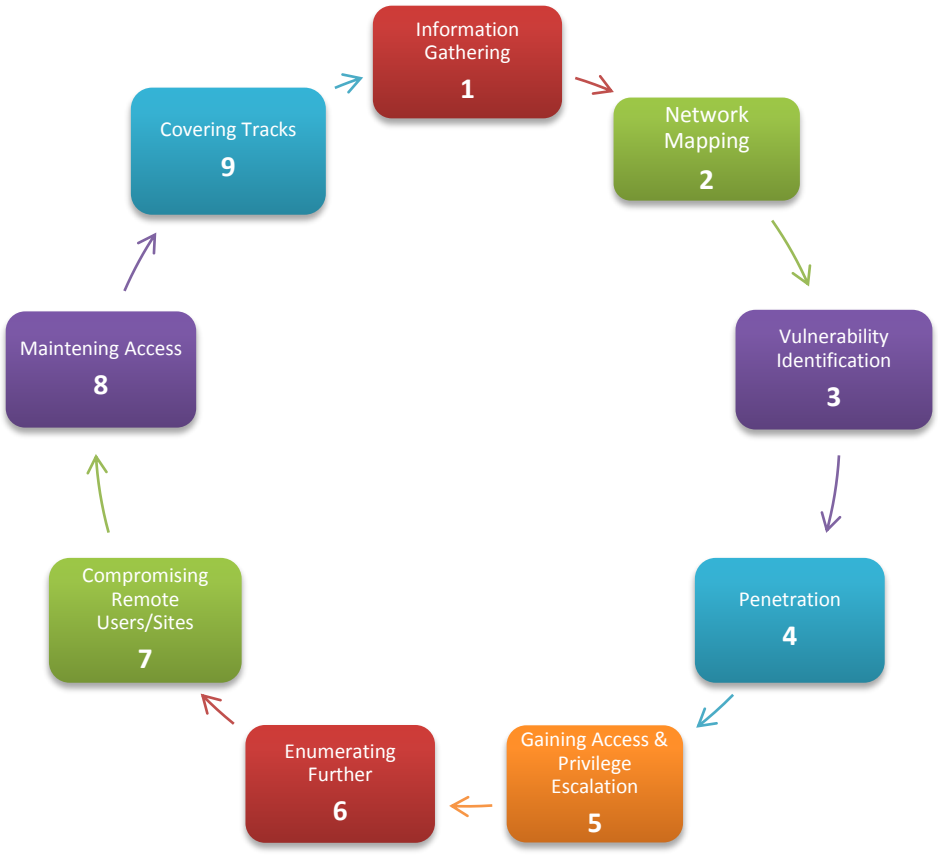


Figura. 5.2. Open Source Security Testing Methodology ([51] Herzog, 2010)

5.2.1. Test de penetración desde una de las sedes a la DMZ

En la presente prueba se evaluará las siguientes herramientas:

- Palo Alto Networks
- KFSensor

El primer servidor a ser analizado es un Windows Server 2008. Una vez realizado el test de penetración, en la Tabla. 5.1. se muestra los resultados otorgados por el equipo de Palo Alto Networks durante los diferentes ataques, tomando una acción de bloqueo para los ataques de severidad mediana, alta y crítica, y de alerta para los ataques de severidad informacional y baja.

Threat	ID	Severity	Action	Count
HTTP Cross Site Scripting Vulnerability	35864	critical	drop-all-packets	2
Apache Chunk Encoding Parsing Buffer Overflow Vulnerability	30143	critical	drop-all-packets	1
Generic HTTP Cross Site Scripting Attempt	31476	High	drop-all-packets	2
Sun ONC RPC Multiple fragments in One Packet Evasion	33191	High	drop-all-packets	1
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	30921	High	drop-all-packets	1
FTP: login Brute-force attempt	40001	High	drop-all-packets	1
AWStats Remote Code Execution Vulnerability	30089	High	drop-all-packets	1
Microsoft Windows win.ini access attempt	30851	High	drop-all-packets	1

Adobe ColdFusion Multiple Directory Traversal Vulnerabilities	33452	High	drop-all-packets	1
Generic HTTP Cross Site Scripting Attempt	31477	High	drop-all-packets	1
Microsoft ASP.NET Path Validation Security Bypass Vulnerability	30133	medium	drop-all-packets	1
Microsoft IIS WebHits.DLL Source Disclosure Vulnerability	30321	medium	drop-all-packets	1
Google Search Appliance ProxyStyleSheet Cross-Site Scripting Vulnerability	30178	medium	drop-all-packets	1
Microsoft IIS Alternate Data Streams ASP Source Disclosure	30319	medium	drop-all-packets	1
Microsoft IIS HTR Request Source Disclosure Vulnerability	30324	medium	drop-all-packets	1
Apache HTTP Server mod_log_config Null Cookie Denial of Service Vulnerability	34945	medium	drop-all-packets	1
HTTP SQL Injection Attempt	30514	medium	drop-all-packets	1
HTTP SQL Injection Attempt	35826	medium	drop-all-packets	1
HTTP SQL Injection Attempt	33338	medium	drop-all-packets	1
raSMP User-Agent Parsing Cross-Site Scripting Vulnerability	33468	medium	drop-all-packets	1
Microsoft ASP.Net Information Leak Vulnerability	33435	Low	alert	3

Cart32 Clients Information Disclosure Vulnerability	30916	Low	alert	1
HTTP Directory Traversal Request Attempt	33194	Low	alert	1
HTTP Directory Traversal Vulnerability	30844	Low	alert	1
HTTP Cross Site Scripting Attempt	32658	Low	alert	1
Cart32 Expdate Information Disclosure Vulnerability	30918	Low	alert	1
SSL Renegotiation Denial of Service Vulnerability	33862	Low	alert	1
Microsoft remote desktop connect initial attempt	33020	informational	alert	5
Microsoft Windows SMB Negotiate Request	35364	informational	alert	3
DNS Zone Transfer AXFR Attempt	33337	informational	alert	2
NetBIOS null sesión	31710	informational	alert	2
FTP Login Failed	40000	informational	alert	1
HTTP TRACE Method	30510	informational	alert	1
Microsoft Windows PNP Service Access	30865	informational	alert	1
HTTP OPTIONS Method	30520	informational	alert	1
Microsoft RPC ISystemActivator bind	30846	informational	alert	1
NetBIOS nbtstat query	31707	informational	alert	1
Microsoft RPC Endpoint Mapper	30845	informational	alert	1
HTTP TRACK Method	30853	informational	alert	1

Tabla. 5.1. Reporte de Palo Alto Networks en el test de penetración al servidor Windows de la DMZ

Posteriormente se procederá a analizar el reporte entregado por Qualys que permitirá visualizar todo lo que un atacante podría hacerlo, pese a tener el equipo de Palo Alto Networks de por medio.

Dentro del reporte entregado por la herramienta, se han encontrado once vulnerabilidades confirmadas y cinco potenciales (ver Figura. 5.3.).

Summary of Vulnerabilities

Vulnerabilities Total	69

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	1	1	0	2
4	0	1	0	1
3	3	3	4	10
2	7	0	11	18
1	0	0	38	38
Total	11	5	53	69

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	6	0	9	15
Information gathering	0	0	10	10
Windows	3	4	2	9
Web server	0	0	9	9
TCP/IP	0	0	8	8
Total	9	4	38	51

Vulnerabilities by Severity

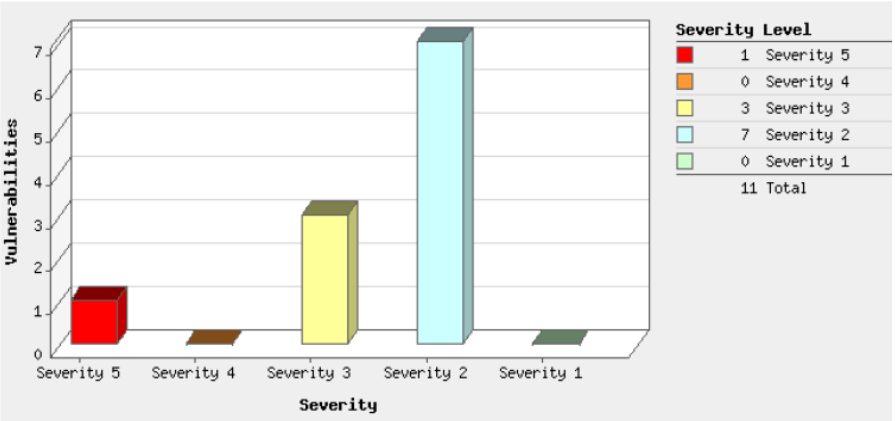


Figura. 5.3. Resumen de vulnerabilidades del servidor Windows de la DMZ

Posteriormente se visualizará la información de sistema operativo y servicios que se encontraros activos en el servidor (ver Figura. 5.4.).

Figura. 5.4. Sistema operativo y servicios detectados en el servidor Windows de la DMZ

Las vulnerabilidades que dejó visualizar el equipo de Palo Alto Networks se pueden ver en la Figura 5.5.:

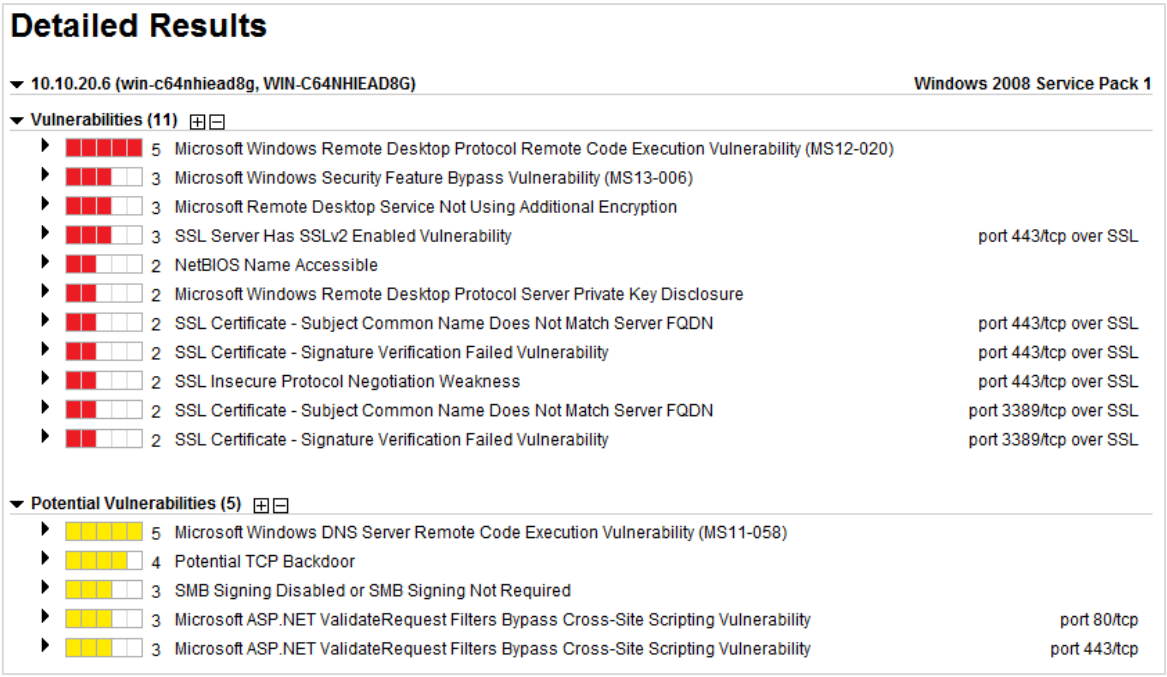


Figura. 5.5. Vulnerabilidades detectadas en el servidor Windows de la DMZ

En todas las vulnerabilidades se mostrará una descripción de la amenaza, el impacto, la solución, el cumplimiento (no aplicable), la explotabilidad, los códigos maliciosos asociados y el resultado para llegar a esa vulnerabilidad (ver Figura. 5.6.).

2 SSL Certificate - Signature Verification Failed Vulnerability — port 3389/tcp over SSL

QID:	38173	**CVSS Base:**	9.4[1]
Category:	General remote services	**CVSS Temporal:**	6.9
CVE ID:	-		
Vendor Reference	-		
Bugtraq ID:	-		
Service Modified:	05/22/2009		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=WIN-C64NHIEAD8G unable to get local issuer certificate

Figura. 5.6. Ejemplo de detalle de vulnerabilidad detectada en el servidor Windows de la DMZ

En este caso solo existen dos vulnerabilidades explotables, el resto son vulnerabilidades de configuración, antes las cuáles ningún elemento de seguridad es capaz de tomar acción por lo que la única remediación es corregirlas con las sugerencias entregadas en el reporte. Las dos vulnerabilidades explotables son las siguientes:

- Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- Microsoft Windows DNS Server Remote Code Execution Vulnerability (MS11-058)

La primera es confirmada y la segunda es potencial, para seguir con el test de penetración se debe proceder a explotar esas vulnerabilidades. Para la primera vulnerabilidad existen cuatro empresas que tienes exploits para explotarla (ver Figura. 5.7.) en cambio la segunda tiene solo una empresa (ver Figura. 5.8.).

Figura. 5.7. Exploits para Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability

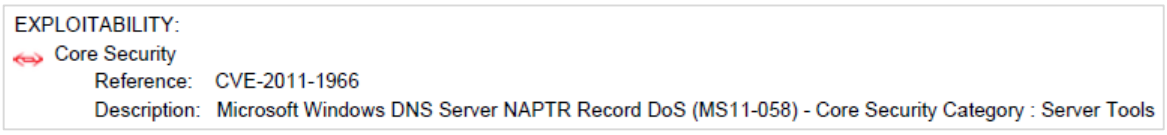


Figura. 5.8. Exploits para Microsoft Windows DNS Server Remote Code Execution Vulnerability

Para explotar la primera se va a utilizar el exploit desarrollado por metasploit, la cuál es la herramienta que viene incluida en la máquina virtual backtrack. Para este caso se va a utilizar el exploit /auxiliary/dos/Windows/rdp/ms12_020_maxchannelids, en este exploit se debe configurar el host a ser atacado y posteriormente ejecutrarlo (ver Figura. 5.9.).

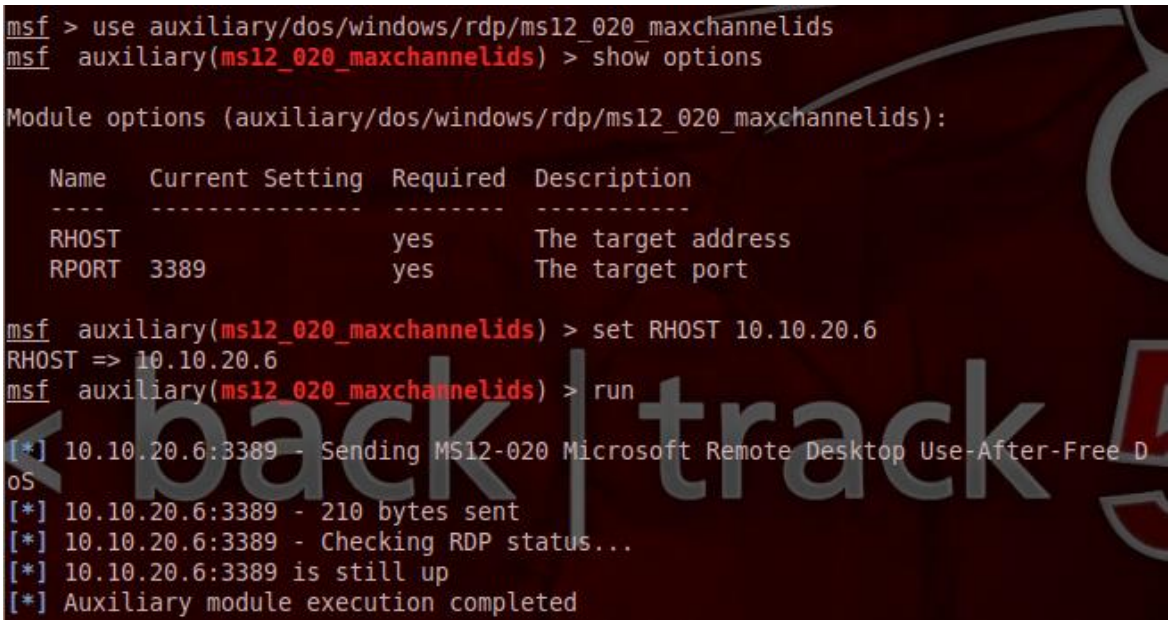


Figura. 5.9. Explotación de Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)

Una vez realizado el ataque de negación de servicio, se comprobó que el servidor no tuvo ningún efecto y posterior a la revisión de los logs, se pudo notar que el equipo de Palo Alto Networks había sido el responsable de bloquear dicho intento de ataque (ver Tabla. 5.10.)

Threat	ID	Severity	Action	Count
Microsoft Windows Remote Desktop Code Execution Vulnerability	34673	critical	drop-all-packets	1
Microsoft remote desktop connect initial attempt	33020	informational	Alert	1

Tabla. 5.2. Reporte de Palo Alto Networks indicando el bloque de intento de ataque al servidor Windows de la DMZ

Una vez detectado el bloqueo, dentro del baúl de amenazas de Palo Alto Networks también se pudo comprobar que el CVE de esta vulnerabilidad es reconocido (ver Figura. 5.10.).

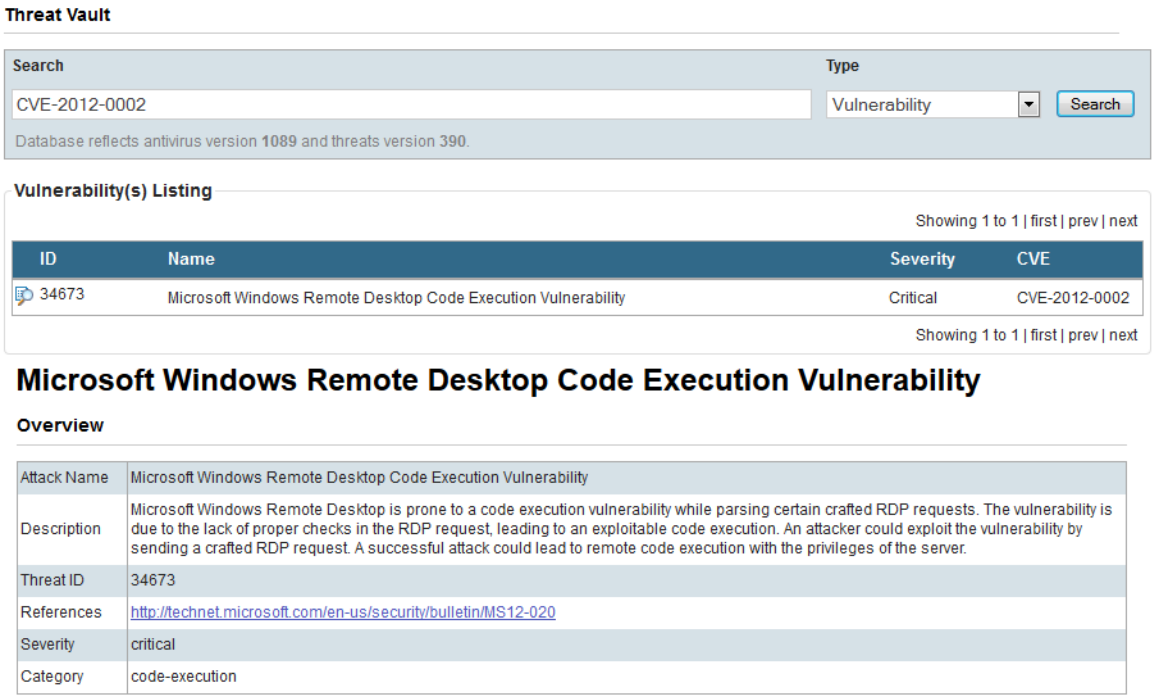


Figura. 5.10. CVE-2012-002 reconocido dentro del baúl de amenazas de Palo Alto Networks ([52] Palo Alto Networks, 2013)

La segunda vulnerabilidad únicamente es explotable con la herramienta Core Security, debido a que la misma es pagada, esta prueba no se va a poder realizar. Sin embargo se comprobó que dicho CVE si esté reconocido dentro del baúl de Palo Alto Networks (ver Figura. 5.11.).

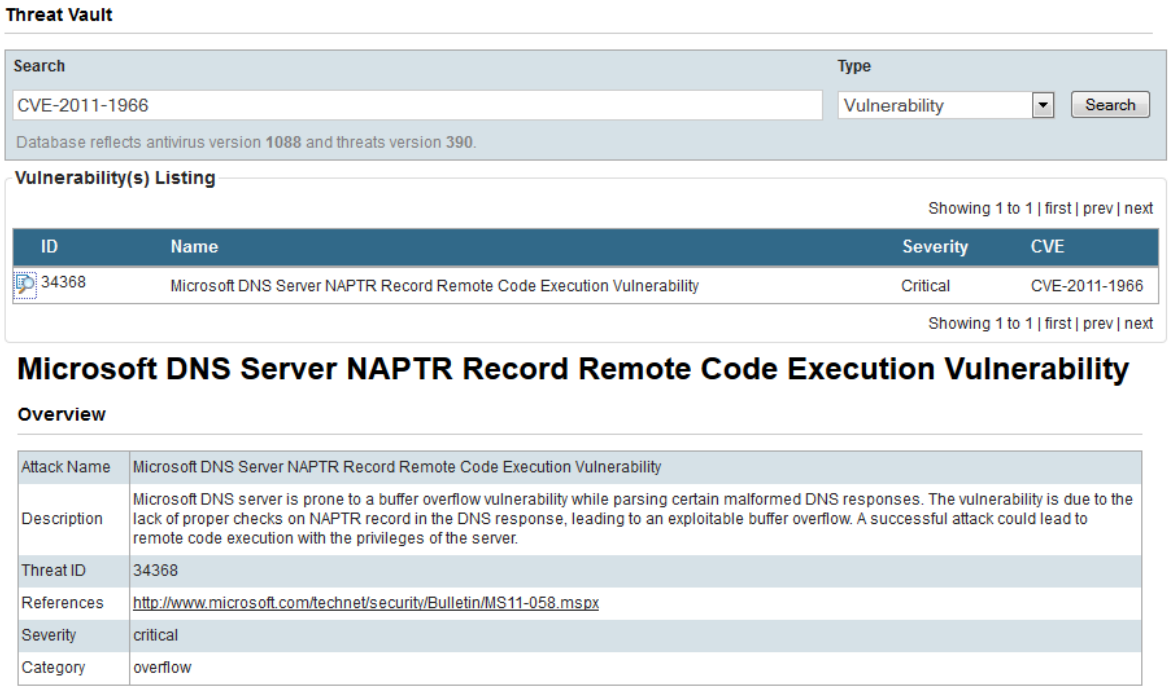


Figura. 5.11. CVE-2011-1996 reconocido dentro del baúl de amenazas de Palo Alto Networks ([52] Palo Alto Networks, 2013)

El segundo servidor a ser analizado es un CentOS 6.2. Una vez realizado el test de penetración, en la Tabla. 5.3. se muestra los resultados otorgados por el equipo de Palo Alto Networks durante los diferentes ataques, tomando una acción de bloqueo para los ataques de severidad mediana, alta y crítica, y de alerta para los ataques de severidad informacional y baja.

Threat	ID	Severity	Action	Count
HTTP Cross Site Scripting Vulnerability	35864	critical	drop-all-packets	1
phf CGI program remote command execution vulnerability	32790	critical	drop-all-packets	1
HTTP /etc/passwd Access Attempt	30852	high	drop-all-packets	3
Generic HTTP Cross Site Scripting Attempt	31476	high	drop-all-packets	2
Generic HTTP Cross Site Scripting Attempt	31477	high	drop-all-packets	2

Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	30921	high	drop-all-packets	1
Webhints Improper URI Sanitization Remote Command Execution Vulnerability	30101	high	drop-all-packets	1
FTP server in Solaris remote authorization bypass and information disclosure vulnerability	32789	high	drop-all-packets	1
Novell eDirectory MS-DOS Device Name Denial of Service	31020	high	drop-all-packets	1
AWStats Remote Code Execution Vulnerability	30089	high	drop-all-packets	1
HTTP /etc/passwd access attempt	35107	high	drop-all-packets	1
Google Search Appliance ProxyStyleSheet Cross-Site Scripting Vulnerability	30178	medium	drop-all-packets	1
Apache Tomcat Servlet Engine Directory Traversal	30873	medium	drop-all-packets	1
HTTP SQL Injection Attempt	30514	medium	drop-all-packets	1
Oracle 9i HTTP Server Globals.JSA File Access	33759	medium	drop-all-packets	1
HTTP SQL Injection Attempt	35826	medium	drop-all-packets	1
Hylafax Faxsurvey Remote Command Execution Vulnerability	30953	medium	drop-all-packets	1
HTTP SQL Injection Attempt	33338	medium	drop-all-packets	1

raSMP User-Agent Parsing Cross-Site Scripting Vulnerability	33468	medium	drop-all-packets	1
Apache SSI Error Page XSS Vulnerability	31910	medium	drop-all-packets	1
Apache HTTP Server Reverse Proxy Security Bypass Vulnerability	34485	medium	drop-all-packets	1
Snort URIContent Rules Detection Evasion Vulnerability	33334	low	alert	2
HTTP Cross Site Scripting Attempt	32658	low	alert	2
test-cgi remote file listing vulnerability	32792	low	alert	1
HTTP Directory Traversal Request Attempt	33194	low	alert	1
HTTP Apache 2.0 Path Disclosure Vulnerability	30818	low	alert	1
HTTP Directory Traversal Vulnerability	30844	low	alert	1
FTP Bounce Attack	33439	low	alert	1
Cart32 Expdate Information Disclosure Vulnerability	30918	low	alert	1
SSL Renegotiation Denial of Service Vulnerability	33862	low	alert	1
Microsoft Windows SMB Negotiate Request	35364	informational	alert	7
NetBIOS null sesión	31710	informational	alert	3
Windows SMB Login Attempt	31696	informational	alert	3
FTP Login Failed	40000	informational	alert	2
SSH2 Login Attempt	31914	informational	alert	1
HTTP TRACE Method	30510	informational	alert	1
Windows Local Security Architect Security Identifier Lookup	30843	informational	alert	1

Microsoft Windows PNP Service Access	30865	informational	alert	1
HTTP OPTIONS Method	30520	informational	alert	1
Microsoft Windows Server Service NetrShareEnum access	30862	informational	alert	1
Microsoft Windows user enumeration	30842	informational	alert	1
HTTP TRACK Method	30853	informational	alert	1
Windows Local Security Architect LsarQueryInformationPolicy	30858	informational	alert	1

Tabla. 5.3. Reporte de Palo Alto Networks en el test de penetración al CentOS servidor de la DMZ

Posteriormente se procederá a analizar el reporte entregado por Qualys que permitirá visualizar todo lo que un atacante podría hacerlo, pese a tener el equipo de Palo Alto Networks de por medio.

Dentro del reporte entregado por la herramienta, se han encontrado once vulnerabilidades confirmadas y 5 potenciales (ver Figura. 5.12.).

Summary of Vulnerabilities

Vulnerabilities Total	79

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	2	0	0	2
3	5	14	4	23
2	10	2	9	21
1	3	0	30	33
Total	20	16	43	79

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Web server	5	8	5	18
General remote services	6	4	7	17
Information gathering	1	0	14	15
CGI	2	2	4	8
TCP/IP	1	0	6	7
Category	Confirmed	Potential	Information Gathered	Total
Total	15	14	36	65

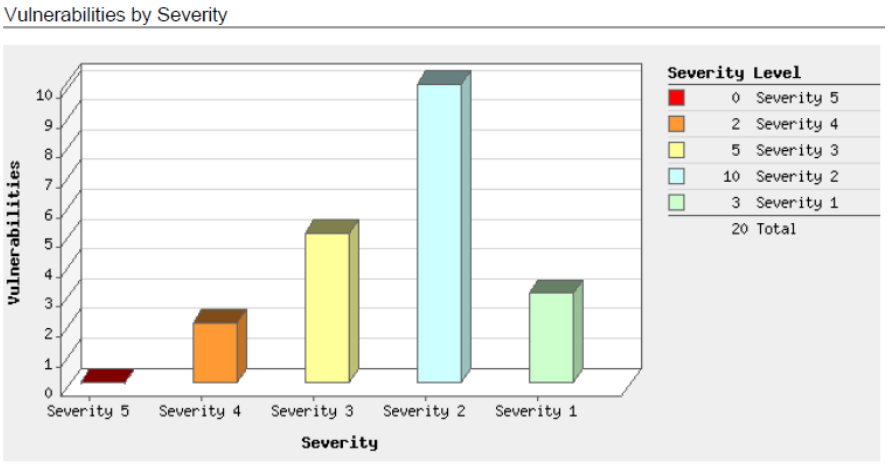
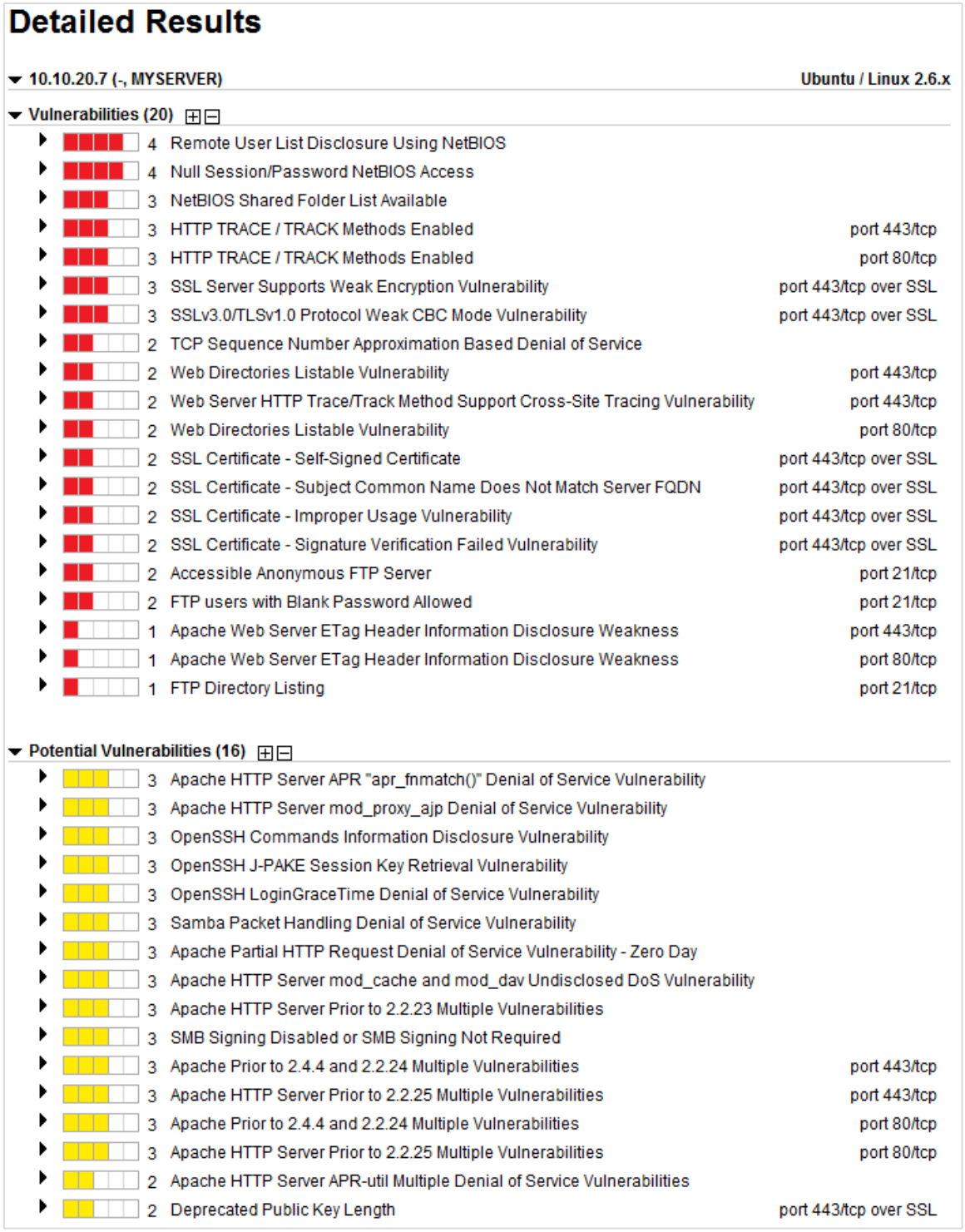


Figura. 5.12. Resumen de vulnerabilidades del servidor CentoOS de la DMZ

Posteriormente se visualizará la información de sistema operativo y servicios que se encontraros activos en el servidor (ver Figura. 5.13.).

Figura. 5.13. Sistema operativo y servicios detectados en el servidor CentOS de la DMZ

Las vulnerabilidades que dejó visualizar el equipo de Palo Alto Networks se pueden ver en la Figura 5.14.:



Detailed Results

10.10.20.7 (-, MYSERVER) — **Ubuntu / Linux 2.6.x**

Vulnerabilities (20)

4	Remote User List Disclosure Using NetBIOS	
4	Null Session/Password NetBIOS Access	
3	NetBIOS Shared Folder List Available	
3	HTTP TRACE / TRACK Methods Enabled	port 443/tcp
3	HTTP TRACE / TRACK Methods Enabled	port 80/tcp
3	SSL Server Supports Weak Encryption Vulnerability	port 443/tcp over SSL
3	SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability	port 443/tcp over SSL
2	TCP Sequence Number Approximation Based Denial of Service	
2	Web Directories Listable Vulnerability	port 443/tcp
2	Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability	port 443/tcp
2	Web Directories Listable Vulnerability	port 80/tcp
2	SSL Certificate - Self-Signed Certificate	port 443/tcp over SSL
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 443/tcp over SSL
2	SSL Certificate - Improper Usage Vulnerability	port 443/tcp over SSL
2	SSL Certificate - Signature Verification Failed Vulnerability	port 443/tcp over SSL
2	Accessible Anonymous FTP Server	port 21/tcp
2	FTP users with Blank Password Allowed	port 21/tcp
1	Apache Web Server ETag Header Information Disclosure Weakness	port 443/tcp
1	Apache Web Server ETag Header Information Disclosure Weakness	port 80/tcp
1	FTP Directory Listing	port 21/tcp

Potential Vulnerabilities (16)

3	Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability	
3	Apache HTTP Server mod_proxy_ajp Denial of Service Vulnerability	
3	OpenSSH Commands Information Disclosure Vulnerability	
3	OpenSSH J-PAKE Session Key Retrieval Vulnerability	
3	OpenSSH LoginGraceTime Denial of Service Vulnerability	
3	Samba Packet Handling Denial of Service Vulnerability	
3	Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day	
3	Apache HTTP Server mod_cache and mod_dav Undisclosed DoS Vulnerability	
3	Apache HTTP Server Prior to 2.2.23 Multiple Vulnerabilities	
3	SMB Signing Disabled or SMB Signing Not Required	
3	Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities	port 443/tcp
3	Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities	port 443/tcp
3	Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities	port 80/tcp
3	Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities	port 80/tcp
2	Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities	
2	Deprecated Public Key Length	port 443/tcp over SSL

Figura. 5.14. Vulnerabilidades detectadas en el servidor CentOS de la DMZ

En este caso no existen vulnerabilidades explotables, todas son vulnerabilidades de configuración, antes las cuáles ningún elemento de seguridad es capaz de tomar acción por lo que la única remediación es corregirlas con las sugerencias entregadas en el reporte.

Finalmente el honeypot va a simular ser un servidor totalmente explotable para poder capturar al atacante mediante su comportamiento. Y simplemente lo que hará el es registrar todas las acciones que intenta hacer contra los diferentes servicios simulados existentes (ver Figura. 5.15.).

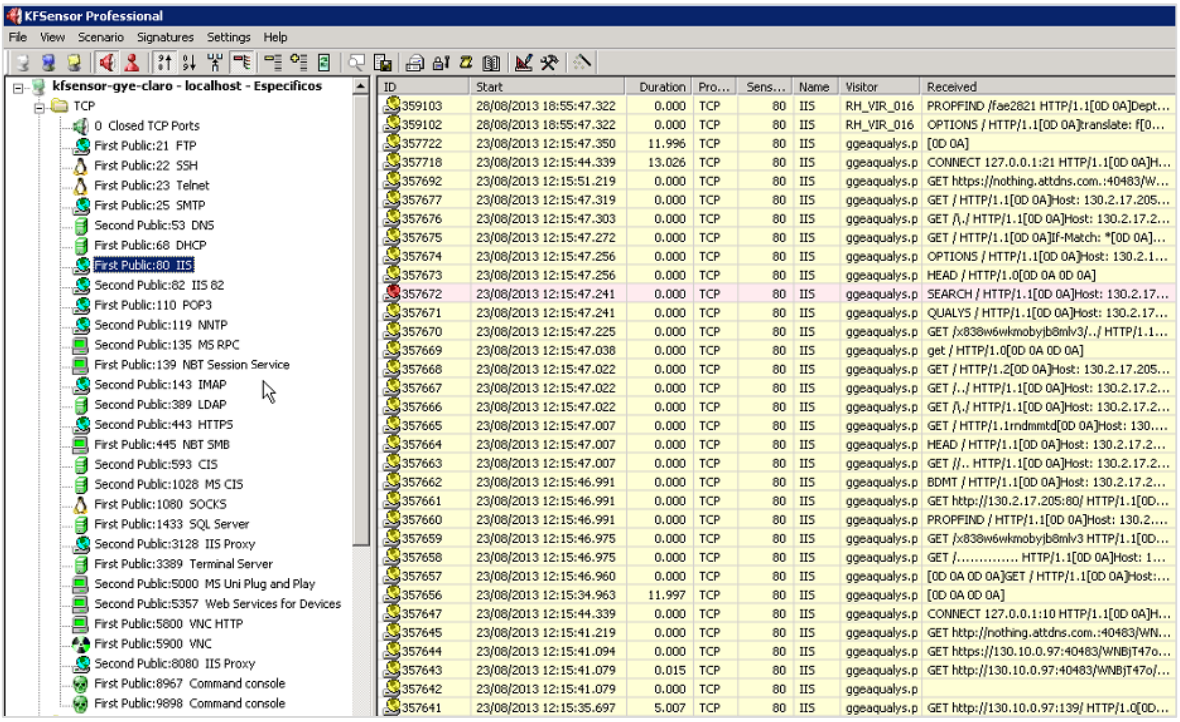


Figura. 5.15. Eventos registrados por KFSensor posterior al ataque con Qualys

5.2.2. Test de penetración desde una de las sedes simuladas a una aplicación WEB

En la presente prueba se evaluará las siguientes herramientas:

- Palo Alto Networks
- ModSecurity

El objetivo planteado en esta sección es realizar la instalación de Owasp Broken Web Applications, la cual es una máquina virtual, que tiene cierta cantidad de aplicaciones las mismas que pueden ser utilizadas para realizar pruebas de seguridad (ver Figura. 5.16), esta máquina tiene serios problemas de seguridad y esta diseña para ser utilizada con fines netamente educativos. ([53] OWASP, 2012)

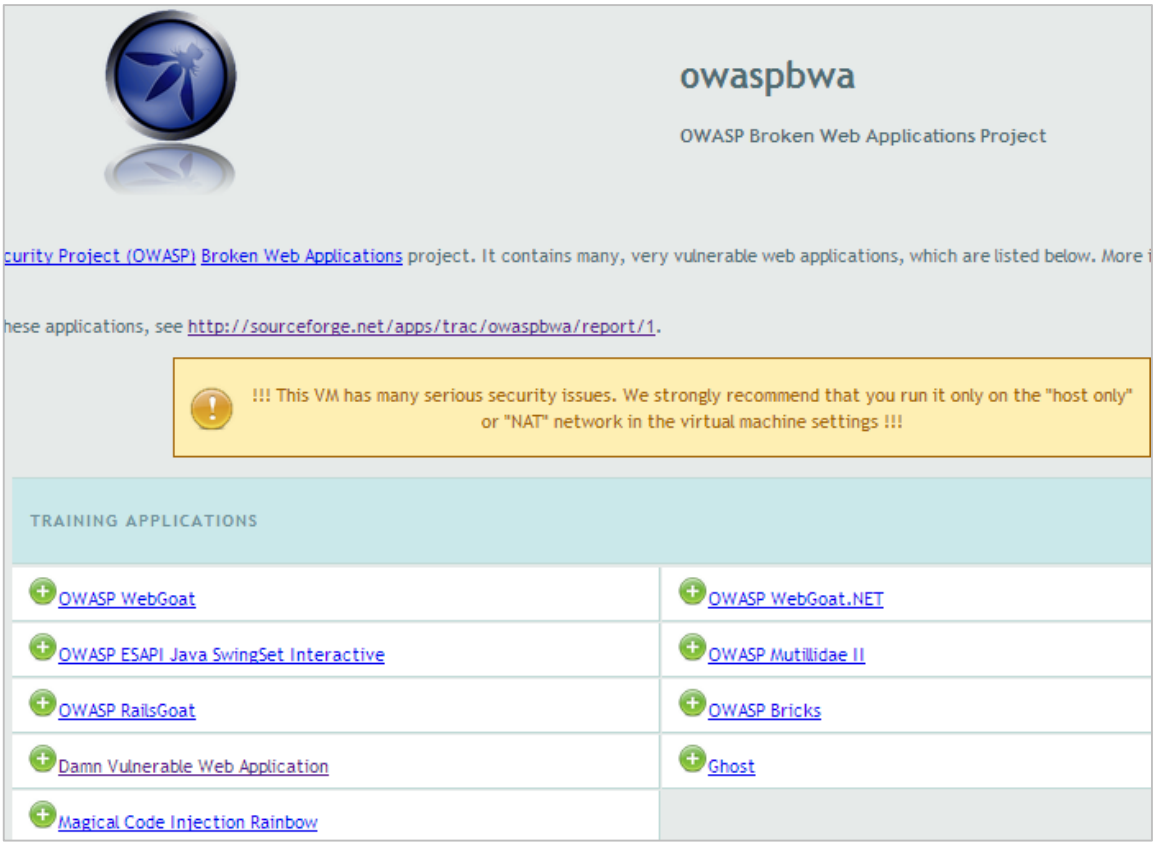


Figura. 5.16. OWASP Broken Web Application

En estas pruebas se utilizará la aplicación web DVWA (Damn Vulnerable Web Application), que se caracteriza por ser intencionalmente vulnerable. Su principal objetivo es poder ayudar a desarrolladores o profesionales en seguridad a realizar ataques contra este servidor web o puede ser utilizado para realizar pruebas de protección con diversas herramientas pero de manera legal, en un ambiente totalmente controlado.

Para ingresar a DVWA se utilizan el usuario admin y el password admin (ver Figura. 5.17.), se observa que son credenciales poco seguras ya que son de las primeras opciones que puede utilizar un atacante para ingresar.

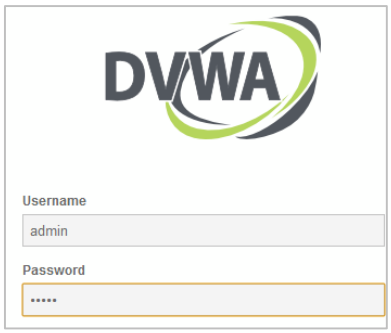


Figura. 5.17. Credenciales DVWA

Posteriormente se procederá a la explotación de DVWA

SQL Injection

Se observa como los campos son explotables, ya que al probar una inyección, el resultado es una consulta donde se muestran todos los usuarios de la base de datos (ver Figura. 5.18.).

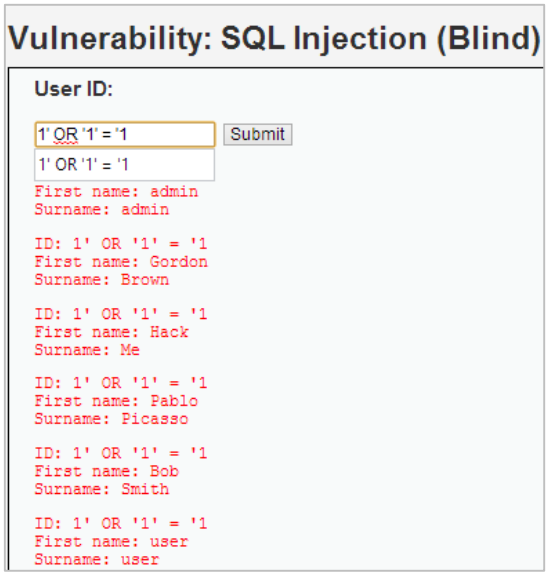


Figura. 5.18. Usuarios Base de Datos de DVWA

Puede suceder que al explotar el campo no se entregue el valor de Surname, sino que el valor entregado será el md5 (Ver Figura. 5.19.).

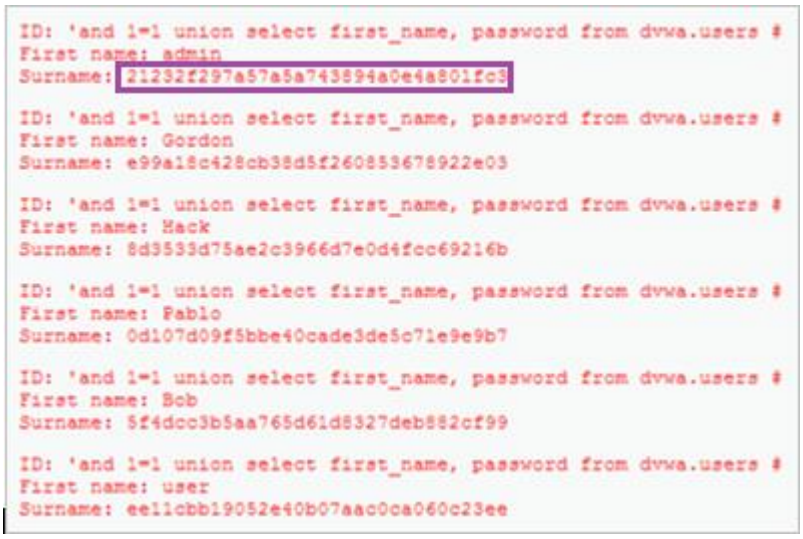


Figura 5. 19 md5 de Contraseñas DVWA

Existen herramientas como Reverse Hash Calculator (ver Figura. 5.20.) que nos podrán mostrar el valor del md5, en este caso se ingresará el Surname del usuario admin para obtener así la contraseña.

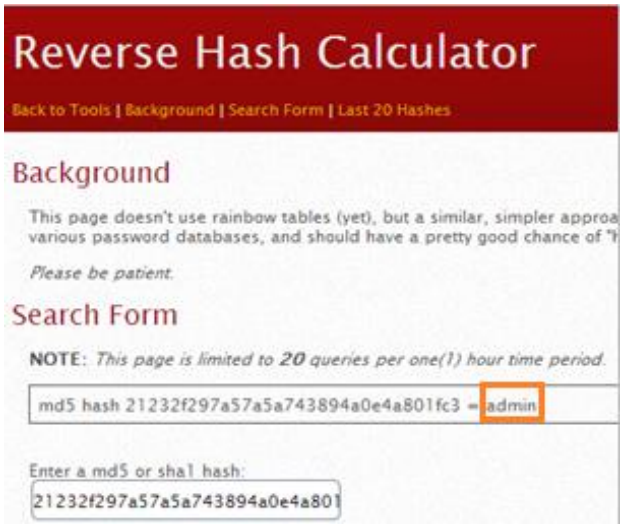


Figura. 5.20. Reverse Hash Calculator ([54] SANS Technology Institute, 2013)

A continuación se muestra como se intentó hacer nuevamente un ataque de SQL Injection (ver Figura. 5.21.) y este ataque fue detenido por ModSecurity (ver Figura. 5.22).

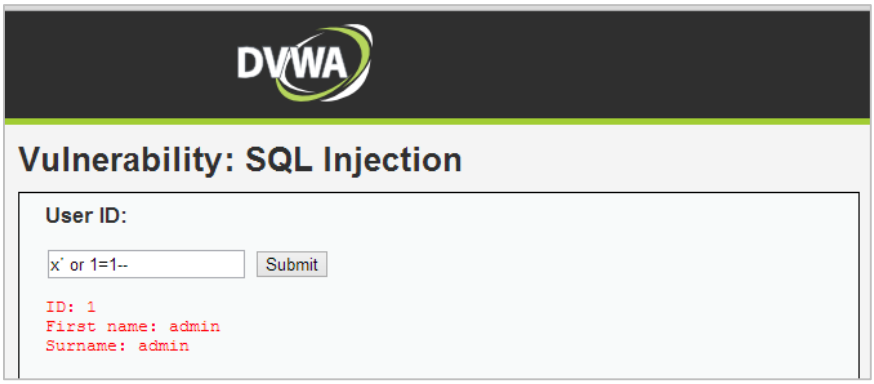


Figura. 5.21. Ataque SQL Injection

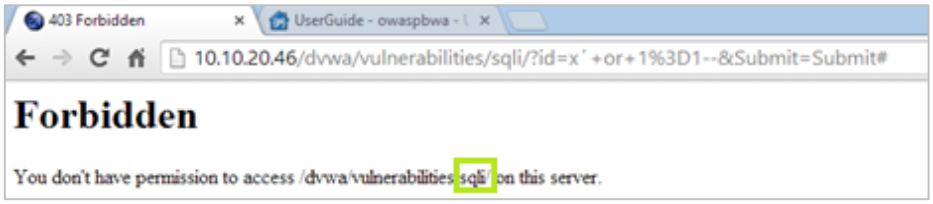


Figura. 5.22. Bloqueo de ModSecurity a ataque SQL Injection

De igual manera al realizar un ataque con SQL Injection (Blind) (ver Figura. 5.23.) también será detenido por el WAS ModSecurity (ver Figur.a 5.24.).

Figura. 5.23. Ataque SQL Injection Blind

Figura. 5.24. Bloqueo de ModSecurity a ataque SQL Injection Blind

Al ingresar a los log de ModSecurity se podrá observar la hora, fecha, tipo de ataque y regla que impidió realizar el ataque, en este caso se mostrarán los ataques

de SQL Injection que intentaron ejecutarse (ver Figura. 5.24.), y ModSecurity al estar en modo de bloqueo impidió que se ejecutaran.

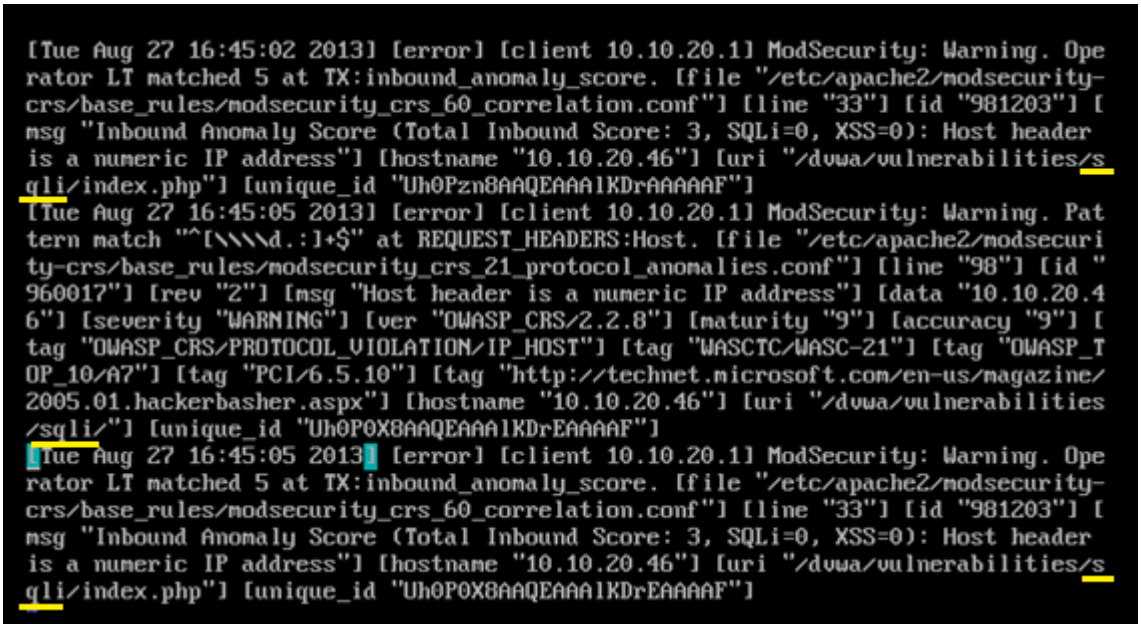


Figura. 5.25. Logs de ModSecurity a ataque SQL Injection

Cross Site Scripting (XSS)

Este tipo de vulnerabilidad consiste en ejecutar código HTML o Javascript, esto puede ocasionar que se cambie completamente la interfaz del sitio web atacado al ejecutar scripts maliciosos perjudicando a los usuarios que ingresen.

Existen 2 formas de ejecutar XSS, la primera es cuando el código ejecutado es almacenado en una base de datos (ver Figura. 5.26.) de manera que cuando se realice una consulta en la base de datos el código se ejecutará (ver Figura. 5.27.), la otra forma en que se realiza XSS es de manera reflejada, es decir todo lo que ingresa el usuario se mostrará en la pantalla (ver Figura. 5.28).

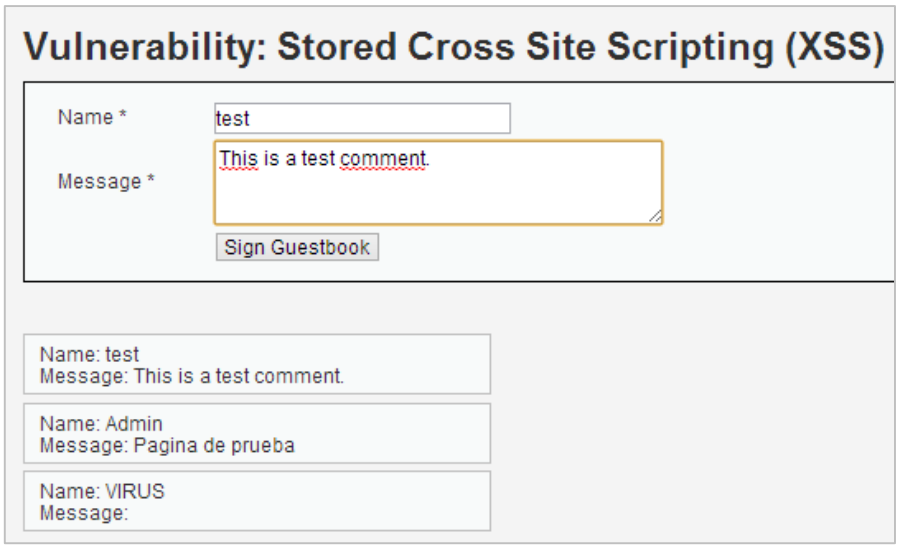


Figura. 5.26. Vulnerabilidad de Cross Site Scripting Almacenada

Figura. 5.27. Ejecución de Vulnerabilidad de Cross Site Scripting Almacenada

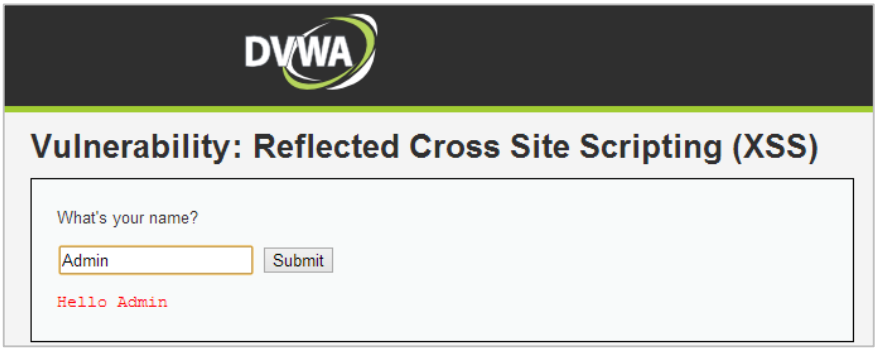


Figura. 5.28. Vulnerabilidad de Cross Site Scripting Reflejada

Con XSS Reflected al ingresar un código se podrá mostrar lo que el usuario desee (ver Figura. 5.29.), pueden ser imágenes o una URL que redireccione hacia otro sitio web, los cuales son comúnmente sitios de malware que buscan realizar descargas de virus o contaminar al equipo visitante.

Figura. 5.29. Ejecución de Vulnerabilidad de Cross Site Scripting Reflejada

Al activar las reglas de ModSecurity, se despliega un pop-up al tratar de explotar las vulnerabilidades de DVWA, en ModSecurity existen reglas de bloqueo para XSS reflejado (ver Figura. 5.30.) y para XSS Almacenado (ver Figura. 5.31.).

Figura. 5.30. Bloqueo de ModSecurity a ataque XSS Reflejado

Figura. 5.31. Bloqueo de ModSecurity a ataque XSS Almacenado

En los logs de ModSecurity se observa como el WAS bloqueó tanto XSS Reflejado como XSS Almacenado (ver Figura. 5.32.).

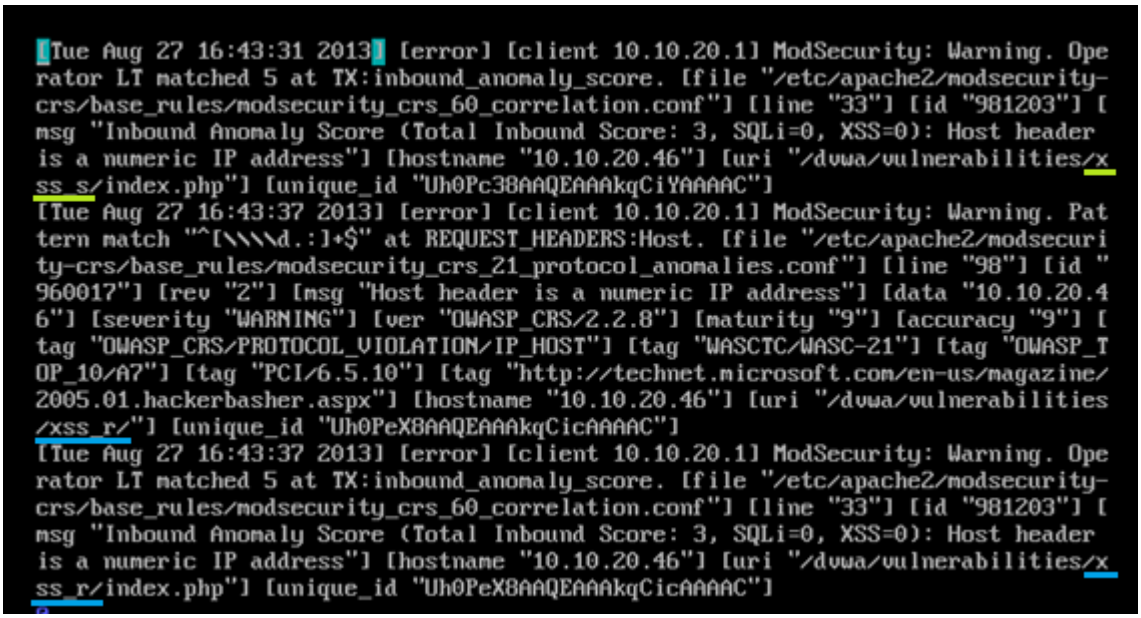


Figura. 5.32. Logs de ModSecurity a ataque XSS Reflejado

Command Excecution

Con esta vulnerabilidad es posible ejecutar comandos de consola desde el sitio web, permitiendo que el usuario que la explote pueda ver, modificar o eliminar archivos del servidor, en este caso se observará el código fuente (ver Figura. 5.33.) en donde se indicará que el sitio tiene la vulnerabilidad Command Execution, además de no tener ningún tipo de filtro para evitar que se ingresen símbolos como comillas.

```
<div class="body_padded">
	<h1>Vulnerability: Command Execution</h1>

	<div class="vulnerable_code_area">

		<h2>Ping for FREE</h2>

		<p>Enter an IP address below:</p>
		<form name="ping" action="#" method="post">
			<input type="text" name="ip" size="30">
			<input type="submit" value="submit" name="submit">
		</form>

		<pre>PING 10.10.10.45 (10.10.10.45) 56(84) bytes of data.
64 bytes from 10.10.10.45: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from 10.10.10.45: icmp_seq=2 ttl=64 time=0.014 ms
64 bytes from 10.10.10.45: icmp_seq=3 ttl=64 time=0.022 ms

--- 10.10.10.45 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.014/0.020/0.024/0.004 ms
</pre>
```

Figura. 5.33. Código Fuente DVWA

Una vez que se ha observado la existencia de esta vulnerabilidad se procede a obtener información del sistema (ver Figura. 5.34.), en este caso nos indica que es un servidor de 64 bits.

Figura. 5.34. Arquitectura del sistema DVWA

Una vez cargadas las reglas de ModSecurity, no se permitirá ejecutar ningún código malicioso hacia el servidor (ver Figura. 5.35.), así mismo se mostrarán los logs de error enviados por ModSecurity (ver Figura. 5.36.).

Figura. 5.35. Bloqueo de ModSecurity a ataque de Ejecución de Código

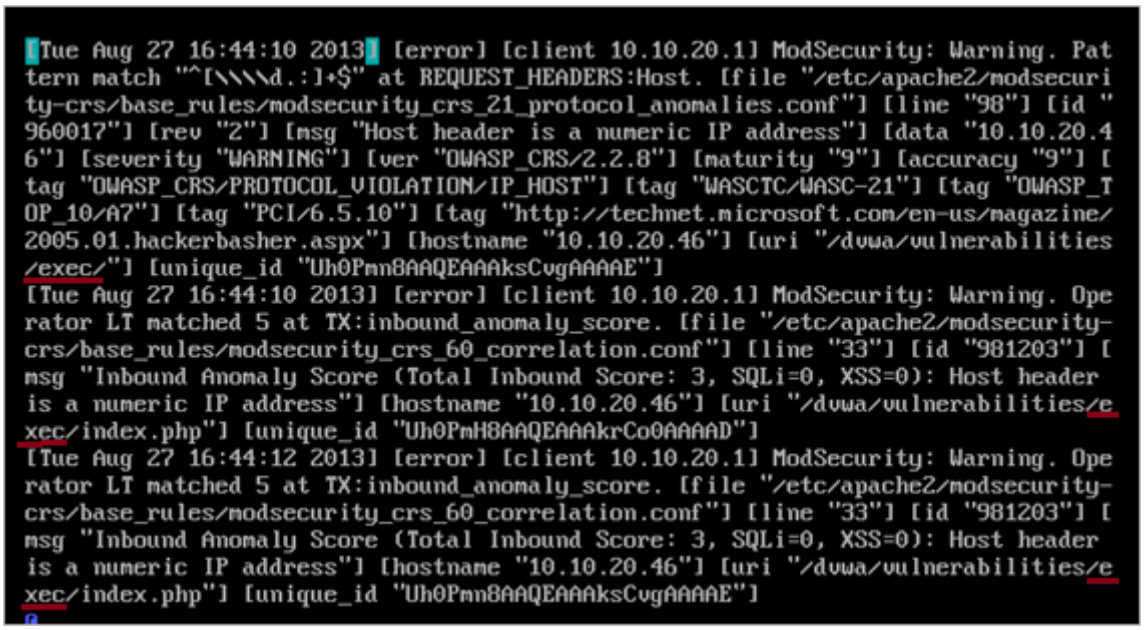


Figura. 5.36. Logs de ModSecurity a ataque de Ejecución de Código

Brute Force

Existen gran cantidad de herramientas para realizar ataques de fuerza bruta, en esta ocasión se usará el complemento de Firefox llamado FireForce. ([55] Mozilla, 2013)

El primer paso es crear un archivo de texto el cual se llamará passq.txt en el cual se colocará una serie de passwords para que FireForce realice la búsqueda respectiva, a continuación se cargará un diccionario (ver Figura. 5.37.), en caso contrario se indicará cual fue el password encontrado (ver Figura. 5.38.).

Figura. 5.37. Vulnerabilidad de Fuerza Bruta

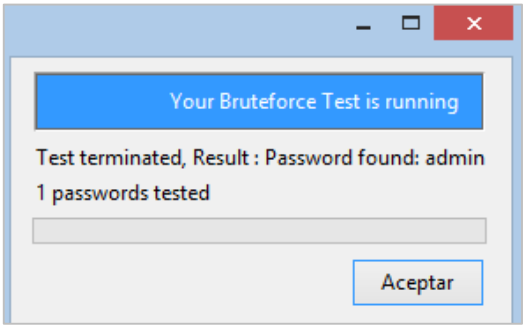


Figura. 5.38. Diccionario encontrado con FireForce

Al observar los logs de ModSecurity se ve que ha existido un ataque de fuerza bruta (ver Figura. 5.39.)

Figura. 5.39. Logs de ModSecurity a ataque de Fuerza Bruta

Análisis con Qualys:

Se realizó un primer escaneo con Qualys hacia el servidor web por medio de la herramienta WAS de Qualys (Web Application Scanning). Este primer escaneo se lo realizó, antes de cargar las reglas de ModSecurity, se puede observar (ver Figura. 5.40.) que existen tres vulnerabilidades de Cross Site Scripting y una de SQL Injection, además de vulnerabilidades de Path las cuales son básicamente son vulnerabilidades en la configuración del sitio web.

Summary of Vulnerabilities

Group Name	Severity 5	4	3	2	1	Total
XSS	3	0	0	0	0	3
SQL	1	0	0	0	0	1
PATH	0	0	0	11	0	11
INFO	3	0	3	2	10	18
Total	7	0	3	13	10	33

Figura. 5.40. Vulnerabilidades halladas con WAS de Qualys y ModSecurity sin reglas cargadas

Ninguna de las vulnerabilidades encontradas son explotables (ver Figura. 5.41.)

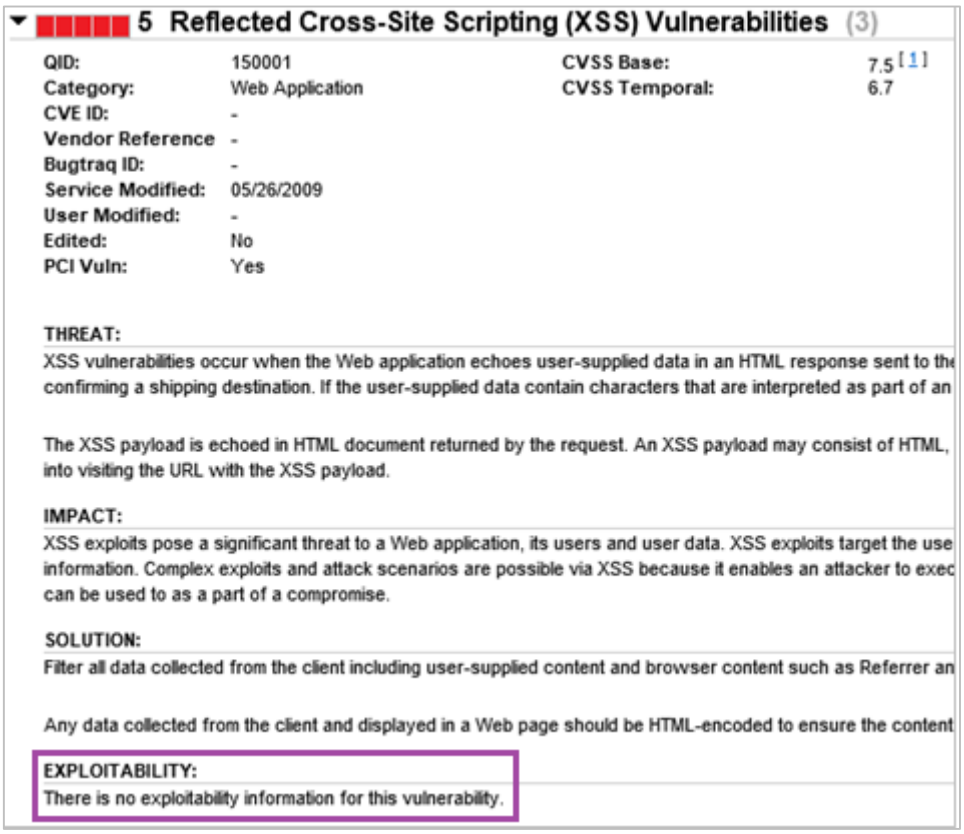


Figura. 5.41. Vulnerabilidades no explotables

Al realizar un segundo escaneo con las reglas de ModSecurity activas, se observa como ModSecurity bloqueo las vulnerabilidades de XSS y SQL Injection (ver Figura. 5.42.), debido a que estas son parte de las reglas activas de OWASP que fueron cargadas a ModSecurity para su funcionamiento.

Summary of Vulnerabilities

Group Name	Severity 5	4	3	2	1	
XSS	0	0	0	0	0	0
SQL	0	0	0	0	0	0
PATH	0	0	0	4	0	4
INFO	0	0	1	4	12	17
Total	0	0	1	8	12	21

Figura. 5.42. Vulnerabilidades halladas con WAS de Qualys y ModSecurity con reglas cargadas

El Firewall de Nueva Generación de Palo Alto Networks trabajando en modo IPS detectó que existió un intento de intrusión (ver Tabla. 5.4.), se observa que solo detectó un tipo de escaneo de XSS mientras que dejó pasar el resto de ataques, debido a que el IPS trabaja en capa 3 a diferencia del Web Aplication Firewall el cual trabaja en la capa de aplicación, detectando así las vulnerabilidades que se le escaparon a Palo Alto.

Threat	ID	Severity	Action	Count
Apache Wicket Unspecified XSS Vulnerability	36041	critical	drop-all-packets	7
HTTP Directory Traversal Vulnerability	30844	low	Alert	182
HTTP Unauthorized Error	34556	informational	Alert	4
HTTP WWW-Authentication Failed	31708	informational	Alert	4

Tabla. 5.4. Firewall de Palo Alto en modo IPS

5.2.3. Descarga de diferentes tipos de archivos maliciosos conocidos

En la presente prueba se evaluará las siguientes herramientas:

- Palo Alto Networks
- Kaspersky

Para esta prueba se va a descargar dos diferentes archivos maliciosos nuevos pero conocidos del sitio http://www.malwaredomainlist.com para comprobar el bloqueo inmediato de Palo Alto Networks y estos archivos se los va a tranferir a través de un dispositivo extraíble para comprobar el bloqueo inmediato de kaspersky.

Los dos archivos utilizados serán los siguientes:

- Trojan.FakePutt - http://update-critical.com/firefox/FirefoxUpdate.exe
- Trojan.Ransom.PA - http://cincyty.com/chrome/ChromeUpdate.exe

La respuesta de Palo Alto Networks ante el intento de descarga de los archivos fue de bloqueo inmediato (ver Figura. 5.43.).

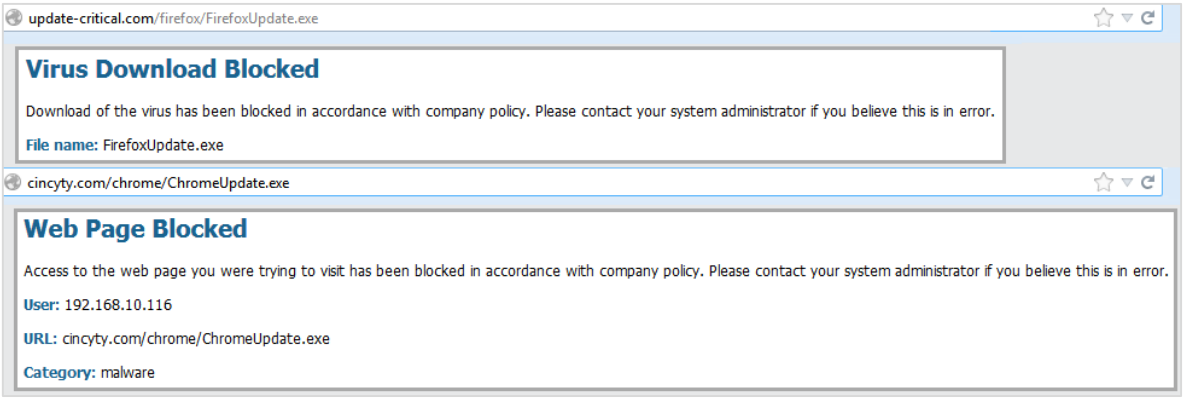


Figura 5. 43 Ataques conocidos bloqueados por Palo Alto Networks

La respuesta de Kaspersky al conectar el dispositivo extraíble con los archivos maliciosos fue de bloqueo y remediación inmediata (ver Figura. 5.44.).

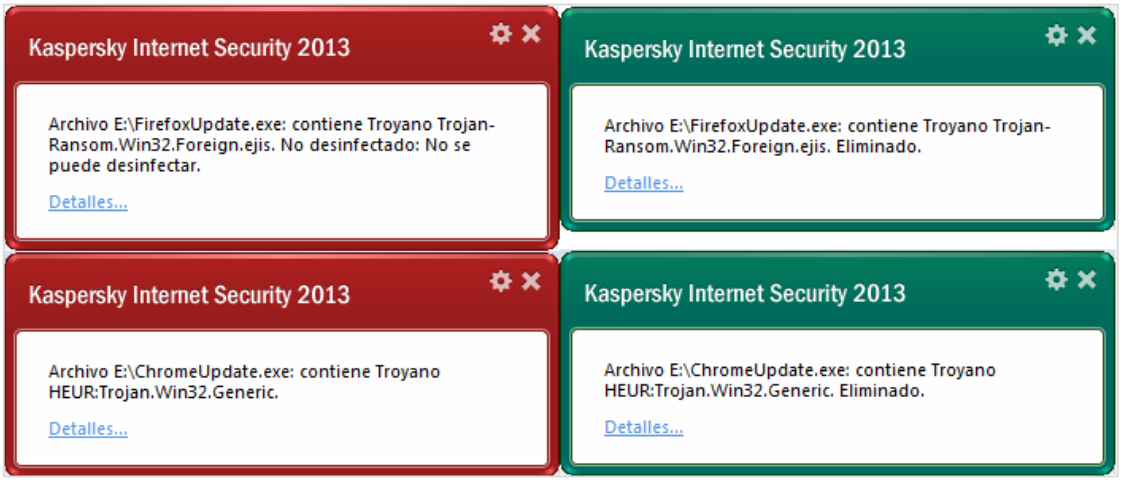


Figura. 5.44. Ataques conocidos bloqueados por Kaspersky

5.2.4. Descarga de un archivo malicioso de día cero

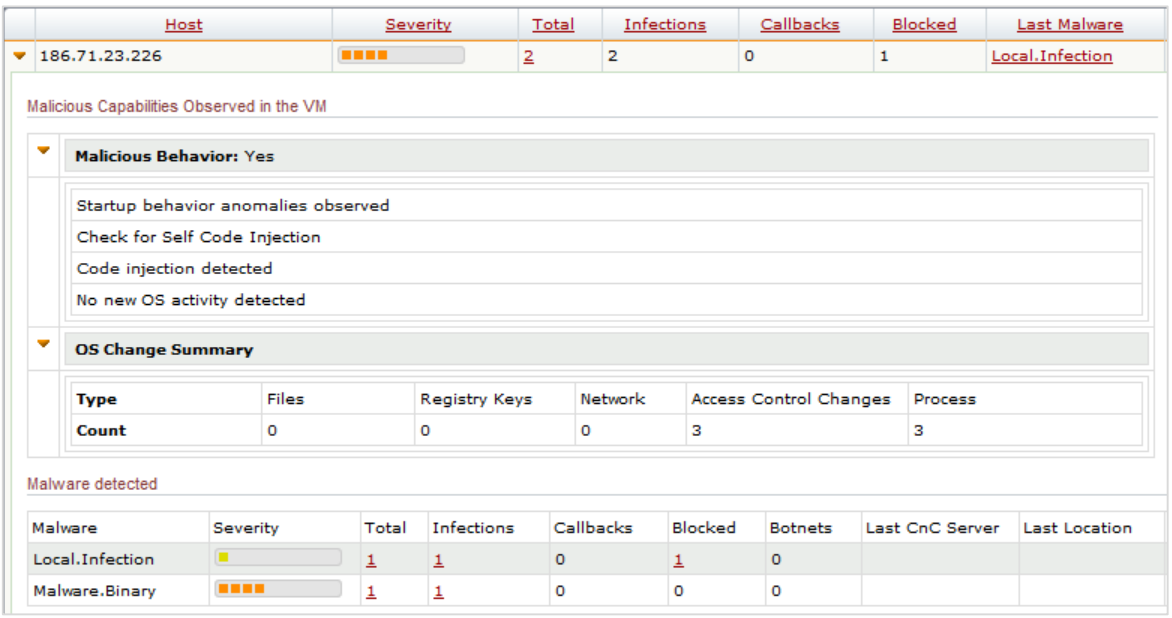
En la presente prueba se evaluará las siguientes herramientas:

- FireEye
- Wildfire de Palo Alto Networks

Cualquier herramienta que sea basada en firmas, será totalmente inútil al tratar de detectar un ataque de día cero. Para descargarse ataques de día cero hay como descargarse de diferentes sitios web actualizados instantáneamente o crear uno con diferentes herramientas disponibles en el mercado.

En este caso se procedió a investigar en la web un archivo malicioso para descargar que no sea bloqueado en primera instancia por Palo Alto Networks ni por Kaspersky y que tampoco sea detectado por Snort.

Posterior a la descarga se pudo visualizar que FireEye confirmó que este archivo era malicioso enviándole al mismo a sus métodos de detección basados en máquinas virtuales. FireEye le denominó a este evento como Malware.Binary. Este evento representa la detección de uno o más archivos binarios que están siendo transferidos y detectados por el equipo de FireEye como maliciosos. El comportamiento malicioso se determina observando cambios sospechosos en el sistema operativo. El evento sugiere que la fuente original del tráfico subyacente podría estar infectado con posterioridad a la descarga y ejecución de un binario malicioso (ver Figura. 5.45.).



Host	Severity	Total	Infections	Callbacks	Blocked	Last Malware
186.71.23.226		2	2	0	1	Local.Infection

Malicious Capabilities Observed in the VM

Malicious Behavior: Yes

- Startup behavior anomalies observed
- Check for Self Code Injection
- Code injection detected
- No new OS activity detected

OS Change Summary

Type	Files	Registry Keys	Network	Access Control Changes	Process
Count	0	0	0	3	3

Malware detected

Malware	Severity	Total	Infections	Callbacks	Blocked	Botnets	Last CnC Server	Last Location
Local.Infection		1	1	0	1	0		
Malware.Binary		1	1	0	0	0		

Figura. 5.45. Ataque de día cero detectado por FireEye

En el reporte entregado por FireEye se puede observar el comportamiento anómalo por el cual se difinió el archivo como malicioso e incluso es posible realizar la descarga del binario malicioso (ver Figura. 5.46.) para analizarlo internamente o subirlo a sitios como www.virustotal.com para determinar que antivirus ya reconocieron el archivo como malicioso.

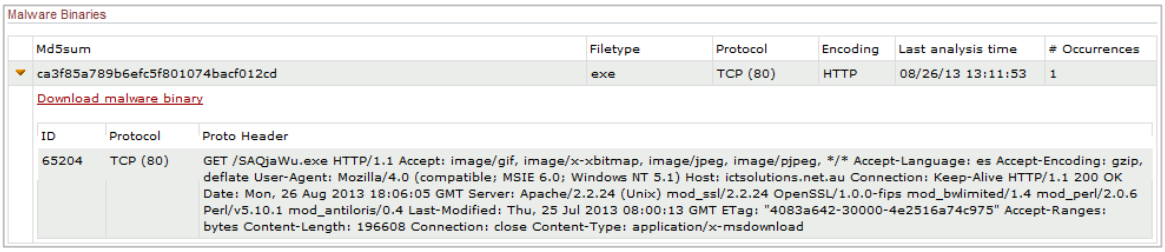


Figura. 5.46. Binario malicioso detectado por FireEye

El otro elemento que se posee herramientas para detectar ataques de día cero es el sandbox de Palo Alto Networks llamado Wildfire. Revisando el portal del mismo detectó también el archivo como malicioso, indicando de igual manera el comportamiento anómalo (ver Figura. 5.47.).

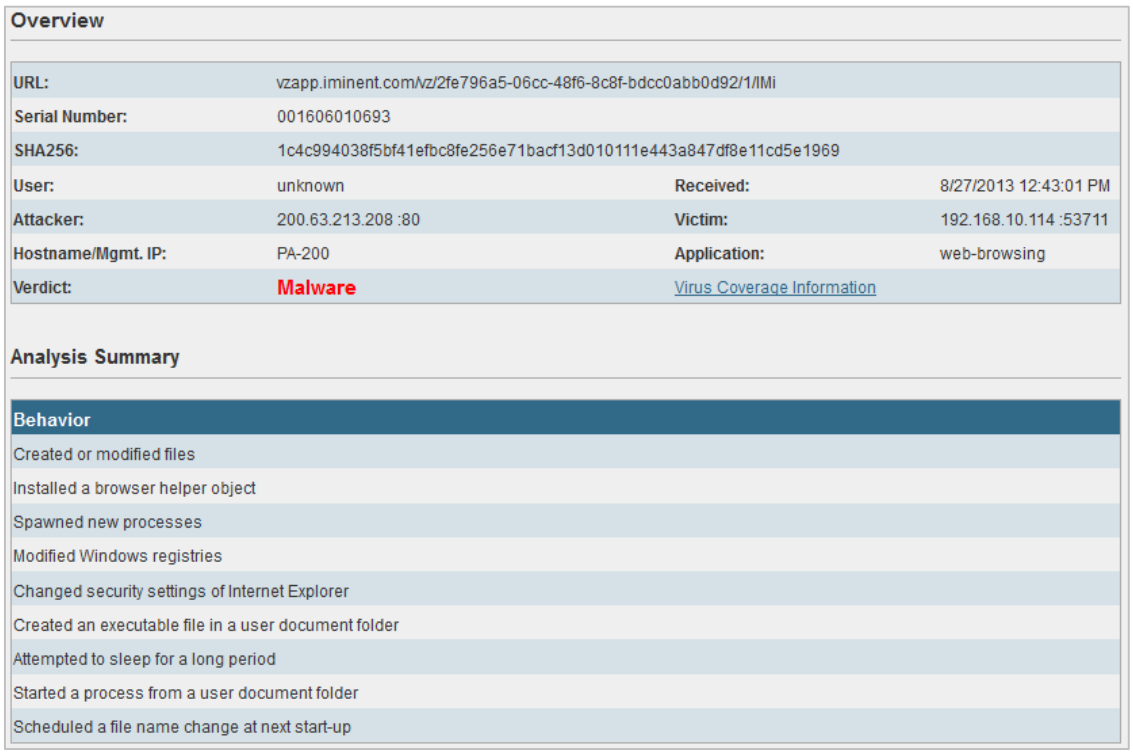
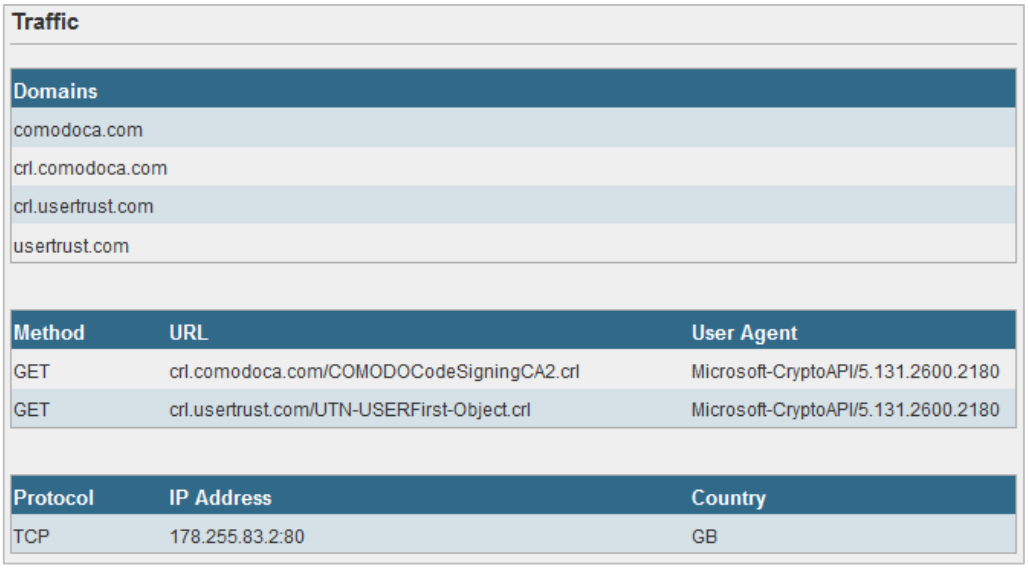


Figura. 5.47. Comportamiento de ataque de día cero detectado por WildFire

Además del comportamiento, el reporte permite visualizar las características del tráfico (ver Figura. 5.48.) y los eventos detallados a nivel de registros, procesos y archivos.



Traffic

Domains
comodoca.com
crl.comodoca.com
crl.usertrust.com
usertrust.com

Method	URL	User Agent
GET	crl.comodoca.com/COMODOCodeSigningCA2.crl	Microsoft-CryptoAPI/5.131.2600.2180
GET	crl.usertrust.com/UTN-USERFirst-Object.crl	Microsoft-CryptoAPI/5.131.2600.2180

Protocol	IP Address	Country
TCP	178.255.83.2:80	GB

Figura. 5.48. Detalle de tráfico de ataque de día cero detectado por Wildfire

5.2.5. Infección de un host para análisis de comportamiento con los sensores

En la presente prueba se evaluará las siguientes herramientas:

- Snort
- BotHunter

El objetivo de esta prueba es infectar un host para observar el valor agregado que pueden proveer snort y bothunter para detectar comportamientos específicos.

En este caso se tomó el host 192.168.10.82 y se lo infectó con variedades de troyanos. Snort se caracteriza por generar una gran cantidad de falsos negativos, pero debido a la gran cantidad de firmas que tiene es capaz de proveer información valiosa para una investigación forense. En este caso se realizó una petición a la base de datos para observar las alertas generadas posteriores a la infección.

En este caso Snort dio información de descarga de ejecutables de diferentes direcciones IP, tráfico detectado de SPAN, un agente de usuario sospechoso instalado y tráfico a un servidor de comando y control (ver Figura. 5.49.).

```
mysql> SELECT COUNT(*) AS ip_cnt, INET_NTOA(ip_src), INET_NTOA(ip_dst), sig_name FROM events_with_join WHERE INET_NTOA(ip_src)="192.168
.10.82" OR INET_NTOA(ip_dst)="192.168.10.82" GROUP BY sig_name ORDER BY ip_cnt DESC;
+--------+------------------+-----------------+-----------------------------------------------------------------------------------+
| ip_cnt | INET_NTOA(ip_src) | INET_NTOA(ip_dst) | sig_name                                                                          |
+--------+------------------+-----------------+-----------------------------------------------------------------------------------+
|    103 | 62.76.189.216     | 192.168.10.82     | ET POLICY PE EXE or DLL Windows file download                                     |
|     48 | 62.76.189.216     | 192.168.10.82     | ET INFO Packed Executable Download                                                |
|     31 | 192.74.239.200    | 192.168.10.82     | ET INFO EXE - Served Attached HTTP                                                |
|      3 | 62.76.189.216     | 192.168.10.82     | ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)                    |
|      2 | 192.168.10.82     | 192.74.239.200    | ET INFO Exectuable Download from dotted-quad Host                                 |
|      2 | 192.168.10.82     | 82.165.105.70     | ET CURRENT_EVENTS Fake FedEX/Pony spam campaign URI Struct                        |
|      2 | 192.168.10.82     | 75.98.78.111      | ET POLICY User-Agent (NSIS_Inetc (Mozilla)) - Sometimes used by hostile installers |
|      1 | 85.159.235.119    | 192.168.10.82     | GPL SHELLCODE x86 inc ebx NOOP                                                    |
|      1 | 192.168.10.82     | 204.188.238.141   | ET CNC Zeus/Spyeye/Palevo Tracker Reported CnC Server TCP (group 9)               |
+--------+------------------+-----------------+-----------------------------------------------------------------------------------+
9 rows in set (0.17 sec)
```

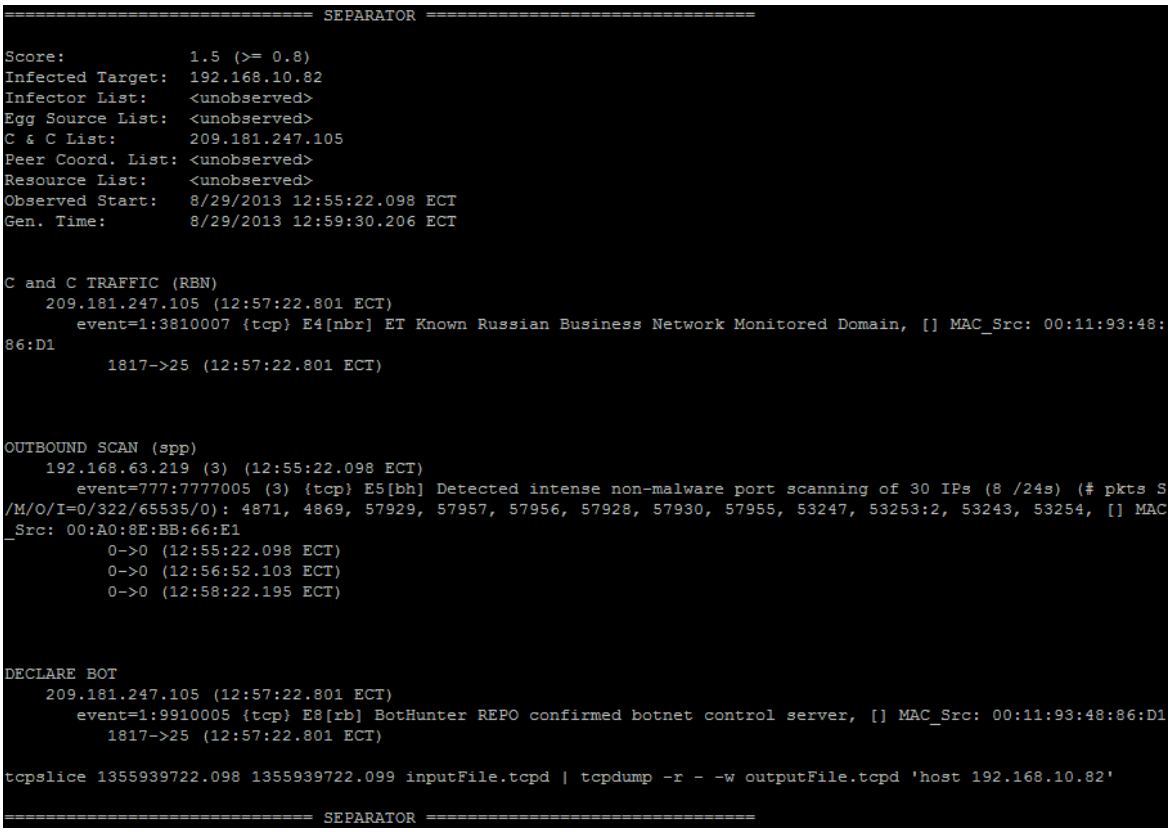
Figura. 5.49. Alertas de Snort generadas por host infectado

Para complementar la investigación es interesante investigar las direcciones IP externas para notar si han sido reportadas por algún sitio de malware, para este fin se procedió a investigar las direcciones en el sitio www.virustotal.com obteniendo que la mitad de direcciones IP han sido reportadas (ver Tabla. 5.5.)

Dirección IP	# de detecciones por virus total
62.76.189.216	2
192.74.239.200	3
82.165.105.70	0
75.98.78.111	0
85.159.235.119	0
204.188.238.141	1

Tabla. 5.5. Reputación en virus total de direcciones IP's comunicadas por el host infectado

En cambio, BotHunter creo un perfil en el que se pueden observar diferentes etapas del proceso de infección, en este perfil se puede observar que hubo comunicaciones con servidores de comando y control, una escaneo hacia afuera (interpretado como posible intento de propagación) y una comunicación con un servidor de control de botnets confirmado por el equipo de investigación de BotHunter (ver Figura. 5.50.).



```
============================== SEPARATOR ==============================

Score:            1.5 (>= 0.8)
Infected Target:  192.168.10.82
Infector List:    <unobserved>
Egg Source List:  <unobserved>
C & C List:       209.181.247.105
Peer Coord. List: <unobserved>
Resource List:    <unobserved>
Observed Start:   8/29/2013 12:55:22.098 ECT
Gen. Time:        8/29/2013 12:59:30.206 ECT


C and C TRAFFIC (RBN)
    209.181.247.105 (12:57:22.801 ECT)
       event=1:3810007 {tcp} E4[nbr] ET Known Russian Business Network Monitored Domain, [] MAC_Src: 00:11:93:48:
86:D1
          1817->25 (12:57:22.801 ECT)



OUTBOUND SCAN (spp)
    192.168.63.219 (3) (12:55:22.098 ECT)
       event=777:7777005 (3) {tcp} E5[bh] Detected intense non-malware port scanning of 30 IPs (8 /24s) (# pkts S
/M/O/I=0/322/65535/0): 4871, 4869, 57929, 57957, 57956, 57928, 57930, 57955, 53247, 53253:2, 53243, 53254, [] MAC
_Src: 00:A0:8E:BB:66:E1
          0->0 (12:55:22.098 ECT)
          0->0 (12:56:52.103 ECT)
          0->0 (12:58:22.195 ECT)



DECLARE BOT
    209.181.247.105 (12:57:22.801 ECT)
       event=1:9910005 {tcp} E8[rb] BotHunter REPO confirmed botnet control server, [] MAC_Src: 00:11:93:48:86:D1
          1817->25 (12:57:22.801 ECT)

tcpslice 1355939722.098 1355939722.099 inputFile.tcpd | tcpdump -r - -w outputFile.tcpd 'host 192.168.10.82'

============================== SEPARATOR ==============================
```

Figura. 5.50 Perfil de BotHunter generado por el host infectado

5.3. EVALUACIÓN DE RESULTADOS

Posterior a las pruebas realizadas se pudo comprobar que no existió ningún tipo de ataque que no pueda ser detectado o bloqueado por los elementos de seguridad de la red.

Además de demostró la necesidad de un sistema integral de seguridad ya que hay varios tipos o vectores de ataques que no pueden ser detenidas por las diferentes soluciones.

Los puntos más importantes concluidos posteriores al análisis son:

- Es necesario una herramienta que sea capaz de detectar y bloquear ataques de día cero.
- Un firewall de siguiente generación no es capaz de reemplazar la existencia de un firewall de aplicaciones WEB, debido a que trabajan en diferentes capaz del modelo OSI.

- Se deben tener dispositivos de seguridad instalados en los dispositivos finales principalmente para evitar ataques que no sean generados a través de la red. Por ejemplo: dispositivos extraíbles.
- Es necesario el uso de sensores que puedan proveer mayor información para un análisis forense.
- Un honeypot es una forma sencilla y económica de detectar ataques basados y no basados en firmas.

5.4. PLAN DE CONTINGENCIA

Una vez que se ha detectado la existencia del malware en la estación de trabajo, es necesario seguir una serie de pasos con el fin de evitar que el virus se expanda hacia otros usuarios. ([56] Kaspersky Lab, 2013)

- Desconectar al ordenador infectado de Internet, esto es debido a que el malware podrá obtener información personal y enviarla por este medio a terceros, o realizar el envío del mismo malware a todas las direcciones de correo que formen parte de la libreta de direcciones del host infectado.
- Si el host forma parte de una red de área local, será necesario desconectarlo, evitando así la propagación hacia todos los dispositivos que forman parte de la red interna.
- En caso de que el host infectado no pueda arrancar desde el disco duro (error al iniciar), se debe iniciar el sistema operativo en modo seguro o utilizando el disco de inicio de Windows.
- Realizar una copia de seguridad de los archivos sensibles que contengan datos críticos, para esto se utilizará una unidad extraíble como Cd, discs duro extraíble, flash memory, etc.
- En caso de que el equipo no disponga de un antivirus, proceder a la instalación del mismo.
- Proceder a la instalación de las actualizaciones del antivirus, cabe recalcar que un antivirus sin actualizaciones se vuelve una herramienta obsoleta, para realizar este paso no se debe utilizar el ordenador infectado ya que se encuentra desconectado del Internet.

- Una vez cargadas las actualizaciones, se deberá realizar un análisis completo del sistema.
- En este punto existen 2 opciones:
    - El software malicioso fue eliminado, y con esto terminará el proceso de limpieza del ordenador.
    - El malware no fue eliminado, en este caso se necesitará formatear el equipo totalmente y si no se elimina de esta manera significa que el malware ha afectado la BIOS de la máquina y no podrá ser removido, la solución es cambiar la tarjeta madre del computador afectado.
- Una vez que el malware ha sido removido del ordenador será necesario ponerlo en cuarentena para confirmar que efectivamente ya no se encuentra infectado, y a partir de este momento seguir todas las seguridades necesarias para evitar un nuevo ataque.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

La tendencia en los siguientes años será que por lo menos un 50% de la información se encuentre en la nube, esto logrará que los atacantes se vuelvan más sofisticados y persistentes en busca de esa información.

No existe ninguna persona o empresa que esté utilice cualquier tipo de dispositivo informático que se encuentre excluyente a los ataques informáticos ya que todos tienen información que pueden interesar a diferentes tipos de atacantes.

La necesidad de conectividad de empresas grandes y el crecimiento tecnológico está haciendo que cada vez existan más redes de área metropolitana y redes de áreas de campus, y debido al alto valor que manejan las empresas en temas informativos, la necesidad de seguridades avanzadas está incrementando el capital presupuestado anual en herramientas de seguridades en redes.

Las redes de área metropolitana y redes de área de campus requieren mayores protecciones que una LAN debido a que tiene más puntos de falla y requiere proteger todos sus enlaces de manera que se pueda mitigar en ataque independientemente desde que enlace se genere el mismo.

No existe ninguna herramienta que sea capaz de detectar y bloquear la gran variedad de ataques que existen actualmente por lo que siempre se debe buscar un sistema integral de manera que las diferentes herramientas sean capaces de bloquear ataques que las otras no son capaces de hacerlo.

Además de la calidad de las herramientas, es necesario realizar configuraciones adecuadas a la funcionalidad de las mismas dependiendo de cada empresa, esto logrará tener un mayor control y visibilidad del entorno de red.

Es necesario evaluar cada entorno de red y detectar y corregir las vulnerabilidades que pueden existir en los enlaces y en los sistemas operativos, servicios y aplicaciones de servidores de elementos de red, herramientas de seguridad, servidores y dispositivos finales.

El factor humano es el eslabón más débil en la cadena de seguridad de una empresa por lo que para reducir el riesgo de infección es obligatorio tener un personal capacitado con políticas de seguridad de la información regulatorias trabajando en estaciones de trabajo seguras y actualizadas.

El sistema de seguridad propuesto ha demostrado ser seguro ante las diferentes pruebas realizadas con una gran diversidad de ataques y vectores de ataque, emulando las posibles situaciones que pueden aparecer en el entorno empresarial.

6.2. RECOMENDACIONES

Se recomienda a las empresas destinar un capital anual específico y necesario para seguridad de la información buscando soluciones proactivas antes que reactivas.

Los análisis de vulnerabilidades se deben hacer por lo menos trimestralmente de manera que todos los equipos se encuentren actualizados minimizando el nivel de riesgo de sufrir un ataque.

Gartner y Forrester son un muy buen punto de partida para buscar soluciones de seguridad informática y estar actualizados con las mejores herramientas del mercado.

Referencias Bibliográficas

[1] Wikipedia. (2 de Marzo de 2013). *Wikipedia - Malware.* Obtenido de http://en.wikipedia.org/wiki/Malware

2] Miller, L. C. (2012). *Modern Malware for Dummies.* New Jersey: John Wiley & Sons, Inc.

[3] Forum, W. E. (2012). *Global Risks 2012.* Geneva.

[4] FireEye, Inc. (2013). *FireEye Corporate Presentation.*

[5] Wikipedia - PlayStation Network outage. (4 de Abril de 2013). Obtenido de http://en.wikipedia.org/wiki/PlayStation_Network_outage

[6] Albanesius, C. (6 de Mayo de 2011). Obtenido de PC Magazine: http://www.pcmag.com/article2/0,2817,2385041,00.asp

[7] Wikipedia - Operation Aurora. (6 de Abril de 2013). Obtenido de http://en.wikipedia.org/wiki/Operation_Aurora

[8] Andrew, R.-J. (2012). *Gartner's Top Predictions for 2012: Control of IT Slips Away*. Obtenido de http://www.cisco.com/web/KR/events/CiscoPlus/html/Session/Day2/PDF/speech2.pdf

[9] Rose Andrew, H. N. (2013). *Understand Security And Risk Budgeting For 2013.*

[10] Greg, Y. (2013). *Magic Quadrant for Enterprise Network Firewalls.*

[11] Gartner. (2013). *Gartner's annual Security & Risk Management Summit 2013*. Obtenido de [12:26:52] Grace Katherine Arteaga Delgado: http://www.gartner.com/technology/summits/apac/security/

[12] Pazmiño, I. P. (2012). *Ethical Hacking Course.*

[13] EC-Council. (2013). *Certified Ethical Hacker v.7.1.*

[14] FireEye Inc. (2012). *Commercial & Technical Training.* Bogotá.

[15] Gartner Inc. (2013). *Gartner - Research Methodologies*. Obtenido de http://www.gartner.com/technology/research/methodologies/research_mq.jsp

[16] Gartner Inc. (2011). *Gartner Magic Quadrant for Enterprise Network Firewalls.*

[17] Gartner Inc. (2013). *Gartner Magic Quadrant for Enterprise Network Firewalls.*

[18] Monarque, V. (2012). *Donde está mi red? Firewall e IPS Tradicional vs. NGFW.*

[19] Palo Alto Networks. (2012). *PA - 201.*

[[20] Palo Alto Networks. (2012). *Customer Overview.*

[21] Doug Dineley, H. M. (17 de Agosto de 2009). *InfoWorld - The greatest open source software of all time*. Obtenido de http://www.infoworld.com/d/open-source/greatest-open-source-software-all-time-776?page=0,0

[22] Burks, D. (22 de Junio de 2012). *Security Onion*. Obtenido de http://securityonion.blogspot.com/

[23] Montoro, R. (2012). *Snort Training.* Guayaquil.

[24] The Snort Project. (2013). *Snort Users Manual 2.9.5*. Obtenido de [13:14:19] Pablo Atiaga: http://manual.snort.org/

[25] Mischel, M. (2009). *ModSecurity 2.5 Securing your Apache installation and web applications.* Birmingham.

[26] Ristic, I. (2012). *ModSecurity Handbook*. Obtenido de http://www.modsecurity.org/documentation/modsecurity-apache/1.9.3/modsecurity-manual.html

[27] Guofei Gu, P. P. (2007). *BotHunter-Usernix07.* Atlanta.

[28] Phillip Porras, M. F. (2012). *Cyber-TA: BotHunter distribution page*. Obtenido de http://www.cyber-ta.org/releases/botHunter/index.htm

[29] Keyfocus Ltda. (2013). *KFSensor Overview*. Obtenido de http://www.keyfocus.net

[30] Palo Alto Networks. (2013). *Palo Alto Networks - PA-200*. Obtenido de https://paloaltonetworks.com/products/platforms/firewalls/pa-200/overview.html

[31] Palo Alto Networks. (2010). *Zone Protection Profiles.* Sunnyvale.

[32] Palo Alto Networks. (2012). *Palo Alto Networks - Administrator's Guide Release 5.0.*

[33] FireEye. (2013). *Web Malware Protection System - Ficha Técnica.*

[34] FireEye. (2012). *FireEye Web MPS Operator's Guide Version 6.2.0.*

[35] Sourcefire Inc. (2013). *Snort - Download Snort Rules*. Obtenido de http://snort.org/snort-rules/

[36] Emerging Threats Pro, LLC. (2013). *Emerging Threats - Open Source Community*. Obtenido de http://www.emergingthreats.net/open-source/open-source-overview/

[37] Trustwave's SpiderLabs Team. (2013). *modsecurity Open Source Web Application Firewall*. Obtenido de http://www.modsecurity.org/

[38] OWASP. (Julio de 2013). *OWASP ModSecurity Core Rule Set Project*. Obtenido de https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

[39] Center for Internet Security. (2013). *Security Benchmarks*. Obtenido de http://benchmarks.cisecurity.org/

[40] Borghello, C. (4 de Abril de 2013). Obtenido de Segu Info: http://blog.segu-info.com.ar/2013/04/nueva-vulnerabilidad-en-facebook.html#axzz2dxNRJsXO

[41] Qualys Inc. (2013). *QualysGuard Evaluator's Guide.*

[42] Kioskea. (Julio de 2013). *Ataques al servidor Web*. Obtenido de http://es.kioskea.net/contents/16-ataques-al-servidor-web

[43] Qualys Inc. (2013). *Qualys Guard WAS 3.0 Getting Starded Guide.*

[44] Reid, T. (1700). *Ensayos en los Poderes Intelectuales del Hombre.*

[45] Gartner. (Enero de 2012). *Magic Quadrant for Endpoint Protection Platforms.*

[46] Kaspersky Lab. (6 de Agosto de 2013). *Kaspersky - About Us*. Obtenido de http://www.kaspersky.com/about/news/business/2013/Independent_experts_named_Kaspersky_Internet_Security_as_the_industrys_best

[47] Dennis Technology Labs. (2013). *Home Anti-Virus Protection.*

[48] Kaspersky Lab. (2013). *Kaspersky - Internet Security*. Obtenido de http://latam.kaspersky.com/productos/productos-para-el-hogar/internet-security

[49] Secunia. (2013). *Secunia Stay Secure*. Obtenido de http://secunia.com/vulnerability_scanning/personal/

[50] Microsoft. (2011). *Pymes y autónomos*. Obtenido de http://www.microsoft.com/business/es-es/content/paginas/article.aspx?cbcid=227

[51] Herzog, P. (2010). *Open Source Security Testing Methodology Manual.*

[52] Palo Alto Networks. (2013). *Threat Vault - Palo Alto Networks*. Obtenido de https://threatvault.paloaltonetworks.com/

[53] OWASP. (2012). *OWASP Broken Web Applications Project*. Obtenido de https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

[54] SANS Technology Institute. (2013). *Reverse Hash Calculator*. Obtenido de https://isc.sans.edu/tools/reversehash.html

[55] Mozilla. (2013). *Addons Mozilla Fireforce*. Obtenido de https://addons.mozilla.org/es/firefox/addon/fireforce/

[56] Kaspersky Lab. (2013). *Qué hacer si su ordenador está infectado*. Obtenido de http://www.viruslist.com/sp/viruses/encyclopedia?chapter=153280800