UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

MAESTRÍA EN TELEMÁTICA

SIMULACIÓN DE ATAQUES A REDES IP EN UN ENTORNO CORPORATIVO REAL

PROYECTO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGÍSTER EN TELEMÁTICA

AUTOR: ING. HELMUTH LENIN HERRERA FIGUEROA

DIRECTOR: ING. DIEGO ARTURO PONCE VÁSQUEZ. PhD.

Octubre 2015

CUENCA-ECUADOR

RESUMEN

En una sociedad en continuo desarrollo donde la tecnología avanza a pasos agigantados las organizaciones cada vez más competitivas, dependen de sus redes de datos para el desarrollo y continuidad de sus negocios y un problema presentado puede ocasionar pérdidas representativas.

Uno de los problemas presentes en la actualidad es de la falta de medidas de seguridad en sus redes de datos. El aumento de atacantes ha desencadenado habilidades especiales que junto a las fallas de seguridad en las organizaciones ponen en peligro la información de la organización.

Los antecedentes, estado del arte, necesidades a ser satisfechas, problemas a ser resueltos, justificación del proyecto, objetivos generales y específicos de la tesis, además del alcance, representan el material presentado en el capítulo 1.

En el capítulo 2 se desarrollará un estudio teórico sobre seguridad, al final se mostrará una infraestructura de una organización en donde en base a esta se replicará un escenario virtual en condiciones similares terminando este capítulo haciendo una introducción a la herramienta de seguridad escogida; en la cual en el capítulo 3 se explicará desde la instalación de una solución de protección hasta la ejecución de los ataques con herramientas para el efecto, con estos resultados en el capítulo 4 se realiza propuestas de mejora, conclusiones y recomendaciones en base a lo ejecutado.

PALABRAS CLAVE.

- Seguridad Informática.
- Ataques a Redes de Datos.

- Herramientas para realizar Ataques a Redes de Datos.

ABSTRACT

In a society in continuous development where technology is advancing by leaps and bounds increasingly competitive organizations depend on their data networks for development and business continuity and submitted representative problem can cause losses.

One of the problems present today is the lack of security measures in their data networks. Increasing attackers unleashed with special abilities that security flaws in organizations threatening organizational information outsiders can profit from this.

Background, state of the art, needs to be met, problems to be solved, justification of the project, aims and objectives of the thesis, in addition to the scope, represent the material presented in Chapter 1.

In Chapter 2 a theoretical study on Security Issues will be held at the end of an infrastructure of an organization is displayed where based on a virtual stage this will be replicated in similar conditions ending this chapter with an introduction to the chosen security tool; in which in Chapter 3 step by step will be explained from the installation of a protection solution to execution of attacks tools for this purpose, with these results suggestions for improvement are made, and finally an analysis of the best presents Information Security practices thus in chapter 4 a series of conclusions and final recommendations are made.

KEYWORDS.

- Information Security
- Attacks to Data Networks.

- Tools for Attacks to Data Networks.
- Perimeter Security Tool.

ÍNDICE DE CONTENIDO

CAPITULO 1

INTRODUCCIÓN

CAPITULO 2

CONCEPTOS BASICOS

CAPITULO 3

EJECUCION DE ATAQUES

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

Yo, Helmuth Lenin Herrera Figueroa, autor de la tesis "SIMULACION DE ATAQUES A REDES IP EN UN ENTORNO CORPORATIVO REAL", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

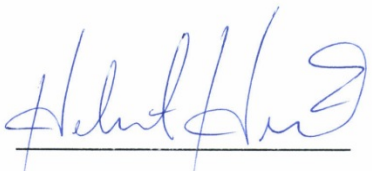
Cuenca, Junio de 2015

Helmuth Lenin Herrera Figueroa

C.I: 0103428462

Yo, Helmuth Lenin Herrera Figueroa, autor de la tesis "SIMULACION DE ATAQUES A REDES IP EN UN ENTORNO CORPORATIVO REAL", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Magíster en Telemática. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, Junio de 2015



Helmuth Lenin Herrera Figueroa

C.I: 0103428462

CAPITULO 1

Introducción

1.1 Introducción.

El continuo desarrollo de las telecomunicaciones y de Internet ha introducido nuevas Aplicaciones y requerimientos para usuarios fijos y móviles. Esto genera riesgos de seguridad de nuestra información. Si estamos en un entorno corporativo no solo la información personal se ve amenazada sino información crucial del giro de un negocio.

Los riesgos de ataques a la información surgen a partir de las debilidades de las redes de Datos y de los sistemas, estos ataques ya sea internos o externos pueden dejar inoperables ciertos servicios y recursos de hardware y software generando pérdidas económicas y exponiendo nuestra información.

Al existir personas dedicadas al hurto de información, ya sea por dinero o placer dentro de una misma empresa o desde el exterior, es preciso contar con mecanismos de Seguridad que permitan descartar acciones que pongan en riesgo la información. [1]

Para esto se pretende realizar un análisis de una red de Datos de una organización replicada en un escenario virtual, a la cual se va realizar diversos tipos de Ataques de manera controlada con el propósito de hacer una evaluación del nivel de seguridad y proponer acciones de protección.

Antecedentes.

El acceso a la información y al conocimiento provisto por los servicios de telecomunicaciones, representa un factor importante en el progreso y desarrollo de las naciones y permite la disminución de la brecha digital. Frente a esta realidad, se están desarrollando cambios sociales que afectan significativamente a la capacidad de los departamentos de TI para mantener la seguridad de la Red.

Frecuentemente y en la actualidad las Redes de Datos poseen mecanismos de protección y prevención, por más mínimo que este sea, sin embargo estos mecanismos a pesar de ser imprescindibles, requieren implementar mayores controles y deben ser constantemente actualizados ya que la seguridad de la información frente a los intrusos de la red debe ser proactiva antes que reactiva. [2].

Estado del Arte.

En la Actualidad las organizaciones dependen de sus diferentes tipos de software y bases de datos que manejan su información importante y crucial de su giro de negocio, los mismos que están constantemente expuestos a amenazas [2] de seguridad que se producen si se encuentra una vulnerabilidad o debilidad que pueda ser aprovechada, como por ejemplo de índole ambiental (temperatura, humedad, fuego, etc), de energía (apagones, variaciones de energía) o debido a factores humanos (acceso no autorizado, negligencia, falta de trabajo de diagnóstico y errores humanos). También estas amenazas pueden ser digitales como malware (virus, troyanos, DoS, etc) y Hackers. Estas últimas pueden causar desde una interrupción de un servicio web hasta un acceso externo no autorizado en muchas ocasiones con malas intenciones. [2]

La información constantemente amenazada, tiene que ser protegida tanto de los usuarios internos de la empresa como de atacantes externos, el objetivo de esta protección es garantizar que los recursos informáticos de la empresa así como la información no tengan daños o alteraciones.

Uno de los ataques más comunes que se presentan en las redes de datos de una organización es el ataque de escaneo de puertos mediante el cual un atacante explora uno o varios servidores en busca de potenciales puertas abiertas o brechas de seguridad y topologías, que implica además un alto tráfico en la red, lo que se manifiesta en tiempos altos de respuesta de los sistemas informáticos. [3]

Dentro de este marco, la comunidad científica muestra interés en la implementación de soluciones para disminuir los ataques a la seguridad haciendo uso de tecnologías de virtualización como por ejemplo.

Keller y Naues, [4] formulan la implementación de un laboratorio colaborativo de seguridad utilizando máquinas virtuales.

P. Li y Mohammed [5] proponen la integración de las tecnologías de virtualización para la educación de seguridad en redes implementando un laboratorio remoto de detección de intrusiones.

Otros investigadores [6] [7], han utilizado el concepto de Honeynet basada en máquinas virtuales, como una herramienta de seguridad cuyo propósito es el estudio de las técnicas y motivaciones de los atacantes al romper los sistemas de seguridad.

En este mismo ámbito [8], [9] han utilizado las plataformas de virtualización para recuperación de desastres y mitigación de ataques reales a redes IP. [10].

En un marco muy similar al presente trabajo, se tienen varios estudios desarrollados en escenarios virtualizados con herramientas de libre distribución

como el de Fuertes, [10] quienes realizan un conjunto de ataques y presentan opciones de mitigación con scripts en Linux con un alto grado de efectividad, sin embargo el dominio de herramientas Linux puede ser limitado en la práctica y susceptible a errores humanos.

El presente trabajo por su parte tiene como objetivo reflejar la infraestructura real de una organización en un escenario Virtual, en donde se realizarán una serie de ataques reales que permitan determinar el nivel de seguridad perimetral que se tiene y proponer mejoras que son traducidas en mecanismos de control y mitigación, todo esto con una herramienta de pago y con interfaces gráficas que permiten un ahorro de tiempo en el manejo de la herramienta, que al final con su conjunto de módulos de software que incluye la herramienta nos permitirán observar un alto grado de efectividad, como su único inconveniente se resalta su costo.

El escenario virtual sobre el cual se aplicarán los ataques en el presente documento, contiene los elementos más importantes que existen en la infraestructura real que son:

- Acceso a Internet.
- Atacante Externo.
- Equipo de Seguridad Perimetral.
- Servidor Web Interno. (Víctima).

Se justifica la infraestructura propuesta ya que representa el escenario de un organismo del sector público de la ciudad el cual se encuentra funcionando el cual también es el reflejo de otras organizaciones que tienen un patrón común. Se destaca además la presencia de un servidor proxy reverso para todos los servidores web internos en la realidad los cuales no son publicados al internet directamente, esto como una opción adicional de seguridad.

Finalmente de acuerdo con la Norma ISO 27002, un nivel adecuado de Seguridad Informática se puede conseguir implementando una cantidad de controles en el momento que sea necesario con el objetivo de cumplir los objetivos específicos de seguridad de una determinada Organización. Los controles pueden ser entre otros la implementación de políticas, planes de contingencia, manuales o procedimientos, funciones de software, etc; lo importante de la implementación de controles radica en que puedan ser constantemente monitoreados, revisados y mejorados.

De acuerdo con investigaciones recientes, en un futuro las Amenazas se centran en dos grandes áreas: ingeniería social (manipulación de formularios, llamadas no Solicitadas, mails, mensajes, etc) y ataques multivectoriales donde se combinan diferentes tipos de soporte (correo electrónico, mensajes en blogs, redes sociales, wikis,...., voz, vídeo, audio, etc.) [3].

Varios aspectos como los ocurridos en el año 2013, en violaciones de datos cruciales. El robo y la publicación de información de inteligencia estadounidense y fugas de Información a WikiLeaks [4] sacudieron las relaciones diplomáticas a nivel mundial, el ataque de los servidores de la empresa privada de Inteligencia de USA Stratfor, etc.

En Febrero de 2015 Kaspersky Labs informa el robo millonario de más de 1000 millones de Dolares mediante un malware conocido como Carbanak, realizado por criminales cibernéticos originarios de Rusia, Ucrania, China y varios países europeos, a cientos de bancos alrededor del mundo, siendo el blanco de esta acción sin precedentes las propias entidades bancarias y con técnicas de Amenazas Persistentes Avanzadas (APT por sus siglas en inglés) los hackers simularon que

cada actividad fraudulenta era realizada por empleados del banco, el dinero robado fue depositado en bancos en China o Estados Unidos.

Situación en el Ecuador.

En Nuestro país en lo referente a la Seguridad de la Información muchas empresas privadas en entornos PYMES han optado en la adopción de Firewall Perimetral (cortafuegos de red que en ocasiones engloban múltiples funcionalidades o servicios en un mismo equipo de protección) como opción de Seguridad.

Es en este tipo de entorno en donde realizaremos una serie de procedimientos que pretenden encontrar debilidades que permitan a un supuesto atacante encontrar información confidencial o simplemente ingresar a una red de Datos ajena. También generaremos propuestas de protección a nivel de red local como el control de usuarios con sistemas AAA (Radius) sistemas de detección de intrusiones (IDS), control de puertos de red, control de accesos inalámbricos, uso de VLANs dentro de la empresa, VPNs, etc, que serán analizados en presente documento.

Un aspecto importante destacar a nivel nacional es el avance de la tecnología que ha permitido y popularizado servicios bancarios como es la Banca en Línea, que brinda al usuario la posibilidad de realizar transacciones y consultas a través de la Internet. Desafortunadamente, también la delincuencia cibernética hace de las suyas con el robo de claves y la estafa, en nuestro país esto ya tiene jurisprudencia y está tipificado como un delito que se lo denomina Delito Informático.

De acuerdo con la Superintendencia de Bancos del Ecuador los casos más comunes de Delitos informáticos fundamentalmente usan técnicas para obtener claves, mediante “Phishing, Phaming, Malware bancario (troyanos y keyloggers),

Skimming ataques de hombre en el medio, etc", la estafa piramidal, el hoax y la carta nigeriana además de los casos de clonación de tarjetas de crédito, entre otros.

Ante el creciente número de afectados de fraudes electrónicos, el 17 de Enero de 2012 la Superintendencia de Bancos del Ecuador en resolución JB-2012-2090 exige a todas las entidades Financieras tener un seguro contra delitos informáticos y menciona "*las instituciones financieras contratarán anualmente con las compañías de seguro privado, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares...."* [4].

Ante esto varias entidades financieras han implementado sistemas de seguridad Web para sus sitios transaccionales como por ejemplo módulos WAF (Caso especial del Banco del Pichincha) que anula las técnicas descritas anteriormente, entre otros sistemas de seguridad, sin embargo en la actualidad todavía existen entidades financieras y organizaciones privadas y gubernamentales que permiten en sus sitios web el pago mediante tarjetas de crédito sin esquemas de seguridad que exponen al usuario a este tipo de amenazas.

También es importante mencionar que en Diciembre de 2013 se publicó el acuerdo Ministerial 166 que entre varios puntos en su Artículo 1, dispone "*a las entidades de la Administración Pública Central, Institucional y que dependan de la Función Ejecutiva el Uso Obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de la Seguridad de la Información".*

En el Ecuador el tema legal de la seguridad informática se destaca a partir del último registro oficial de Código penal Integral del 2014 en la sección tercera *"Delitos contra la seguridad de los activos de los sistemas de información y comunicación*" y en su artículo 230 se contempla sanciones para quien desarrolle copias de sitios de

confianza para que los usuarios ingresen información sensible (Ecuador, 2014). Sin embargo, el artículo se refiere a modificación de registros DNS para re direccionar a los usuarios a otras páginas, el phishing no manipula en lo absoluto registros DNS, simplemente dirige a una página con diseño similar a la original, pero distinto dominio [5].

En la actualidad, la Fiscalía General del Estado responsabiliza a las instituciones del Sistema Financiero exigiendo a la Superintendencia de Bancos la restitución del 100% de los perjuicios causados por fraudes informáticos a sus clientes.

1.2 Descripción del Problema o Necesidad.

Necesidades a ser Satisfechas.

Al ser la información considerada como uno de los factores más importantes dentro de una organización y su protección relacionado directamente con la seguridad de la Información se plantea la necesidad de determinar el nivel de seguridad perimetral que brinda una determinada solución planteada de una organización en función de sus objetivos específicos, que puede ser el reflejo de otras con similares características de Infraestructura de Red.

Problemas a ser resueltos.

Ante esta problemática se plantea realizar diferentes ataques generados por herramientas de software y controlados debido a que son aplicados dentro de un entorno virtual, el propósito del presente trabajo es observar el comportamiento de la solución de seguridad perimetral propuesta y determinar el nivel de seguridad en

función de sus objetivos específicos de seguridad de la organización y proponer mecanismos de protección necesarios dentro de una infraestructura existente.

1.3 Justificación del proyecto de tesis.

Al finalizar el presente proyecto de tesis se dispondrá de un documento en donde se parte de una Infraestructura Real de una organización que se encuentra en producción y funcionando la cual por efectos de confidencialidad no se publica su nombre (es una red que tiene similitud con varias infraestructuras por tanto el caso de estudio puede ser aplicado a varias organizaciones tomando las consideraciones necesarias), la misma a su vez es replicada en un entorno virtual mediante la herramienta de virtualización VMWare. El objetivo que se pretende es determinar la seguridad que brinda la herramienta perimetral propuesta frente a una serie de ataques externos mediante Herramientas de Software.

Para ello se realiza un estudio teórico de los fundamentos de Seguridad Informática estudiadas en el capítulo 2; en el capítulo 3 se realizará la parte práctica que incluye desde la instalación y configuración de la solución perimetral propuesta dentro de un escenario virtual y una serie de ataques mediante herramientas para el efecto, finalizando en el capítulo 4 con conclusiones y recomendaciones.

Beneficios para el usuario.

Empresas y Organizaciones que no toman en consideración aspectos importantes como la Seguridad de la Información al observar los resultados de este documento se podrán dar cuenta de la necesidad de invertir en tecnología ya que es un aspecto que pone en peligro la Información y continuidad de una organización.

La posibilidad de poseer un documento informativo y de respaldo en donde se observe el comportamiento de una solución de seguridad determinada ante eventuales ataques externos. El estudio podrá ser replicado con gran facilidad en otras organizaciones ya que la red propuesta tiene similitud con muchas otras.

Beneficios para el estudiante.

Aplicar el conocimiento adquirido, poniendo en práctica en la aplicación de procedimientos que permitan determinar el nivel de seguridad de una Red de Datos de una Organización.

Poder realizar un estudio con la probabilidad de ser replicado en otras organizaciones y proponer medidas de prevención.

1.4. Objetivos de la tesis de grado

Objetivo general

Realizar ataques controlados dentro de un escenario virtual que contemple las condiciones reales de una empresa, con el propósito de evaluar el estado de seguridad perimetral y proponer mejoras en el ámbito de seguridad.

Objetivos específicos:

Objetivos tangibles

- Crear un escenario virtual en donde se explique paso a paso la instalación de un sistema de Seguridad.
- Identificar herramientas existentes que permitan realizar ataques a una red de datos o test de penetración.

- Generar un Documento en donde se Evalúe el nivel de seguridad de una red de Datos mediante la simulación de Ataques reales.
- Promover la Generación de Conocimiento pudiendo el presente estudio servir como base para futuros desarrollos en medida del avance de la tecnología y de ataques a futuro.

Objetivos intangibles.

Desarrollar un estudio que sirva de sustento técnico y justificativo de inversión en tecnología para protección de la información, de aplicación en corto plazo y pueda ser replicado de manera de tener un escenario de pruebas y laboratorio.

1.5 Alcance del proyecto.

El presente trabajo será desarrollado según lo señalado en los objetivos planteados, el proceso a seguir será el siguiente:

Inicialmente, en un primer capítulo se indicará los antecedentes, estado del arte, necesidades a ser satisfechas, problemas a ser resueltos, justificación del proyecto, objetivos generales y específicos así como el alcance del presente documento.

En el capítulo 2 se desarrollará un estudio teórico sobre: Seguridad Informática, conceptos básicos, metodologías de ataques, Hackeo Ético, estudio y clasificación de vulnerabilidades, amenazas comunes, recomendaciones de seguridad, aplicaciones peligrosas, seguridad en redes y aplicaciones web, estándares de Seguridad, se realiza también un análisis actual de la organización en relación al cumplimiento de la normativa vigente realizando para ello un análisis de riesgos y en

base a datos estimados un porcentaje de cumplimiento de la normativa y finalmente se mostrará una infraestructura de una organización en donde en base a esta se replicará un escenario virtual en condiciones similares terminando este capítulo haciendo una introducción a la herramienta de seguridad escogida; en la cual en el capítulo 3 se explicará desde la instalación de una solución de Seguridad Perimetral propuesta en un entorno virtual práctico que incluye también un escenario de atacante y víctima, en donde se seguirá el proceso de Ethical hacking en sus etapas de Reconocimiento, escaneo y análisis de vulnerabilidades y finalmente la ejecución de ataques de penetración, con estos resultados en el capítulo 4 se realiza una serie de conclusiones y recomendaciones finales.

CAPITULO 2

Conceptos Básicos

2.1 Seguridad en Redes de Datos

Inicialmente las redes de datos fueron utilizadas para el envío y recepción de correo electrónico y compartir impresoras. Ahora, la gente realiza transacciones bancarias, compras, ventas, declaraciones de impuestos, etc; haciendo a las organizaciones cada vez más dependientes de sus redes de datos, a tal punto que un problema por más pequeño que parezca puede llegar a comprometer la continuidad de actividades.

Los registros de varias compañías a nivel mundial indican que “la mayoría de ataques no son cometidos por intrusos si no por miembros internos con resentimiento” [6], lo cual es demostrado en un estudio de la consultora Datapro Research Corp., se indica que el 80% de los problemas de seguridad de información en una organización, son generados por sus empleados. [7].

En conclusión, mantener un esquema de seguridad implica considerar este hecho, además de estar alerta frente a adversarios los cuales a menudo son muy inteligentes, dedicados y bien financiados. [6]

2.2 Problemas de Seguridad en las Redes de Datos

Los problemas de Seguridad pueden clasificarse en la ausencia de:

2.1.1 Confidencialidad

2.1.2 Autenticación

2.1.3 No Repudio

2.1.4 Control de Acceso

La Confidencialidad intenta proteger la información del alcance de usuarios no autorizados. [6]

La Autenticación intenta determinar con quien se va a interactuar antes de revelar información delicada o hacer un trato de negocios.

El no repudio se ocupa de las firmas es decir, de comprobar que un cliente hizo efectivamente un trato, cuando el luego deduce que no lo hizo.

Finalmente, cómo asegurar un mensaje recibido realmente fue el enviado y no fue interceptado o quizás modificado en su camino.

En Redes de Datos para lograr seguridad, cada capa del modelo de protocolo en capas tiene su contribución. [6]

La capa física por ejemplo podemos proteger contra la intervención del medio de transmisión encerrando estas en tubos sellados con gas a alta presión. Cualquier intento de hacer agujero en el tubo liberara un poco de gas, con lo cual la presión disminuirá y se disparará una alarma. Algunos sistemas militares usan esta técnica". [6].

En la capa de enlace de datos, los paquetes de un enlace directo pueden cifrarse cuando se envíen desde una máquina y descifrarse cuando lleguen a su destino, y esto sería suficiente sin embargo "esta solución se viene abajo cuando los paquetes tienen que atravesar varios enrutadores, puesto que los paquetes tienen

que descifrarse en cada enrutador, dentro del cual son vulnerables a posibles ataques". [6]

En la "capa de red pueden instalarse firewalls para permitir o denegar paquetes" [6], lo que da lugar a un breve esquema de seguridad (IP).

En la capa de transporte pueden cifrarse conexiones enteras, de extremo a extremo y *"por último, los asuntos como la autenticación de usuario y el no repudio solo pueden manejarse en la capa de aplicación"* [6].

Un punto importante de destacar es que *"casi toda la seguridad se basa en principios de criptografía, a excepción de la seguridad en la capa física".* [6]

2.3 Conceptos de Seguridad

2.3.1 Amenaza

Una amenaza es un "evento que puede llegar a causar daño a los bienes informáticos, puede ser una persona, un programa malicioso o un suceso natural o de otra índole y representa los posibles atacantes que pueden incidir negativamente sobre las debilidades informáticas" [8].

2.3.2 Análisis de Riesgo

Es el procedimiento que permite determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos e implica los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que pueden llegar a tener.

2.3.3 Bienes informáticos

Son los componentes informáticos que se requieren proteger de que se materialice una amenaza y que pueda causar daño sobre estos.

2.3.4 Riesgo

Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático causando un impacto negativo en la organización.

2.3.5 Riesgo Residual

Es el riesgo remanente después de aplicados los controles de seguridad para minimizarlo.

2.3.6 Seguridad

En términos informáticos es usado para minimizar los riesgos a los que están sometidos los bienes informáticos hasta llevarlos a niveles adecuados.

2.3.7 Sistema Informático

Es el conjunto de bienes informáticos que dispone una organización para su correcto funcionamiento y la consecución de sus objetivos.

2.3.8 Vulnerabilidad

En un sistema informático es un aspecto susceptible de ser atacado o de dañar su seguridad, representan las debilidades o aspectos falibles o atacables en el sistema informático y califican el nivel de riesgo del mismo.

2.3.9 Pruebas de Penetración

En términos de seguridad, una prueba de penetración se produce cuando un ataque es exitoso y un intruso es capaz de ingresar atravesando el equipo perimetral, la prueba de penetración puede conseguir una lectura de unos pocos bits de datos de red o tan grande como una sesión de un usuario con privilegios restringidos. Uno de los objetivos principales de la seguridad es evitar este tipo de penetraciones.

Un método común para poner a prueba la capacidad de las medidas de seguridad perimetral es realizar una prueba de penetración.

Las pruebas de penetración es fuerte intento de irrumpir su red protegida utilizando cualquiera los medios necesarios. Es común que las organizaciones contraten a consultores externos para realizar las pruebas de penetración por lo que los probadores no están al tanto de los elementos confidenciales de la configuración de la seguridad, diseño de redes, y otros secretos internos.

Las pruebas de penetración busca encontrar cualquiera y todas las debilidades en su perímetro de seguridad existente.

Una vez que se descubre una debilidad, las contramedidas pueden ser seleccionados y desplegados para mejorar la seguridad. Una diferencia significativa entre las pruebas de penetración y real atacante es que una vez que se descubre una vulnerabilidad, el intento de intrusión cesa antes de explotar la vulnerabilidad sea explotado y cause daños en el sistema.

Las pruebas de penetración pueden realizarse utilizando herramientas de software de ataque automatizadas o manualmente utilizando scripts. Las herramientas automatizadas de ataque varían dependiendo de la calidad profesional de diferentes escáneres de vulnerabilidad (existen escáneres disponibles en el Internet). También

se utilizan a menudo Herramientas manuales para pruebas de penetración, pero se debe tener muy en cuenta que se tiene mucha responsabilidad en saber cómo perpetrar un ataque.

Las pruebas de penetración se deben realizar sólo con el consentimiento y conocimiento del personal de TI, la ejecución de pruebas de seguridad sin la debida experiencia, podría resultar en la pérdida de la productividad, regularmente los intentos de penetración son una buena manera de juzgar con precisión los mecanismos de seguridad desplegados por una organización. Las pruebas de penetración también pueden revelar áreas donde parches o configuración de seguridad son insuficientes y donde las nuevas vulnerabilidades se han desarrollado. [8]

2.4 Métodos de Ataques.

Los atacantes se centran en violar el perímetro de seguridad de un sistema con el propósito de obtener acceso a los datos, alterar o destruirlos, e inhibir acceso válido a los datos y recursos con varios propósitos, principalmente económico; los medios por los que los ataques se ejecutan varían mucho, algunos son extremadamente complejos y requieren un conocimiento detallado de los sistemas de víctimas y técnicas de programación, mientras que otros son muy fáciles de ejecutar y requieren de una dirección IP y la capacidad para manipular algunas herramientas o scripts. Pero a pesar de que hay muchos tipos diferentes de ataques, pueden ser generalmente agrupados y clasificados en categorías. [8]

A continuación se enumera y se describe las metodologías de ataques:

1. De Fuerza bruta o Ataque de Diccionario.
2. Negación de Servicio.

3. Spoofing.
4. Ataque de hombre en el medio.
5. Sniffers.
6. Crackers.

2.4.1 Ataque de Fuerza Bruta y Diccionario.

Un ataque de diccionario y fuerza bruta se estudian a menudo juntos, ya que su objetivo común son las contraseñas. Cualquier tipo de ataque puede ser dirigido a un archivo de base de datos de contraseñas o a un símbolo de inicio de sesión activa.

Un ataque de fuerza bruta es un intento de descubrir las contraseñas de cuentas de usuario de forma sistemática, intenta cada posible combinación de letras, números y símbolos. Con la velocidad de las computadoras modernas y la capacidad de emplear la computación distribuida, los ataques de fuerza bruta tienen éxito incluso si se trata de contraseñas seguras. Con tiempo suficiente, todas las contraseñas pueden ser descubiertas usando un método de ataque de fuerza bruta.

La mayoría de las contraseñas de 14 caracteres o menos necesitan cerca de 7 días en un sistema rápido usando un programa de ataque de fuerza bruta contra un robo de archivo de base de datos de la contraseña (el tiempo real que se necesita para descubrir contraseñas depende de la algoritmo de cifrado utilizado).

Cuanto más larga sea la contraseña es más costoso y consume mucho tiempo a un ataque fuerza bruta. Cuando el número de posibilidades se incrementa, el costo de realizar un ataque exhaustivo aumenta también. En otras palabras mientras más larga sea la contraseña más tiempo se tardará el sistema de ataque en reconocerla.

Un ataque de diccionario es un intento de descubrir las contraseñas mediante una lista predefinida de contraseñas comunes o esperadas. Este tipo de ataque es llamado así porque la lista de contraseñas posibles es tan larga como si se estuviera utilizando todo el diccionario para buscar una palabra en este caso una contraseña. Los Ataques a las contraseñas emplean un método de ataque criptográfico conocido como el ataque de cumpleaños. Este ataque también puede ser llamado encuentro de Hash reverso o explotación de colisión. Básicamente, el ataque explota el hecho de que si dos mensajes son modificados por una función de hash y los valores de hash son iguales, entonces los dos mensajes son probablemente el mismo. Una forma de expresar esto en notación matemática o criptográfica es H (M) = H (M'). Las contraseñas se almacenan en un archivo que contiene la base de datos de cuentas en un sistema seguro. Sin embargo, en lugar de ser almacenada como texto claro, las contraseñas se modifican con una función de hash y sólo sus valores hash se almacenan realmente. Esto proporciona un nivel razonable de protección. Sin embargo, mediante la comparación de hash inversa, una herramienta de Crack de contraseñas busca posibles contraseñas (ya sea a través de la fuerza bruta o métodos de diccionario) que tienen el mismo valor hash que el valor almacenado en el archivo de base de datos de cuentas. Cuando se descubre una coincidencia de valor hash, entonces se dice que la herramienta ha crackeado la contraseña.

Las combinaciones de estas dos metodologías de ataque a las contraseñas pueden ser utilizadas lográndose resultados excelentes. Por ejemplo, un ataque de fuerza bruta puede utilizar una lista de diccionario como el origen de su suposición.

Los ataques de diccionario son a menudo exitosos debido a la previsibilidad de la naturaleza humana para seleccionar contraseñas basadas en experiencias

personales. Desafortunadamente, las experiencias personales a menudo se transmiten al mundo que rodea simplemente por la forma en que viven y actúan sobre una base diaria. Si un individuo es fanático de los deportes, la contraseña podría basarse en nombre de un jugador o de un disco de éxito. Si usted tiene niños, la contraseña puede estar basadaen sus nombres o fechas de nacimiento. Si usted trabaja en una industria, la contraseña podría basarse en el nombre o siglas de la industria o nombres de productos. Cuantos más datos sobre la víctima se consigue por medio de ingeniería social más exitosa será la lista de diccionario personalizada.

La protección de contraseñas contra los ataques de la fuerza bruta y ataques de diccionario requiere numerosas precauciones de seguridad y una rígida política de seguridad. En primer lugar, el acceso físico a los sistemas debe ser controlado. Si un atacante logra acceso físico a un servidor de autenticación, puede robar el archivo de contraseñas en cuestión de segundos. Una vez que un archivo de contraseñas es robado, todas las contraseñas están en peligro.

En segundo lugar, controlar fuertemente y monitorear el acceso electrónico a los archivos de contraseñas. Los usuarios finales y los usuarios que no son los administradores de cuentas no tienen necesidad de acceder al archivo de base de datos de contraseñas para el trabajo diario. Si descubre un acceso no autorizado al archivo de base de datos, se deberá investigar de inmediato. Si no se determinar un acceso válido, se puede considerar que todas las contraseñas están comprometidas.

En tercer lugar, elaborar una política de contraseñas que hace cumplir mediante programación contraseñas seguras y prescribir medio por el cual los usuarios finales pueden crear contraseñas fuertes. Cuanto más fuerte y más largo es el contraseña, más tiempo tomará para que pueda ser descubierto en un ataque de

fuerza bruta. Sin embargo, con tiempo suficiente, todas las contraseñas pueden ser descubiertas a través de métodos de fuerza bruta. Así, contraseñas cambiantes regularmente son necesarias para mantener la seguridad. Contraseñas estáticas más de 30 días deben ser considerada en peligro, incluso si ningún otro aspecto de un fallo de seguridad ha sido descubierto.

En cuarto lugar, implementar dos factores de autenticación, tales como el uso de la biometría o token de manera adicional a la contraseña.

En quinto lugar, el uso de control de bloqueo de cuentas para evitar ataques de fuerza bruta y ataques de diccionario en un inicio de sesión. Para los sistemas y servicios que no admiten controles de bloqueo de cuentas, como la mayoría de los servidores FTP, emplear un inicio de sesión extenso y un IDS para buscar intentos de ataques de contraseña rápidos y lentos.

En sexto lugar, cifrar archivos de contraseñas con el cifrado más potente disponible para su sistema operativo. Mantener rígido control sobre todos los medios de comunicación que tienen una copia del archivo de base de datos de contraseñas, tales como cintas de respaldo y algunos tipos de discos de arranque o de reparación.

Las contraseñas son un mecanismo de seguridad pobre cuando se usa como el único elemento de disuasión contra accesos no autorizados. Los ataques de fuerza bruta y ataques de diccionario muestran que las contraseñas solo ofrecen poco más que un bloqueo temporal. [8].

2.4.2 Ataque de Denegación de Servicio.

Son ataques que impiden que el sistema de procesamiento responda al tráfico legítimo de solicitudes de recursos y objetos. La forma más común de los

ataques de negación de servicio es cuando se transmite tantos paquetes de datos a un servidor que no les puede responder a todos los procesos. Otras formas de ataques de denegación de servicio se centran en la explotación de un fallo o vulnerabilidad conocida en un sistema operativo, servicio o aplicación. La explotación de la falla a menudo resulta en caída del sistema o la utilización de CPU al 100 por ciento. No importa en qué consiste el ataque real, cualquier ataque que hace que la víctima no puede realizar las actividades normales se puede considerar un ataque de denegación del servicio. Ataques de denegación de servicio puede dar lugar a fallos del sistema, reinicios del sistema, corrupción de datos, bloqueo de servicios y más.

Desafortunadamente, ataques de denegación de servicio basado en inundación (tráfico capaz de causar una denegación de servicio en una víctima) un servidor con datos son una forma de vida en Internet. De hecho, no se conoce ningún medio para prevenir un ataque de denegación de servicio por inundación. Además, debido a la capacidad de falsificar paquetes o explotar servicios legítimos de Internet, a menudo es imposible rastrear el origen real de un ataque y detener a los culpables.

Hay varios tipos de ataques de denegación de inundación. Primeramente el ataque original empleado con un único sistema de ataque inundando una sola víctima con un flujo constante de paquetes. Esos paquetes podría ser solicitudes válidas que nunca se completaron o paquetes malformados o fragmentados que consume la atención del sistema víctima. Esta forma simple de DoS es fácil de terminar justo mediante el bloqueo de los paquetes de la dirección IP de origen.

Otra forma de ataque se denomina denegación de servicio distribuido (DDoS). Una denegación del servicio se produce cuando el atacante compromete varios sistemas

y los utiliza como lanzamiento de plataformas contra una o más víctimas. Los sistemas comprometidos utilizados en el ataque son a menudo llamados esclavos o zombis. El resultados de un ataque DDoS en una víctima se efectiviza cuando es inundado con datos de numerosas fuentes. Un Ataque DDoS se pueden detener mediante el bloqueo de los paquetes de sistemas comprometidos. Pero esto también puede resultar en el bloqueo de tráfico legítimo porque las fuentes de la inundación paquetes son propias víctimas y no el autor original del ataque. Estos tipos de ataques están etiquetados como distribuidos porque numerosos sistemas están implicados en la propagación del ataque en contra de la víctima.

Una forma más reciente de DoS, llamado (DRDOS) *distributed reflective denial of service*, se ha descubierto. Ataques DRDOS se aprovechan de los mecanismos normales de operación de los servicios de internet, como los protocolos DNS y actualizaciones del router. La función de DRDOS es enviar numerosos paquetes de actualización, inicios de sesión o paquetes de control a varios servidores de servicios de Internet o routers con una dirección de origen falsificada de la víctima. Por lo general, estos servidores o routers son parte de una red de producción de alta velocidad, de alto volumen de tráfico, de troncos principales de Internet. Lo que resulta es una inundación de paquetes de actualización, respuestas de acuse de recibo de la sesión, o mensajes de error enviados a la víctima. Un ataque DRDOS da como resultado mucho tráfico de upstream de los sistemas afectados negativamente por la gran cantidad de los datos centrados en la víctima. tipo de ataque se llama un ataque de reflexión por la alta velocidad de los sistemas troncales reflejan el ataque a la víctima. Por desgracia, este tipo de ataques no pueden prevenirse porque explotan las funciones normales de los sistemas. El

bloqueo de estos paquetes de sistemas clave de Internet dejara fuera de una parte importante de la Internet.

No todos los casos de denegación de servicio son el resultado de un ataque malicioso. Los errores en la codificación de los sistemas operativos, servicios y aplicaciones han resultado en condiciones de denegación de servicio. Por ejemplo, un proceso que no libera el control del CPU o un servicio que consume recursos del sistema de manera desproporcionada con solicitudes de servicio que está manejando pueden causar condiciones de denegación de servicio. La mayoría de los vendedores liberan rápidamente parches para corregir estas condiciones autogeneradas DoS, por lo que es importante mantenerse informado.

Han habido muchas formas de ataques DoS cometidos a través de Internet. Algunos de los más populares se discuten a continuación.

Un Ataque de inundación SYN es cuando se llega a romper el apretón de manos estándar de tres vías utilizadas por TCP / IP para iniciar sesiones de comunicación. Normalmente, un cliente envía un paquete SYN a un servidor, el servidor responde con un paquete SYN / ACK al cliente, y el cliente entonces responde con un paquete de vuelta al servidor ACK. Este apretón de manos de tres vías establece una sesión de comunicación que es usada para transmisión de datos hasta que la sesión se termina. (Usando un saludo de 3 vías three-way handshake con paquetes FIN y ACK). Una inundación de paquetes SYN ocurre cuando numerosos paquetes SYN son enviados a un servidor pero el atacante nunca envía al servidor los paquetes de finalización SYN/ACK.

Adicionalmente, las transmisiones de paquetes SYN de transmisión por lo general tienen una dirección de origen falsa por lo que la respuesta SYN/ACK se envía algún lugar que no sea el verdadero creador de los paquetes. El servidor

espera por el paquete ACK del cliente, a menudo durante varios segundos, manteniendo abierta una sesión y consumiendo recursos del sistema. Si un número importante de sesiones abiertas se llevan a cabo (por ejemplo, a través de la recepción de una inundación de paquetes SYN), esto resulta en una denegación de servicio. El servidor puede ser fácilmente sobrecargado manteniendo sesiones abiertas que nunca se finalizaron causando así un fracaso. Ese fracaso puede ser tan simple por ser incapaz de responder a las peticiones legítimas de las comunicaciones o tan grave como un congelamiento de la aplicación o caídas del sistema.

Una contramedida a los ataques de inundación SYN es aumentando el número de conexiones que un servidor puede soportar. Sin embargo, esto por lo general requiere de recursos adicionales de hardware (memoria, velocidad de CPU, etc.) y puede no ser posible para todos los sistemas operativos o los servicios de red. Una contramedida más útil es reducir el tiempo de espera del paquete ACK final. Sin embargo, esto también puede resultar en sesiones fallidas de los clientes conectados a través de vínculos lentos o puede ser obstaculizado por el tráfico de Internet intermitente. Basados en red IDS se puede ofrecer cierta protección contra ataques SYN de inundación al notar numerosos paquetes SYN originados por uno o pocos sitios de origen, resultando en sesiones incompletas. Un IDS podría advertir sobre el ataque o dinámicamente bloquear los intentos de inundación.

Un Ataque Smurf ocurre cuando un servidor de amplificación o de la red se utiliza para inundar una víctima con datos inútiles. Un servidor de amplificación o de red es cualquier sistema que genera respuestas múltiples de paquetes, tales como paquetes ICMP ECHO o paquetes UDP especiales, a partir de un único paquete presentado.

Un ataque común es enviar un mensaje de Broadcast de una subred o red a cada nodo en la red lo que produce uno o más paquetes de respuesta. El atacante envía paquetes con información de solicitud con dirección de origen falsificada de la víctima para el sistema de amplificación. Por lo tanto, toda la respuesta de los paquetes se envía a la víctima. Si la red de amplificación es capaz de producir suficiente tráfico de paquete de respuesta, el sistema de la víctima experimentará una denegación de servicio. Figura 1.

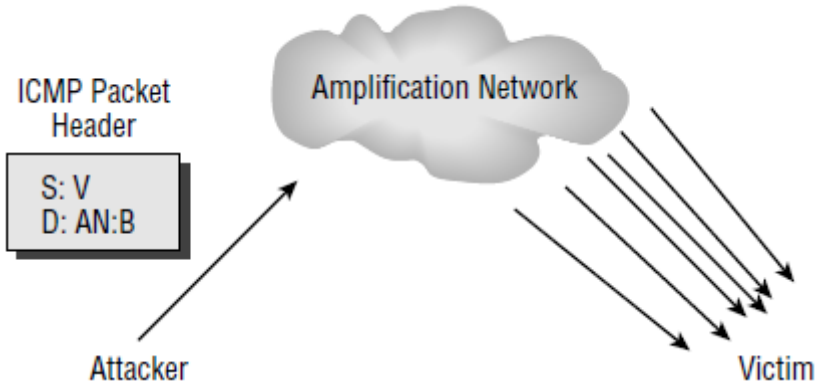


Figura 1. Ataque de Smurf.

La figura muestra los elementos básicos de un ataque Smurf. El atacante envía múltiples paquetes IMCP PING con una dirección de origen falsa como la víctima (V) y una dirección de destino que es el mismo que el difusión de direcciones de la red de amplificación (AN: B). La red de amplificación responde con volúmenes multiplicados de paquetes de eco a la víctima, por lo tanto consumen totalmente el ancho de banda de conexión de la víctima. Otro ataque DoS similar a Smurf es llamado Fraggle. Un ataques fraggle emplea paquetes UDP falsificados en lugar de paquetes ICMP.

Contramedidas para los ataques Smurf incluyen la desactivación de las transmisiones dirigidas hacia los routers fronterizos en toda la red y la configuración de todos los sistemas que caen paquetes ICMP ECHO. Un IDS puede ser capaz de

detectar este tipo de ataque, pero no hay medio para prevenir el ataque que no sea el bloqueo las direcciones de la red de amplificación. Esta táctica es problemático porque la amplificación red suele ser también una víctima.

El ataque de ping de la muerte emplea un paquete ping de gran tamaño. Con herramientas especiales, un atacante puede enviar numerosos paquetes de ping de gran tamaño a una víctima. En muchos casos, cuando el sistema víctima intenta procesar los paquetes, se produce un error, haciendo que el sistema se congele, accidente, o reiniciar el sistema.

El ping de la muerte es más un ataque de desbordamiento de búfer, pero debido a que a menudo resulta en denegar el servicio de un servidor, se considera un ataque DoS.

Contramedidas para el ataque del ping de la muerte incluye mantener al día los parches del sistema operativo y software, codificación adecuada de aplicaciones internas para prevenir desbordamientos de búfer, evitando la ejecución de código con privilegios de System o a nivel de la raíz, y el bloqueo de paquetes de ping en la frontera routers / cortafuegos.

El ataque WinNuke es un asalto especializada contra sistemas Windows 95. Fuera de la banda de datos TCP se envían al sistema de la víctima, que hace que el OS se congele. Contramedidas para este ataque consiste en la actualización de Windows 95 con el parche apropiado o cambiar a un sistema operativo diferente.

El ataque de Stream se produce cuando un gran número de paquetes se envían a numerosos puertos en el sistema de la víctima usando números de código y secuencias aleatorias. El procesamiento realizado por el sistema víctima de intentar dar sentido a los datos dará lugar a una denegación de servicio. Contramedidas incluir un parche en el sistema y el uso de un IDS para el bloqueo dinámico.

El ataque teardrop ocurre cuando un atacante explota un fallo en los sistemas operativos. El fallo existe en las rutinas usadas para el reensamble (es decir, re secuenciar) paquetes fragmentados. Un atacante envía numerosos paquetes fragmentados en formato especial a la víctima, lo que hace que el sistema se congele. Contramedidas para este ataque incluyen parches del sistema operativo y el despliegue de un IDS para la detección y bloqueo dinámico.

El ataque Land se produce cuando el atacante envía numerosos paquetes SYN a una víctima y los paquetes SYN suplantan la misma fuente y destino de dirección IP y el puerto número que la víctima. Esto hace que el sistema piense que envía un paquete de apertura de sesión TCP / IP a sí mismo, lo que provoca un fallo del sistema y por lo general resulta en una congelación del sistema o reinicio del sistema.

Contramedidas este ataque incluyen parches del sistema operativo y el despliegue de un IDS para la detección y bloqueo dinámico. [8]

2.4.3 Ataque de Spoofing.

Spoofing es el arte de fingir ser algo distinto de lo que es. Ataques de suplantación o Spoofing consiste en sustituir fuentes de origen validas como dirección IP y numero el nodo o destinos, con los falsos.

Spoofing está involucrado en la mayoría de los ataques, ya que otorga a los atacantes la capacidad de ocultar su identidad a través de una dirección no real. Spoofing se emplea cuando un intruso utiliza un nombre de usuario y la contraseña robada para acceder al sistema, cuando un atacante cambia la dirección de origen de un paquete malicioso, o cuando un atacante asume la identidad de un cliente para engañar a un servidor en la transmisión de datos controlados.

Existen dos tipos específicos de ataques de suplantación que son suplantación y enmascaramiento. En última instancia, estos ataques son los mismos: alguien es capaz de tener acceso a un sistema de seguro fingiendo ser alguien más. Estos ataques a menudo resultan en una persona no autorizada para el acceso a un sistema a través una cuenta de usuario válido que se ha comprometido. Suplantación se considera un ataque más activo ya que requiere la captura de tráfico de autenticación y la repetición de que el tráfico de tal manera de ganar acceso al sistema. El enmascaramiento es considerado un ataque más pasivo porque el atacante utiliza credenciales previamente robados de cuentas para iniciar sesión en un sistema seguro.

Contramedidas a ataques de suplantación incluyen parches del sistema operativo y el software, lo que permite la comprobación de origen y de destino en los routers, y empleando un IDS para detectar y bloquear ataques. Como regla general, cada vez que el sistema detecta información falsificada, debería registrar elementos de datos en un archivo de registro; entonces el sistema debe eliminar los atacantes. [8].

2.4.4 Ataque de hombre el en medio.

Un ataque man-in-the-middle se produce cuando un usuario malicioso es capaz de inmiscuirse en medio de dos extremos de un enlace de comunicación. Hay dos tipos de ataques man-in-the-middle. Uno consiste en la copia del sniffing del tráfico entre dos partes; esto es básicamente un ataque de sniffer. El otro implica atacantes posicionarse en la línea de comunicación donde actúan como un mecanismo store-and-forward o proxy. El atacante es invisible a ambos extremos de la conexión de comunicación y es capaz de alterar el contenido o el flujo de tráfico. A

través de este tipo de ataque, el atacante puede recopilar credenciales de inicio de sesión o datos sensibles, así como cambiar el contenido de los mensajes intercambiados entre los dos puntos finales.

Para llevar a cabo este tipo de ataque, el atacante debe a menudo alterar la información de enrutamiento y valores DNS, roban direcciones IP o defraudan búsquedas ARP para hacerse pasar por el servidor desde la perspectiva del cliente y hacerse pasar por el cliente desde la perspectiva del servidor. Una consecuencia de un ataque man-in-the-middle es conocida como un ataque de secuestro.

En este tipo de ataque, un usuario malicioso se coloca entre un cliente y el servidor y luego interrumpe la sesión y se hace cargo. A menudo, el usuario malintencionado suplanta al cliente para extraer los datos desde el servidor. El servidor no tiene conocimiento de que se ha producido ningún cambio en el interlocutor. El cliente es consciente de que las comunicaciones con el servidor han cesado, pero hay indicios de por qué las comunicaciones fueron terminadas.

Otro tipo de ataque, un ataque de repetición (también conocido como un ataque de reproducción), es similar a secuestro. Un usuario malintencionado registra el tráfico entre el cliente y el servidor; a continuación, los paquetes enviados desde el cliente al servidor se reproducen o retransmitido al servidor con ligeras variaciones de la dirección IP de fecha y hora y la fuente (es decir, spoofing). En algunos casos, esto permite que el usuario malicioso reinicie un enlace de comunicación con un servidor. Una vez que la sesión de comunicación es reabierto, el usuario malintencionado puede intentar obtener los datos o acceso adicional. El tráfico capturado es a menudo el tráfico de autenticación (es decir, lo que incluye las credenciales de inicio de sesión, como el nombre de usuario y contraseña), pero podría ser también servicio de tráfico de acceso o controlar el tráfico de mensajes.

Repetición de ataques pueden prevenirse mediante el empleo de reglas de secuencia complejas y sellos de tiempo para prevenir paquetes retransmitidos sean aceptadas como válidas.

Contramedidas a este tipo de ataques requieren mejoras en el establecimiento de la sesión, de identificación, autenticación y procesos. Algunos ataques man-in-the-middle se ven frustrados a través de parches del sistema operativo y el software. Un IDS no puede por lo general detectar un man-in-the-middle o secuestrar ataque, pero a menudo puede detectar las actividades anormales que ocurren a través de la comunicación "segura" en enlaces. Sistemas operativos y muchos IDS menudo pueden detectar y bloquear los ataques de repetición. [8]

2.4.5 Ataque de Sniffer.

Un ataque de sniffer (también conocido como un ataque snooping) es cualquier actividad que resulta en la obtención de información de un usuario malicioso sobre una red o el tráfico a través de esa red. Un sniffer es a menudo un programa de captura de paquetes que duplica el contenido de los paquetes que viajan por el medio de red en un archivo. Ataques Sniffer menudo se centran en las conexiones iniciales entre clientes y servidores para obtener iniciar sesión credenciales (por ejemplo, nombres de usuario y contraseñas), claves secretas, y así sucesivamente. Cuando se realiza correctamente, ataques sniffing son invisibles para el resto de entidades de la red y, a menudo preceden a la suplantación de identidad o ataque secuestro. Un ataque de repetición (discutido en la sección anterior) es un tipo de ataque de sniffer.

Contramedidas para prevenir o detener la inhalación ataques requieren mejora en el el control de acceso físico, la vigilancia activa de sniffing de las firmas (como en busca de retardo de paquetes, adicional al enrutamiento de lúpulo, o paquetes perdidos, que pueden ser realizados por algunos IDS), y el uso de tráfico cifrado a través de conexiones de red internos y externos. [8]

2.4.6 Ataque de Spamming.

El spam es el término que describe los mensajes de correo electrónico, grupos de noticias o foros de discusión no deseados. Correo No Deseado puede ser tan inocuo como un anuncio de un vendedor bien intencionado o como maligna como inundaciones de mensajes no solicitados con virus o troyanos adjuntos. Generalmente spam no es una amenaza, sino más bien un tipo de ataque de denegación de servicio. Cuando aumenta el nivel de spam, localizar el acceso a los mensajes legítimos puede ser difícil. Además del valor molestia, correo no deseado consume una parte significativa de los recursos de Internet (en forma de ancho de banda y procesamiento de la CPU), lo que resulta en general más lento el rendimiento de Internet y una menor disponibilidad de ancho de banda para todos.

Ataques de spam implican inundaciones de mensajes no deseados a casilla de correo electrónico de la víctima. Estos ataques causan problemas DoS llenando el espacio de almacenamiento. En casos extremos, los ataques de spam pueden causar un congelamiento del sistema e interrumpir la actividad de otros usuarios en la misma subred o ISP. Contramedidas ataque spam incluyen el uso de filtros de correo electrónico, servidores proxy de correo electrónico, y IDS para detectar, seguimiento, y poner fin a los intentos de la inundación de spam.

Contramedidas ataque spam incluyen el uso de filtros de correo electrónico, servidores proxy de correo electrónico, y IDS para detectar, seguimiento, y poner fin a los intentos de la inundación de spam. [8]

2.4.7 Crackers.

Los Crackers son usuarios maliciosos decididos a emprender un ataque contra una persona o sistema. Los crackers pueden estar motivados por la codicia, el poder o reconocimiento. Sus acciones pueden resultar en propiedad robada (datos, ideas, etc.), sistemas de movilidad reducida, seguridad comprometida, de opinión pública negativa, acción de pérdida de mercado, reducción de la rentabilidad, y la pérdida de productividad.

Un término comúnmente confundido con cracker es hackers, quienes son entusiastas de la tecnología sin malas intenciones. Muchos autores y los medios de comunicación a menudo usan el término hacker cuando en realidad son cuestiones relacionadas con crackers.

Para evitar que se ejecuten ataques DoS se requiere de esfuerzo vigilante para mantener sistemas de parcheado y configurado correctamente. IDS y sistemas honey pot a menudo ofrecen medios para detectar y recoger pruebas para procesar a los crackers una vez que hayan llegado al perímetro controlado. [8]

2.5 Control de Acceso.

La gestión de control de acceso de un sistema implica un conocimiento profundo del sistema y ataques maliciosos comunes. El monitoreo de un sistema proporciona la base para la rendición de cuentas de usuarios autenticados. Los trails de auditoría y los archivos de registro proporcionan detalles acerca de usuarios válidos y actividades no autorizadas, así como la estabilidad y el rendimiento del

sistema. El uso de un IDS puede simplificar el proceso de examinar la abundante cantidad de datos recogidos a través del monitoreo.

Hay dos tipos de IDS: basados en Host y red. IDS basado en host es útil para la detección de intrusiones específicas sobre sistemas individuales. Un IDS basado en red es útil para detectar actividad global de la red corporativa. Hay dos tipos de métodos de detección empleados por IDS: basado en el conocimiento y basada en el comportamiento. Un IDS basado en el conocimiento utiliza una base de datos de firmas de ataques a detectar intentos de intrusión. Sin embargo, no reconoce los nuevos métodos de ataque. Una basada en el comportamiento IDS utiliza patrones de actividad aprendió a detectar eventos anormales, pero produce numerosos falsos positivos hasta que haya adquirido los conocimientos suficientes sobre el sistema que está supervisando.

Honey Pots, cajas de arena entre otras, son herramientas útiles para la prevención de las actividades maliciosas que se produzcan en la red real, mientras se atrae al intruso a permanecer el tiempo suficiente para reunir pruebas para el procedimiento.

Los scanners de vulnerabilidades son herramientas de detección basada en firmas que exploran un sistema para obtener una lista de vulnerabilidades conocidas. Estas herramientas producen informes que indican las vulnerabilidades descubiertas y proporcionar recomendaciones para mejorar la seguridad del sistema.

Las pruebas de penetración son un mecanismo útil para probar la fuerza y la eficacia de medidas de seguridad desplegadas y la política de seguridad de una organización. Se requiere de una previa aprobación antes de realizar una prueba de penetración.

Existen numerosos métodos de ataques que cometen intrusos en contra de los sistemas. Algunos de los ataques más comunes son la fuerza bruta, diccionario, denegación de servicio, spoofing, hombre intermedio, spam y ataques de sniffing. Cada tipo de ataque utiliza diferentes medios para infiltrarse, daño o sistemas de interrumpir y cada uno tiene contramedidas únicas para prevenirlos que han sido estudiadas en líneas anteriores.

2.6 Fases para realizar un Hackeo Ético

Pariendo de la Definición de su término en inglés Ethical Hacking, consiste en explotar las vulnerabilidades existentes en el sistema de estudio o interés, valiéndose de herramientas de software que permiten “penetrar” a la red objetivo de manera de verificar y evaluar la seguridad de los diferentes sistemas, redes, aplicaciones web, bases de datos, servidores, etc. Para realizar un hackeo ético se deberá definir un procedimiento a partir del cual se extraerá una serie de conclusiones y recomendaciones, este procedimiento consiste en un conjunto de fases el cual deberá seguir un orden exacto para obtener resultados determinantes [8].

2.6.1 Fase de reconocimiento

En esta fase se intenta investigar todo lo relacionado con el objetivo del ataque, se debe realizar un análisis minucioso del entorno previo al ataque, acudiendo a herramientas que permitan obtener la mayor cantidad de información e ingeniería social.

Finalmente en esta etapa debemos aplicar sniffing o herramienta similar, para obtener mediante la captura de tráfico ciertos datos de interés [8].

2.6.2 Escaneo, análisis y evaluación de vulnerabilidades.

En esta etapa se buscan vulnerabilidades que se puedan explotar y se analizan puertos y formas que permitan ingresar a la red y sistemas objetivos, esta es la etapa previa a la ejecución del ataque. Dentro del análisis que se efectúa en esta etapa de análisis de vulnerabilidades se descarta las que correspondan a fallas temporales o de cierta forma no muy convincente concentrándose en aquellas que sean totalmente explotables [8].

2.6.3 Ataque o prueba de penetración.

De acuerdo a la definición, se considera ataque al proceso de acceder a un equipo objetivo y la manipulación de este sin consentimiento. Sin embargo deberá tomarse en cuenta que un ataque no tiene como único objetivo el acceso a un equipo si no a la información que se dirige hacia él, como por ejemplo un ataque de hombre en el medio el cual puede ser ejecutado sin tener que estar el atacante en el host objetivo, de hecho la mayoría de ataques se ejecutan sin la presencia del atacante en el host objetivo [8].

2.6.4 Mantenimiento de acceso.

El objetivo de esta fase es mantener los privilegios obtenidos procurando no ser descubiertos por el propietario o atacantes [8].

2.6.5 Eliminación de pruebas.

Como su nombre lo sugiere, el objetivo de esta fase es eliminar cualquier tipo de rastro que involucre al atacante, aquí los logs de los sistemas juegan un papel determinante.

Al finalizar estas fases se tiene un informe detallado que contiene las pruebas realizadas, los problemas detectados y las posibles soluciones, además debe contener los tipos de ataques que son vulnerables entre los que tenemos.

De tipo Remoto, cuando los accesos son desde el Internet, de tipo social debido a la manipulación de la información extraída a los empleados, de tipo físico cuando se trata de hardware y servicios obligatorios como copias de seguridad; finalmente se debe informar si se tiene la debilidad de ser atacados por miembros internos de la organización obteniendo privilegios no autorizados o partiendo de algunos privilegios existentes.

Es importante además indicar que las evaluaciones de seguridad se pueden hacer en base a las siguientes técnicas.

Evaluación de Caja Negra, Blanca o Gris, en donde la primera ignora el funcionamiento interno de un sistema, la segunda se parte de un conocimiento completo de la infraestructura de estudio y la última examina la infraestructura de manera interna [8].

2.7 Vulnerabilidades.

Una vulnerabilidad aplicado a la vida cotidiana se asemeja con ciertos errores, descuidos o despistes que tenemos los seres humanos como, olvidar cerrar con llave una la puerta de una casa o peor aún dejar la llave puesta en la puerta de la casa; esto definitivamente no implica que se va a efectuar un robo de las cosas que estén dentro de la casa, pero es mucho más fácil perpetuar un robo que si no estuviera la llave colocada o que la puerta este con llave, la vulnerabilidad por tanto

esta en el hecho de no cerrar la puerta con llave o el hecho de tener la llave puesta en la puerta y un ladrón podría aprovecharse de este hecho si lo llegara a detectar.

Una vulnerabilidad además desde que se manifiesta por primera vez hasta que se solucione necesita pasar por una serie de etapas que parte desde su creación ya sea esta voluntaria o no, descubrimiento por medio de testeo realizado por el desarrollador o una empresa externa, publicación de la existencia de la vulnerabilidad para su rápida corrección y para conocimiento de los usuarios, que estos sean conscientes del riesgo al que se exponen, de tal forma que quede registrado y publicado en las bases de datos de organismos como “Base de Datos de Vulnerabilidades de USA” o Security Focus.

La siguiente fase es la explotación de la misma por medio de Exploits que no es más que un pequeño código que hacen uso de un error o vulnerabilidad para causar un comportamiento inadecuado o inesperado del software o hardware del equipo [8].

Una vez que se ha explotado esta vulnerabilidad, es posible el desarrollo de una actualización también llamada parche que corrija de forma efectiva y en el mejor de los casos corrija de manera permanente el fallo existente; este proceso dura algún tiempo, el cual puede ser aprovechado de sobre manera por los atacantes sin embargo se desarrollan recomendaciones del fabricante para descartar ataques durante este tiempo.

Siendo el objetivo final la solución de este agujero de seguridad creado y una vez obtenido el mismo se deberá difundirlo mediante actualizaciones [8].

2.8 Clasificación de las vulnerabilidades

Es importante definir los elementos de un sistema informático que se quiere defender de un atacante y sobre los que pueden encontrarse vulnerabilidades, a continuación se describen a cada uno de estos elementos.

- Elementos de Hardware y Software. (Los más sensibles a agujeros de seguridad).
- Datos. (consecuencia directa de un fallo hardware/software pero también pueden ser protagonistas de la vulnerabilidad en casos de intercepción de datos)
- Elementos Varios. (Personas o infraestructuras que pueden ser afectados)

También, las vulnerabilidades en función de su origen pueden ser las siguientes [8]:

- Vulnerabilidades basadas en el planteamiento de políticas de seguridad del sistema.
- Vulnerabilidades basadas en fallas tanto en la planificación como en la programación final del software que permitan posible puertas traseras
- Vulnerabilidades basadas en el desconocimiento y falta de responsabilidad en el uso de los equipos que combinadas con una mala configuración de los sistemas provocan una indisponibilidad de los sistemas facilitando un ataque.
- Vulnerabilidad de día cero, la cual se caracteriza por aprovechar vulnerabilidades desconocidas por los creadores y los usuarios de las aplicaciones, es por tanto recién descubierta la cual no tiene solución.

Una vez determinado los elementos susceptibles a ser vulnerados y clasificados de acuerdo con su origen, se describe a continuación algunas de las vulnerabilidades descubiertas en función de sus causas y efectos que provocan [8].

- Vulnerabilidad de validación de entrada.
- Vulnerabilidad de salto de directorio.
- Vulnerabilidad de seguimiento de enlaces.
- Vulnerabilidad de inyección de comandos en el sistema operativo:
- Vulnerabilidad de ejecución de código cruzado
- Vulnerabilidad de inyección SQL2.7.7 Vulnerabilidad de inyección de código
- Vulnerabilidad de error de búfer
- Vulnerabilidad por formato de cadena
- Revelación o filtrado de información.
- Gestión de credenciales
- Permisos
- Problema de autenticación
- De tipo criptográfico
- Falsificación de peticiones en sitios cruzados
- Condición de carrera
- Error gestionando recursos
- Error de diseño

2.9 Vectores de Ataque.

Es el método que realiza una amenaza para atacar un sistema, por tanto se elige en función de varios procedimientos previos, se lo define también como el éxito

de las fases de reconocimiento y escaneo y análisis de vulnerabilidades que describimos anteriormente.

La búsqueda de un vector de ataque comienza con la elección de una organización destinatario de un ataque, que por motivos de seguridad del presente trabajo no ha sido realizada con datos reales; ya que esta información para un cracker con malas intenciones esta información será de vital importancia.

Se describen a continuación una serie de herramientas que permitirán obtener información pública sobre la organización destinatario de un ataque que son [8]:

2.9.1 Nombre del Dominio

2.9.2 Dirección IP

2.9.3 Servicios TCP y UDP disponibles, así como sus puertos disponibles.

2.10 Análisis de Vulnerabilidades mediante Hackeo Etico.

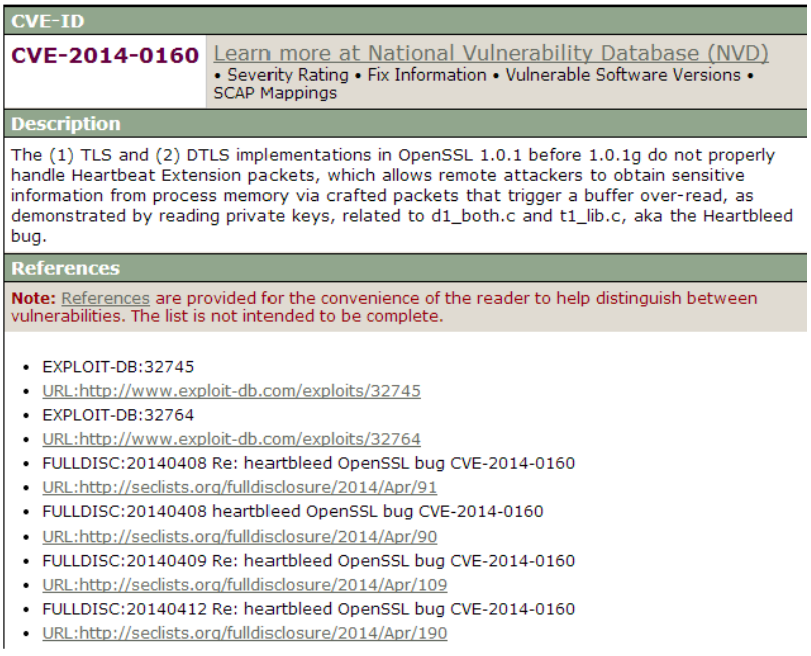
Por definición el análisis de vulnerabilidades es “Utilizar una herramienta o un conjunto de ellas para rastrear y eliminar vulnerabilidades en materia de seguridad sobre aplicaciones que estén siendo ejecutadas por el sistema o sobre la configuración de este [8]”

El primer paso es utilizar una base de datos especializada, las cuales hay varias, una de ellas es www.securityfocus.com en la cual podemos estar al día en cuanto al vulnerabilidades que se van detectando a lo largo del tiempo, sin embargo la búsqueda en este sitio es algo tedioso por lo que existen otras bases de datos como la ofrecida por CVE, que es un diccionario de vulnerabilidades que han sido estudiados y nos ofrece una gran cantidad de referencias y enlaces directos a

exploits que atacan a dicha vulnerabilidad como por ejemplo si buscamos heartbleed, que es una vulnerabilidad puesta al descubierto por open SSL V 1.0.1F, que permite al atacante leer memoria de servidores y clientes con las consecuencias que esto puede producir, a continuación se muestra la información presentada por CVE.

Podemos observar claramente el efecto que provoca esta vulnerabilidad así como las versiones en las que existe esta problemática, también en las referencias tenemos enlaces a exploits que atacan la vulnerabilidad indicada y cuya información se encuentra en otra base de datos de referencia www.exploit-db.com.

Una vez que conocemos sobre vulnerabilidades, necesitamos una herramienta que nos permita escanear la existencia de las mismas [8].



CVE-ID

CVE-2014-0160 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:32745
- URL:http://www.exploit-db.com/exploits/32745
- EXPLOIT-DB:32764
- URL:http://www.exploit-db.com/exploits/32764
- FULLDISC:20140408 Re: heartbleed OpenSSL bug CVE-2014-0160
- URL:http://seclists.org/fulldisclosure/2014/Apr/91
- FULLDISC:20140408 heartbleed OpenSSL bug CVE-2014-0160
- URL:http://seclists.org/fulldisclosure/2014/Apr/90
- FULLDISC:20140409 Re: heartbleed OpenSSL bug CVE-2014-0160
- URL:http://seclists.org/fulldisclosure/2014/Apr/109
- FULLDISC:20140412 Re: heartbleed OpenSSL bug CVE-2014-0160
- URL:http://seclists.org/fulldisclosure/2014/Apr/190

Figura N.-2. Ejemplo de una Vulnerabilidad reportada por el Diccionario CVE.

Existe una herramienta gratuita utilizada por mucho tiempo para realizar un escanner de vulnerabilidades llamada Nessus, sin embargo desde hace algunos

años requiere de una licencia para funcionar. Adicionalmente existe una herramienta open source llamada OpenVAS que también ofrece servicios de escaneo y administración de vulnerabilidades.

2.11 Amenazas de Seguridad Comunes Actualmente.

Las amenazas más comunes a las que se ven expuestas continuamente las redes de datos y equipos informáticos de acuerdo con los reportes de Seguridad de Check Point son los Bots (equipos robots) y amenazas avanzadas persistentes que no son más que un sofisticado método a largo plazo de conseguir un objetivo específico predeterminado las cuales se describen a continuación [2].

2.11.1 Amenazas Avanzadas Persitentes

En los APT **Advanced Persistent threats,** la primera acción es realizar reconocimientos para reunir información sobre el objetivo, luego se ejecuta una intrusión inicial en la red destino de manera de abrir una puerta trasera y permanecer permanentemente en la red, esto se logra gracias a una máquina infectada con un bot, que permite la interacción entre el atacante y el computador infectado sin ser detectado, esto mejora sustancialmente de acuerdo con la cantidad de máquinas infectadas con bots.

Con esto el atacante ya tiene alcanzado su objetivo y desde este momento puede hacer uso de todos los computadores infectados y por supuesto de la red para recoger datos o causar el daño previsto de manera remota mientras mantiene la persistencia sin un método que impida hacerlo [8].

2.11.2 Bots

Una de las "*amenazas de red más significativa actualmente son las Botnet o redes de bots, un bot es un software malicioso que invade e infecta a un equipo permitiendo un que los cibercriminales controlen de manera remota al o los equipos infectados"* [2].

Una vez que un equipo se encuentre infectado con un bot, se busca ejecutar actividades ilegales como por ejemplo hurto de información, difusión de spam, distribución de malware y ataques como por ejemplo denegación de Servicio sin que el usuario del equipo se entere ya que este software no es detectado.

Existen 2 tendencias principales en el actual panorama de amenazas que son generados por bots, siendo la primera opción la creciente industria de delincuencia informática con fines de lucro.

La segunda tendencia hace referencia a la difusión masiva de prácticas ideológicas o políticas que se dirigen a personas y organizaciones para promover una causa política o llevar a cabo una campaña de guerra cibernética.

A diferencia de los virus y otros malwares estáticos tradicionales que en código y en forma permanecen estáticos, los botnets por naturaleza son dinámicos y pueden rápidamente cambiar su forma y patrones de tráfico.

Herramientas anti bot se venden en línea a bajos costos sin embargo a las empresas a que atacaron les costaron millones de dólares. Los bots se han convertido en un gran problema en la actualidad.

De acuerdo con una reciente investigación el 63% de un universo finito de empresas investigadas a nivel mundial posee una red de bot incrustada en la organización sin que su personal de TI lo conozca [2].

Existe miles de bots en la actualidad, la siguiente tabla presenta los botnet más importantes encontradas en investigaciones recientes.

Familia de Botnet	**Actividad Maliciosa**
Zeus	Roba credenciales de banca online
Zwangi	Presenta mensajes publicitarios no deseados
Saliti	Auto propagación de Virus
Kuluoz	Ejecución remota de archivos maliciosos
Juasek	Acciones maliciosas remotas Shell abierto, buscar, crear, borrar archivos, etc
Papras	Roba información financiera y obtiene acceso remoto

Tabla N.-1. Algunos tipos de Botnets con su actividad.

2.11.3 Virus

De acuerdo con el Reporte Anual de la Marca Check Point existen variedad de puntos de entrada para vulnerar los sistemas de seguridad en una organización, vulnerabilidades basadas en navegadores, teléfonos móviles, archivos adjuntos maliciosos, medios extraíbles entre otros. "*Adicionalmente, la explosión de las aplicaciones Web 2.0 y las redes sociales que actualmente son utilizadas a nivel comercial, son blancos para atraer a los hackers quienes encuentran en esto una gran oportunidad para atraer a sus víctimas a hacer un clic en enlaces a sitios y anuncios maliciosos que traen malware como virus, gusanos, spyware, adware, troyanos"*, etc [2].

De acuerdo con el mismo reporte, en el 75% de las organizaciones existe al menos un computador que accede a sitios maliciosos. De igual manera en más del 50% de organizaciones al menos 5 equipos descargan malware.

En estas investigaciones realizadas en un universo finito de organizaciones a nivel mundial, la mayoría de malware está ubicado en USA con un 71%, seguido de Canadá 8%, Reino Unido 4%, Alemania, Israel, Turquía 3%, China, Francia y Eslovaquia con 2%.

Una protección de Antivirus es un buen método de protección contra malware, sin embargo de acuerdo a investigaciones el 23% de los equipos de una organización no se encuentran actualizados el antivirus diariamente, esto implica que estos equipos están expuestos a virus recientes. De manera similar, el 14% de los equipos de una organización ni siquiera ejecutan un antivirus, permitiendo potencialmente malware en los equipos.

2.11.4 Fallos de Seguridad

Una labor indispensable en las organizaciones es vigilar que todos los sistemas totalmente actualizados, en muchas ocasiones, una vulnerabilidad superada hace algunos años, aún pueden ser utilizada para penetrar en los sistemas de grandes y pequeñas organizaciones que no han actualizado sus sistemas con los últimos parches de software.

El gran número de vulnerabilidades descubiertas cada año es abrumadora, de acuerdo con el reporte anual de la marca Check Point, existen más de 5.000 nuevas formas para que los piratas informáticos para causar daños y sistemas de acceso descubiertas desde del año 2012 y muchas más vulnerabilidades sin descubrir utilizados activamente por los ciber criminales. El siguiente Gráfico muestra los

productos más utilizados por casi todas las organizaciones de todo el mundo los cuales son también los más vulnerables, “Oracle, Apple y Microsoft son los principales vendedores vulnerables durante el 2012, mientras que para el 2013 Oracle, Cisco e IBM lideran la cantidad de vulnerabilidades” [2].

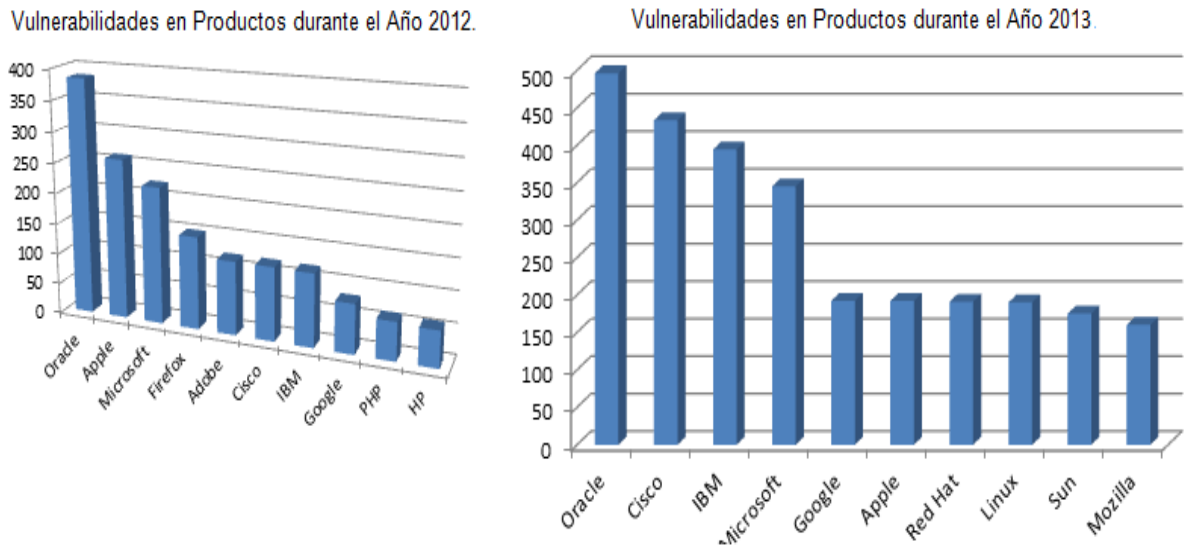


Figura N.-3. Productos Utilizados en Organizaciones con su cantidad de Vulnerabilidades registradas en 2012 y 2013.

Además la investigación revela que los eventos de seguridad relacionados con los productos de Microsoft son más frecuentes frente a otros tipos de software, como Adobe, Apple, etc.

2.11.5 Ataques

En la actualidad los hackers están usando diversas técnicas de ataques conocidas como multivectoriales. El gráfico muestra algunos vectores de ataque más populares de acuerdo con el porcentaje de organizaciones que fue víctima de los mismos, se destaca entre ellos Memory Corruption, Buffer Overflow y Denial of

Service en el 2012, mientras que para el 2013 varía el orden de los mismos como se muestra en la siguiente figura.

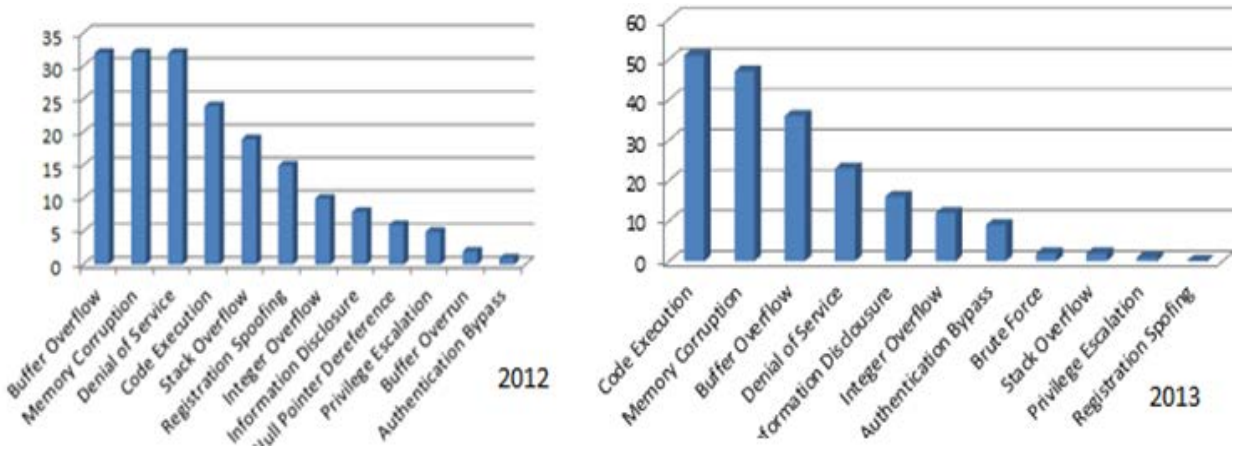


Figura N.-4 Vectores de Ataque más populares durante 2012 y 2013

2.12 Recomendaciones de Seguridad.

De acuerdo con el último reporte de Check Point, debido a que las amenazas son cada vez más sofisticadas, los desafíos de seguridad son mayores para maximizar la seguridad de la red de la organización, se necesita un mecanismo de protección de varios niveles para asegurarlo contra los diferentes vectores de amenazas de la red:

1. *Anti-virus para identificar y bloquear el malware.*
2. *Anti-bot para detectar y prevenir robots.*
3. *IPS para prevenir de forma proactiva intrusiones Web.*
4. *Control y Filtrado de URL, control de aplicaciones para evitar el acceso a sitios web de alojamiento y propagación de malware.*
5. *Seguridad Inteligente en tiempo real y la colaboración global.*
6. *Monitoreo inteligente que proporcione análisis de datos proactivos* [2].

2.12.1 Anti-virus para identificar y bloquear el malware.

Una organización requiere una solución anti-malware que analice los archivos que entra en la red y decida, "*en tiempo real si los archivos están infectados por el malware*". [2]

Esta solución debe evitar que los archivos maliciosos infecten el interior la red y también "*evitar el acceso a sitios web infestados con malware que tratan de ejecutar descargas no autorizadas"* [2].

2.12.2 Anti-bot para detectar y prevenir robots.

Una protección contra bots consta de dos fases: la detección y el bloqueo. Para detectar un robot en una red, se necesita de un mecanismo de descubrimiento de bot multitarea que cubra todos los aspectos de un comportamiento bot, para esto se debe "*incluir un mecanismo de reputación que detecte la IP, URL y direcciones DNS que el operador remoto utiliza para conectarse a redes de bots",* además del envío de correo no deseado, fraudes en un clic, y auto-distribución. Esta protección detecta los patrones de comunicación únicos y protocolos de cada familia de botnet. [2]

La segunda fase después del descubrimiento de equipos infectados es bloquear la comunicación bot de salida a los servidores de mando y control. *"Esta fase neutraliza la amenaza y asegura de que los agentes de bots no puedan enviar información"* sensible y no reciban instrucciones de actividad maliciosa. Por lo tanto, los problemas relacionados a bot son solucionados de inmediato. Este "enfoque permite a las organizaciones mantener la continuidad de trabajo, usuarios pueden trabajar con normalidad, sin saber que una comunicación bot especifica está siendo bloqueada y la organización está protegida con impacto en la productividad". [2]

Debido al apalancamiento de malware realizado por cibercriminales, bots y otras formas de amenazas frecuentemente son dirigidos a múltiples sitios y organizaciones para aumentar la probabilidad del éxito de un ataque, las empresas deben luchar ante estas amenazas compartiendo información sobre las mismas de forma de mantenerse a la vanguardia de las amenazas modernas, por tanto deben colaborar y compartir los datos de amenazas. Sólo de manera conjunta pueden hacer de la seguridad más fuerte y más eficaz.

2.12.3 IPS para prevenir de forma proactiva intrusiones Web.

La prevención de intrusiones de carácter obligatorio en la lucha con los diferentes vectores de ataque cibernético, *"una solución IPS se requiere para la inspección del tráfico profunda con el fin de prevenir intentos malintencionados de violación de la seguridad y tener acceso a activos de la organización*". Una solución adecuada de IPS proporcionará las siguientes características:

- Validación de Protocolo y detección de anomalías.
- Identificar y evitar que el tráfico que no cumpla con los estándares de protocolo y pueda generar un mal funcionamiento del dispositivo o la problemas de seguridad.
- Prevenir la transmisión de cargas desconocidas que pueden explotar una vulnerabilidad específica.
- Prevenir la comunicación excesiva que puede desencadenar un ataque de Denegación de servicio (DoS).

Una visión clara de los sucesos y tendencias de seguridad es otro componente clave en la lucha contra la ciberdelincuencia, un administrador de

seguridad debe tener una clara y constante comprensión de la situación de seguridad de red para ser conscientes de las amenazas y los ataques a los que se enfrenta día a día.

Esta comprensión requiere de una solución de seguridad que puede suministrar una visión general de alto nivel de las protecciones de seguridad y hacer hincapié en la información crítica y los ataques potenciales.

La solución también debe permitir la capacidad de producir investigaciones profundas sobre eventos específicos. La capacidad de tomar acción inmediata de acuerdo a esta información es otra característica importante que permite la prevención en tiempo real y bloqueo de ataques o de forma proactiva para las amenazas futuras. La solución de seguridad debe permitir flexibilidad y debe ser intuitiva de manera de permitir su gestión oportunamente, simplificar el análisis de amenazas y reducir tiempos operacionales. [2]

2.12.4 Control y Filtrado de URL, control de aplicaciones para evitar el acceso a sitios web de alojamiento y propagación de malware.

El control de los sitios de acceso, así como el filtrado de sitios web calificados como maliciosos por diferentes firmas debe ser bloqueado, sitios catalogados como anonimizer, entre otros que propaguen malware y saturación a la red. [2]

2.12.5 Seguridad Inteligente en tiempo real y la colaboración global.

Aplicar un sistema de Seguridad Inteligente en tiempo real implica mantener el sistema de seguridad actualizado de definiciones de firmas de atacantes mediante colaboración a nivel global. [2]

2.12.6 Monitoreo inteligente que proporcione análisis de datos proactivos.

En un entorno de frecuentes amenazas y en constante cambio, las protecciones deben evolucionar frente a las amenazas. Los productos de seguridad no deben únicamente manejar con eficacia los últimos malware, vulnerabilidades y exploits, sino deben ser capaces de llevar a cabo una investigación exhaustiva y proporcionar frecuentes actualizaciones de seguridad.

Un buen servicio de seguridad se basa en:

- Investigación interna del fabricante y la obtención de datos a partir de múltiples fuentes.
- Actualizaciones de seguridad frecuentes de todas las tecnologías pertinentes incluyendo IPS, Anti-Virus y Anti-Bot.
- Soporte accesible y apoyo para responder a preguntas específicas del entorno del cliente. [2]

2.13 Aplicaciones que representan un peligro a la Seguridad.

Las reglas del juego han cambiado, las aplicaciones de Internet que eran consideradas como un pasatiempo o un medio para ver las imágenes de últimos viajes de nuestros amigos y de ver películas divertidas. *"Hoy, las aplicaciones Web 2.0 se han convertido en herramientas esenciales de las organizaciones en la empresa moderna*". Las comunicaciones con colegas, clientes y socios, el hecho de compartir información con otros, y conseguir las últimas noticias, opiniones y puntos de vista.

"Herramientas basadas en Internet como Facebook, Twitter, WebEx, LinkedIn y YouTube para nombrar unos pocos, se están volviendo más y más frecuentes en las empresas y hay que reconocerlos como necesarios para el establecimiento de negocios actualmente".

Es importante discutir los riesgos generales de las aplicaciones web 2.0 y su infraestructura, seguido por un enfoque en aplicaciones específicas que cuentan en uso actualmente en las organizaciones, entre las que destacamos [2].

2.13.1 Aplicaciones Web.

Como la tecnología evoluciona también lo hacen los problemas de seguridad. Herramientas como el Internet también introducen nuevos riesgos de seguridad. "*Un número de aplicaciones útiles de Internet se utilizan como herramientas de ataque contra organizaciones y generan una brecha en la seguridad de la red".*

Aplicaciones como almacenamiento de archivos y recursos compartidos, Uso compartido de archivos Peer-to-Peer, herramientas administrativas y remotas, Medios Sociales entre otros se han utilizado para provocar ciertos exploits a las organizaciones.

Hay una gran variedad de plataformas y aplicaciones que son utilizados por razones personales o de negocios. Cada organización tiene que ser consciente de lo que los empleados están utilizando y con qué propósitos, y luego definir su propia política de Internet.

"En el 91% de las organizaciones, los usuarios se encuentran usando aplicaciones para evadir la seguridad, se esconden identidades, fuga de datos o incluso introducen malware sin su conocimiento" [2].

2.13.2 Aplicaciones P2P. (Agujero de Seguridad).

Las aplicaciones "*Peer-to-Peer (P2P) son usados para compartir archivos entre usuarios. P2P cada vez más son utilizados por los atacantes para distribuir malware entre los archivos compartidos*". Lo que se logra al utilizar este tipo de aplicaciones esencialmente es abrir una puerta trasera a las redes.

No solo permiten a los usuarios compartir carpetas que puedan desviar los datos sensibles, sino que también los usuarios de las organizaciones utilizan el internet de las organizaciones de forma ilegal a través de redes P2P.

De acuerdo con investigaciones el uso de aplicaciones P2P está siendo utilizado por más de la mitad de las organizaciones, (61%) resultaron ser el uso de aplicaciones P2P. Las más importantes son los BitTorrent. [2]

2.13.3 Aplicaciones Anónimas.

Un Anonymizer (o un proxy anónimo) es una herramienta que intenta hacer que la actividad del usuario en Internet sea imposible de rastrear. *"La aplicación utiliza un servidor proxy Anonymizer que actúa como una máscara de privacidad entre un equipo cliente y el resto de Internet. El usuario Accede a Internet, ocultando información personal mediante la ocultación la información de identificación del equipo cliente y el destino que el usuario está tratando de alcanzar*". [2]

Aplicaciones Anonymizer son utilizadas para eludir las políticas de seguridad que son esencialmente en torno a las identidades de los usuarios y las direcciones URL de destino o sitios. Mediante el uso de Anonimizadores, el usuario parece estar en una dirección IP diferente y tratar de acceder a diferentes destinos no prohibitivos por la política de seguridad de la organización.

En algunos casos, Anonimizadores también podrían ser utilizados para ocultar la actividad delictiva. De acuerdo con investigaciones el 43% de las organizaciones utilizan al menos una aplicación Anonymizer por un empleado, siendo la herramienta Tor la más utilizada. 86% de las organizaciones en las que se encontró el uso Anonymizer afirmaron que se trataba de un uso no legítima en conflicto con las directrices y políticas de seguridad. El uso de las aplicaciones Anonymizer es más popular en América que en otros países [2].

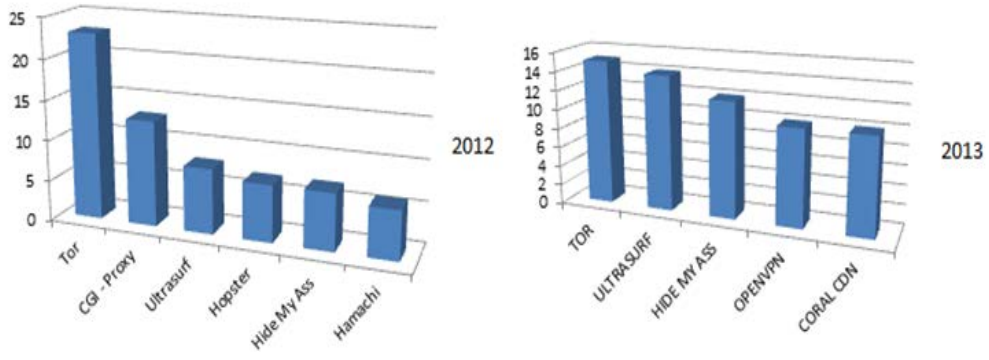


Figura N.-5 Aplicaciones Anonymizer populares durante 2012 y 2013.

Un ejemplo de cómo funciona UltraSurf que es un sofisticado anonimizador, lo tenemos a continuación:

Funciona como un cliente proxy, la creación de un túnel de HTTP encriptado entre el ordenador del usuario y un grupo de servidores proxy o intermediarios, lo que permite a los usuarios pasar por alto los firewalls y la censura.

UltraSurf tiene un diseño muy resistente que "*evade el descubrimiento de servidores proxy que incluye un archivo de caché de direcciones IP del servidor proxy, peticiones DNS, que devuelven direcciones IP codificadas de servidores proxy, documentos cifrados en Google Docs y no modificable, lista de IPs del*

servidor proxy integradas en el programa". Estas técnicas hacen aún más difícil de ser detectado por dispositivos de seguridad [2].

2.13.4 Herramientas de administración remota.

Las Herramientas de administración remota son una solución de problemas cuando se utiliza por administradores de red y personal de helpdesk. Sin embargo, varios ataques en los últimos años han sido posibles gracias a estas herramientas que permiten controlar de forma remota equipos infectados, además infiltrarse a redes, iniciar las pulsaciones de teclado, o robar información confidencial.

Actualmente estas herramientas de administración remotas son importantes en las aplicaciones de negocios y no deben ser bloqueadas por personal de TI sin embargo, su uso debe ser supervisado y controlado para evitar malos usos potenciales.

Según investigaciones el 81% de las organizaciones encuestadas están usando al menos una aplicación de administración remota, siendo Microsoft RDP es el más popular. A continuación se presenta una gráfica que representa el porcentaje de utilización de este tipo de herramientas [2].

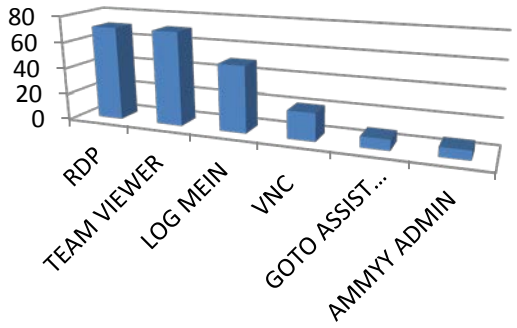


Figura N.-6 Herramientas de Gestión Remota y su porcentaje de uso en 2013

2.13.5 Archivos Compartidos.

La información confidencial se puede conseguir en las manos equivocadas mediante el intercambio de archivos confidenciales. Investigaciones demuestran que representa un alto riesgo el Almacenamiento de archivos y compartir aplicaciones que pueden causar fugas de datos o infecciones de malware sin el conocimiento del usuario.

"De acuerdo con investigaciones el 80% de las organizaciones tienen por lo menos un almacenamiento de archivos o un archivo de uso compartido de aplicaciones que se ejecutan en su red, siendo el 69% que hacen uso de Dropbox, seguido con el 51% Windows Live Office" [2].

2.13.6 Aplicaciones de alto Riesgo.

Las organizaciones industriales y gubernamentales son las que poseen más usuarios de aplicaciones de alto riesgo. "*Hay casos donde el uso de algunas de estas aplicaciones tiene un uso legítimo, por ejemplo, el uso de herramientas de administración remota para mesa de ayuda".* Por todo lo expuesto, el uso de este tipo de aplicaciones debe ser monitoreado constantemente [2].

2.13.7 Redes Sociales

Debido al aumento de la popularidad de las redes sociales, nuevos desafíos se introducen a las organizaciones.

Ciertas aplicaciones de redes sociales podrían dañar la reputación de una organización ya que suelen publicarse información sensible a través de ciertos

usuarios, lo que causa la pérdida de la ventaja competitiva o en su defecto pérdida financiera. Los hackers están aprovechando ingeniería social y nuevas técnicas de hacking para impulsar la actividad botnet. Videos incrustados y enlaces en las páginas de redes sociales se están convirtiendo en lugares populares para los hackers para integrar malware. "*Adicionalmente a los riesgos de seguridad las aplicaciones de redes sociales crean un grave problema de red acaparando ancho de banda. Facebook es sin duda la red social más visitada seguida de Twitter y LinkedIn"* [2].

2.13.8 Facebook.

Uno de los ataques realizado por Hackers utilizando Twitter y Facebook como técnica de ingeniería social para distribuir contenido malicioso tuvo lugar en agosto de 2012 el mismo que fue registrado y dado a conocer en diversos medios de comunicación [2].

El uso de una popular cuenta de twitter fue comprometida, el hacker envió mensajes directos a todos los seguidores de la cuenta hackeada con cierto mensaje con enlace a una dirección URL a una aplicación de Facebook que requiere credenciales de Twitter. En donde la pantalla de inicio de sesión es realmente un servidor web de propiedad por el hacker que se utiliza para recoger credenciales del destinatario. Usando estas credenciales, el hacker puede ahora repetir el mismo proceso con la nueva cuenta hackeada para llegar fácilmente a recoger más contraseñas. Entonces puede utilizar estas credenciales robadas con otros servicios tales como Gmail, Facebook, etc, pero peor que eso, puede utilizar para acceder a las cuentas bancarias, o incluso a servicios como SalesForce y otros [2]. .

2.14 Seguridad en Redes

Es un nivel de Seguridad que garantiza un adecuado funcionamiento de los equipos dentro de una red de computadores y que los usuarios de estos equipos tengan los derechos que les han sido otorgados entre los que se pueden destacar.

- Impedir el acceso a red de personas no autorizadas con fines malignos y autorizar de acceso mediante un sistema de autenticación (AAA) y en canales seguros (VPN) para acceso remoto.
- Impedir que usuarios realicen tareas involuntarias que involucren problemas en el sistema.
- Garantizar el acceso a los datos mediante el conocimiento previo de errores.
- Asegurar la continuidad de los servicios.

Existen Soluciones de Control de Acceso a Red llamados NAC de tipo propietario y open Source:

SOLUCIONES PROPIETARIAS			**SOLUCIONES OPEN SOURCE**	
CISCO NAC	MICROSOFT NAP	End Point Security: NAC Check Point.	FREE-NAC	PACKETFENSE

Tabla N.- 2 Soluciones NAC.

Dentro de un Ambiente Windows, en donde se dispone de un Directorio Activo, equipos Windows, se recomienda la opción de Microsoft NAP, la cual viene como un servicio Adicional en Windows 2008, 2012 Server desde la versión STD.

- Otra opción de Seguridad de Red es el uso de Sistemas de protección contra Malware, que es ofrecida por la Empresa CISCO, conocidos como AMP; pues

en el caso que ingresó un malware a nuestra red, es importante reconocerlo y actuar en nuestra red ya que se considera que ciertos malwares no son reconocidos por los antivirus y tampoco son bloqueadas sus actividades, esta opción es AMP para redes, que consiste en obtener una visibilidad y control de la red para proteger la red de malwares avanzados altamente sofisticados, persistentes, por medio de hardware y software especializado que analizan el comportamiento de la red a través de múltiples vectores de amenazas.

Microsoft Nap (Network Access Protection) como Solución de Control de Acceso a Red.

Es una herramienta que incluye una serie de componentes en el servidor y en el cliente que se habilitan o no dependiendo de la implementación, permite aplicar requisitos de mantenimiento, inspeccionar el estado del equipo cliente, limitar el acceso a red cuando se considera que un equipo no cumple requisitos, entre otras características detalladas a continuación:

- Supervisa y Verifica el estado de los equipos cliente cuando intentan conectarse a una red.
- Contiene una serie de componentes para proteger el acceso a la red.
- Permite detectar el estado de un equipo que intenta conectarse a la red.
- Aisla a clientes que no cumplan con los requisitos.

Los componentes de la infraestructura NAP son clientes de cumplimiento (EC) y servidores de Aplicación (ESS); se requiere una validación de salud y forzar un acceso limitado a la red de equipos que no cumplen requisitos de acceso.

Nap utiliza los siguientes tipos de Acceso a la Red

- Seguridad del protocolo IPSec.
- IEEE 802.1X con autenticación de conexiones de red.
- Conexiones VPN para accesos remotos, Mediante DHCP
- Terminal Server para conexiones al Gateway.

2.15 Seguridad de Aplicaciones Web.

OWASP (Open Web Application Security) en español Proyecto abierto de Seguridad en Aplicaciones Web, es un organismo o comunidad sin fines de lucro, de seguridad informática internacional formado por empresas, organizaciones educativas y particulares dedicados a mejorar la seguridad en Aplicaciones de software, creando artículos, metodologías, documentación, herramientas y tecnologías que pueden ser utilizadas gratuitamente.

Uno de sus artículos más difundidos y más aceptados es OWASP Top 10 que es documento de alto nivel de elaboración que se centra sobre las vulnerabilidades más críticas de las aplicaciones web, el cual es constantemente actualizado, se encuentra en la versión 2013 finalizada la cual es presentada en la siguiente tablina.

OWASP Top 10-2013	**Descripción**
A1-Inyección	Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados. [9]

A2-Pérdida de y gestión de sesiones	Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, o explotar otras fallas de implementación para asumir la identidad de otros. [9]
A3-Secuencia de comandos en sitios cruzados XSS	Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador victima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso. [9]
A4-Referencia directa insegura a objetos	Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados. [9]
A5-Configuración de seguridad incorrecta	Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación [9]
A6-Exposición de datos sensibles	Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito o credenciales de autenticación. Los atacantes pueden robar o modificar tales datos para llevar a cabo fraudes, robos de identidad u otros delitos. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador. [9]

A7-Ausencia de control de acceso a las funciones	La mayoría de aplicaciones web verifican los derechos de acceso a nivel de función antes de hacer visible en la misma interfaz de usuario. A pesar de esto, las aplicaciones necesitan verificar el control de acceso en el servidor cuando se accede a cada función. Si las solicitudes de acceso no se verifican, los atacantes podrán realizar peticiones sin la autorización apropiada. [9]
A8-Falsificación de peticiones en sitios cruzados CSRF	Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas proveniente de la víctima. [9]
A9-Uso de componentes con vulnerabilidades conocidas	Algunos componentes tales como las librerías, los frameworks y otros módulos de software casi siempre funcionan con todos los privilegios. Si se ataca un componente vulnerable esto podría facilitar la intrusión en el servidor o una perdida seria de datos. Las aplicaciones que utilicen componentes con vulnerabilidades conocidas debilitan las defensas de la aplicación y permiten ampliar el rango de posibles ataques e impactos. [9]
A10-Redirecciones y reenvíos no validados	Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder Páginas no autorizadas [9]

Tabla N.- 3. Owasp Top 10, versión 2013.

2.16 Normas y Estándares de Seguridad Informática

Siendo la Seguridad Informática la Protección de la Información contra amenazas cuyo fin pretende asegurar la continuidad de operaciones, minimizar el riesgo y maximizar el retorno de las inversiones y oportunidad de Negocio, varios organismos internacionales han definido estándares y normas que afirman el

cumplimiento de los requerimientos de mayor importancia para la información que son: Confidencialidad, Integridad y Disponibilidad. Se indica a continuación los más comunes a nivel mundial [9].

ISO 17.799.

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización, fue publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

ITIL Information Technology Infrastructure Library

ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Government Commerce, una entidad independiente de la tesorería del gobierno británico. ITIL fue utilizado inicialmente como una guía para el gobierno de británico, pero es aplicable a cualquier tipo de organización.

ISO Serie 27000

A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y

controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act) (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario (ISO 27799).

2.17 Análisis de la situación actual de la Organización en relación al cumplimiento de la Normativa.

Es necesario revisar los aspectos Generales de las normativas, enfocadas a la realidad del objeto de estudio ya que en nuestro país el acuerdo ministerial 166 del Esquema Gubernamental de Seguridad de la Información hace referencia a la normativa internacional ISO/IEC 27001:2005. Este acuerdo, entre otras cosas, obliga a las Administraciones Públicas al uso de la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000 para la gestión de la seguridad de la información, por lo que en nuestro país cada vez más se vuelve necesario implementar esquemas de Seguridad de Información en entidades públicas y privadas.

De acuerdo con el Articulo 2, “Las Entidades de la Administración Pública implementarán en un plazo de 18 meses el Esquema Gubernamental de Seguridad

de la Información (EGSI) que se adjunta al acuerdo como Anexo 1, a excepción de las disposiciones o normas marcadas como prioritarias en el esquema las cuales se implementarán en un período de 6 meses desde la emisión del presente acuerdo".

En el anexo 1 de este acuerdo, en su cuarto párrafo indica que el Esquema Gubernamental de Seguridad de la Información está basado en la norma Técnica Ecuatoriana INEN ISO/IEC 27002 para la gestión de la Seguridad de la Información.

La norma Técnica Ecuatoriana INEN ISO/IEC 27002 por su parte tiene como objeto "establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por una evaluación de riesgos. Esta norma puede servir como guía práctica para el desarrollo de normas de la seguridad de una organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

Una vez determinado los requisitos de seguridad, se deben elegir los controles apropiados dependiendo del sector, actividad y alcance que la organización pretenda asegurar su información, se debe elegir cuantos controles serán realmente aplicados para certificar que los riesgos se reduzcan a un nivel aceptable.

La Norma NTE INEN ISO/IEC 27002 contiene un total de 133 controles que se distribuyen en once secciones principales o dominios que enumera a continuación:

1. Política de la Seguridad.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de la Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Físicas y del Entorno.
6. Gestión de comunicaciones y Operaciones.
7. Control de Acceso.
8. Adquisición, desarrollo y mantenimiento de Sistemas de Información.
9. Gestión de los Incidentes de la Seguridad de la Información.
10. Gestión de la Continuidad del Negocio.
11. Cumplimiento.

Cada sección o dominio consta de una serie de objetivos de control. Para cumplir dichos objetivos, se especifican los distintos controles recomendados en base a las mejores prácticas relacionadas a la seguridad de la información. Existen herramientas de software que facilitan la implementación de un SGSI y análisis y gestión de Riesgos en base a un descubrimiento automático del inventario mediante despliegue de agentes, la interfaz gráfica de la herramienta se muestra en la siguiente figura.

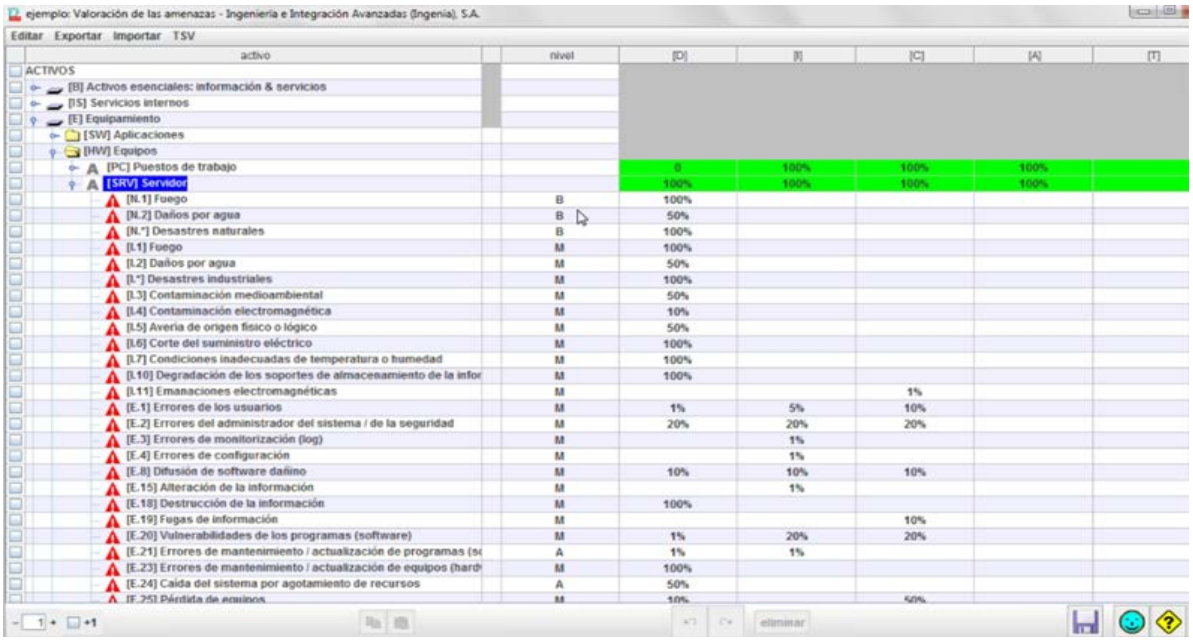


Figura N.- 7. Herramienta de Software que facilita la Implementación de SGSI.

A continuación en la Tabla N.-3 se realiza el análisis de Riesgos de los Bienes Informáticos de la Organización en estudio, aquí podemos observar cada uno de los elementos a proteger, su impacto, las vulnerabilidades a las que están sometidas y el peso indicado del 1 al 10, siendo 10 el valor máximo basándonos con lo indicado en la página 56.

Luego en la Tabla N.-4, en la primera parte, se presenta los valores estimados de pesos o importancia (en un rango de 0 a 5) de cada sección de acuerdo a la realidad del organismo en estudio en donde se destaca que aspectos como la gestión de activos, gestión de comunicaciones y gestión de la continuidad del negocio son los más importantes en la actualidad, esto en relación de que se lleva a cabo por ser un organismo público y cada activo es responsabilidad de una persona y de igual manera con la gestión de las comunicaciones y continuidad del negocio; con estos resultados, se deben tomar medidas que permitan elevar la importancia (peso actual) del resto de secciones.

También se destaca en la tabla 4 los pesos de cada uno de los 39 objetivos de control los cuales son multiplicados por un valor estimado en porcentaje de cumplimiento (de los controles escogidos para cumplir con los objetivos), que permiten estimar un resultado porcentual de cumplimiento de la organización actual que es del 26%.

Se puede concluir de manera categórica que el porcentaje de cumplimiento es bajo, por tanto es preciso tomar las medidas que sean necesarias que le otorguen la importancia a los dominios que al momento no son considerados y ejecutar tareas de manera de implementar correctivos, monitorearlos y mejorarlos.

ANALISIS DE RIESGO DE LOS BIENES INFORMATICOS (CENTRO DE DATOS)								
ELEMENTOS DE HARDWARE Y SOFTWARE								
HARDWARE					**VULNERABILIDAD**			
Can	**DESCRIPCION**	**APLICACIÓN**	**CRITICIDAD / IMPACTO**	**PESO (1-10)**	**Basadas en Planteamiento de Políticas de Seguridad**	**Basadas en fallas de planificación y programación de Sw.**	**Basadas en Descono-cimiento**	**De día cero**
1	UPS APC 22,5 KVA	PROTECCION C.D.	ALTO	10			X	
2	DELL	FIREWALL	ALTO	10	X	X	X	X
1	DELL	DHCP LINUX ALC	ALTO	10	X	X	X	X
1	CHASIS IBM H	CHASIS S. ALTERNO	MEDIO	5		X	X	X
7	SERVIDORES IBM BLADE TIPO CUCHILLA	SITIO ALTERNO	MEDIO	5		X	X	X
1	STORAGE 4700 IBM	ALMACENA VMWARE SITIO ALTERNO	MEDIO	5		X	X	X
1	STORAGE EXPANSIÓN	ALMACENA VMWARE SITIO ALTERNO	MEDIO	5		X	X	X
1	SERVIDOR IBM 3550	AD PRINCIPAL	ALTO	10	X	X	X	X
1	CHASIS IBM FLEX SYSTEM	CHASIS S. PRINCIPAL	ALTO	10		X	X	X
1	NODO CONTROLADOR IBM PARA CHASIS	CONTROLA NODOS S. PRINCIPAL	ALTO	10		X	X	X
5	SERVIDORES IBM FLEX TIPO NODO	SERVIDORES PRINCIPALES VIRTUALIZADOS + BASES DE DATOS S.P	ALTO	10		X	X	X
1	STORWIZE 5000	ALMACENA VMWARE SITIO PRINCIPAL	ALTO	10		X	X	X

1	STORAGE EXPANSIÓN	ALMACENA VMWARE SITIO PRINCIPAL	ALTO	10		X	X	X
2	SWITCH CISCO 4500	COMUNICACIÓN PRINCIPAL	ALTO	10		X	X	X
3	SWITCH CISCO 3750	COMUNICACIÓN PRINCIPAL	ALTO	10		X	X	X
1	SWITCH CISCO 3560	COMUNICACIÓN PRINCIPAL	ALTO	10		X	X	X
1	SWITCH CISCO 3550	COMUNICACIÓN PRINCIPAL	ALTO	10		X	X	X
28	SWITCH CISCO 2960	SWITCH DE ACCESO	MEDIO	5		X	X	X
1	ROUTER MIKROTIK TIP	EQUIPO DE ENLACE A TELEFONIA IP ALCALDIA	MEDIO	7		X	X	X
5	EQUIPOS CONVERSORES DE FIBRA A COBRE	ENLACES EXTERNOS	MEDIO	8		X	X	X
SOFTWARE								
1	LICENCIAMIENTO VMWARE	SERVIDORES INST.	ALTO	1		X	X	X
1	LICENCIAMIENTO VMWARE SRM	SERVIDORES INST.	ALTO	1		X	X	X
1	WIDOWS 2012 STARDAR DC	SERVIDORES INST.	ALTO	1		X	X	X
300	LICENCIAS OFFICE	SERVIDORES INST.	ALTO	1		X	X	X
20	LICENCIAS AUTOCAD	SERVIDORES INST.	ALTO	1		X	X	X
1	LICENCIA BD ORACLE STD	SERVIDORES INST.	ALTO	1	X	X	X	X
1	SOFTWARE REQUERIMIENTOS	SERVIDORES INST.	MEDIO	5	X	X	X	X
1	SOFT. RECAUDACION IMP	SERVIDORES INST.	MEDIO	5	X	X	X	X
1	SOFT. DE COMPRAS.	SERVIDORES INST.	MEDIO	5	X	X	X	X
1	SOFT. CONTABILIDAD	SERVIDORES INST.	MEDIO	5	X	X	X	X
1	SOFT. CONTROL	SERVIDORES INST.	MEDIO	5	X	X	X	X
1	SOFT. GIS.	SERVIDORES INST.	MEDIO	5	X	X	X	X
1	SOFT. APP. VARIAS	SERVIDORES INST.	MEDIO	5	X	X	X	X
1	SOFT. PAGINAS WEB	SERVIDORES INST.	ALTO	10	X	X	X	X
ELEMENTOS VARIOS								
1	Sistema de acceso a personal autorizado al Data center	SERVIDORES INST.	MEDIO	5	X	X	X	X

Tabla N.-3. Análisis de Riesgos de los Bienes Informáticos de la Organización.

PORCENTAJE DE CUMPLIMIENTO DE LA ORGANIZACIÓN.

ITEM	SECCION	PESO	OBJETIVO DE CONTROL	PESO	PORCENTAJE DE AVANCE
1	**POLITICA DE SEGURIDAD**	**3**			
1.1			Política de Seguridad de Información	5	0%
2	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**	**4**			
2.1			Organización interna	2,5	25%
2.2			Terceros	2,5	5%
3	**GESTION DE ACTIVOS**	**5**			
3.1			Responsabilidad sobre los activos	2,5	90%
3.2			Clasificación de la información	2,5	5%
4	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**	**3**			
4.1			Antes del empleo	1,6	5%
4.2			Durante el empleo	1,6	5%
4.3			Cese del empleo o cambio de puesto de trabajo	1,6	5%
5	**SEGURIDAD FÍSICA Y DEL ENTORNO**	**4**			
5.1			Áreas seguras	2,5	50%
5.2			Seguridad de los equipos	2,5	50%
6	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**	**5**			
6.1			Responsabilidades y procedimientos de operación	0,5	5%
6.2			Gestión de la provisión de servicios por terceros	0,5	80%
6.3			Planificación y aceptación del sistema	0,5	80%
6.4			Protección contra el código malicioso y descargable	0,5	80%
6.5			Copias de seguridad	0,5	80%
6.6			Gestión de la seguridad de las redes	0,5	5%
6.7			Manipulación de los soportes	0,5	5%
6.8			Intercambio de información	0,5	5%
6.9			Servicios de comercio electrónico	0,5	80%
6.10			Supervisión	0,5	5%
7	**CONTROL DE ACCESO**	**4**			
7.1			Requisitos de negocio para el control de acceso	0,71	25%
7.2			Gestión de acceso de usuario	0,71	25%
7.3			Responsabilidades de usuario	0,71	25%
7.4			Control de acceso a la red	0,71	5%

7.5			Control de acceso al sistema operativo	0,71	25%
7.6			Control de acceso a las aplicaciones y a la información	0,71	25%
7.7			Ordenadores portátiles y teletrabajo	0,71	25%
8	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	**5**			
8.1			Requisitos de seguridad de los sistemas de información	0,83	25%
8.2			Tratamiento correcto de las aplicaciones	0,83	25%
8.3			Controles criptográficos	0,83	0%
8.4			Seguridad de los archivos de sistema	0,83	25%
8.5			Seguridad en los procesos de desarrollo y soporte	0,83	0%
8.6			Gestión de la vulnerabilidad técnica	0,83	0%
9	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**	**4**			
9.1			Notificación de eventos y puntos débiles de seguridad de la información	2,5	0%
9.2			Gestión de incidentes y mejoras de seguridad de la información	2,5	25%
10	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**5**			
10.1			Aspectos de seguridad de la información en la gestión de la continuidad del negocio	5	80%
11	**CUMPLIMIENTO**	**3**			
			Cumplimiento de los Requisitos Legales.	1,67	0%
			Cumplimiento de las políticas y Normas de Seguridad y cumplimiento técnico.	1,67	10%
			Consideraciones sobre las auditorias de los sistemas de información.	1,67	10%
				54,76	**26%**

Tabla N.-4. Importancia de Cada Dominio y Porcentaje de Cumplimiento Actual.

2.18 Metodología de Análisis y Gestión de Riesgos OSSTMM.

Osstmm es un término derivado de las Iniciales en Inglés (Open Source Security Testing Methodology Manual) que en español significa Manual de Metodología Abierta de Testeo de Seguridad, es uno de los estándares

profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet sin embargo no es la única.

Fue desarrollado por el Instituto de Seguridad y metodologías Abiertas (ISECOM) por su siglas en Ingles, que es una organización sin ánimo de lucro que trabaja de manera continua en el desarrollo de metodologías de uso libre para la verificación de la Seguridad, programación segura, verificación de software y concientización de la seguridad. Debido a ser de carácter software libre, permite a cualquier analista de seguridad en el mundo contribuir en las mejoras de sus versiones, esta metodología intenta establecer un método científico para el análisis de la seguridad, evitando basarse en la experiencia y subjetividades del analista. [20]

De acuerdo con la ISECOM, el resultado de un test de seguridad es difícil de juzgarlo sin una metodología estándar. Un conjunto de variables pueden afectar los resultados de un test como por ejemplo la experiencia y subjetividad del analista, por consiguiente es importante definir un modo correcto de testeo basado en mejores prácticas y en un consenso a nivel mundial.

En la metodología OSSTMM, Seguridad Operacional, significa que no se hacen asunciones de cómo debe funcionar una solución de seguridad; en su lugar se observa cómo se comporta en la realidad.

La metodología OSSTMM, trata de cumplir con la medición del estado de la Seguridad en un ambiente operativo, teniendo en cuenta factores como controles (medidas de seguridad) en las interacciones y las limitaciones (debilidades o vulnerabilidades) que estos puedan presentar.

La seguridad Operacional se obtiene por medio de una combinación entre separación y controles, donde la separación de una amenaza y el activo representa una seguridad Total, por su lado si no es posible separar la amenaza del activo, es posible establecer **controles** para ofrecer protección. OSSTMM define 10 tipos de controles (que abarcan todas las medidas de protección posibles) y también propone el análisis de limitaciones que pueden encontrarse en dichos controles.

Dentro de la Metodología el término RAV (del termino en inglés Risk Assessment Values) representan la percepción de la seguridad, de forma similar a un valor porcentual, en donde un valor de RAV de 100 representa un balance ideal entre las operaciones, controles y limitaciones.

El tipo de testeo que exige la ISECOM para ser considerado un test OSSTMM debe ser:

- Cuantificable.
- Consistente y que se pueda repetir
- Válido más allá del periodo de tiempo actual
- Basado en la expertiz del testeador o analista y no en marcas comerciales.

Proceso de Análisis de Seguridad Según Metodología OSSTMM

El proceso de análisis de Seguridad evalúa las siguientes áreas que reflejan los niveles de seguridad presentes, conocidos como **dimensiones de seguridad**.

Visibilidad

“La visibilidad es lo que puede verse, registrarse, o monitorearse en el nivel de seguridad con o sin la ayuda de dispositivos electrónicos. Esto incluye, pero no

se limita a, ondas de radio, luz por encima del espectro visible, dispositivos de comunicación como teléfonos, GSM, email y paquetes de red como TCP/IP".-

Acceso

El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física. Esto puede incluir, pero no se limita a, una página web, una ventana, una conexión de red, ondas de radio, o cualquier cosa cuya ubicación soporte la definición de casi-público o dinde un computador interactúa con otro por medio de una red. Limitar el acceso significa negar todo excepto lo que este expresamente permitido financieramente y por buenas prácticas. [21]

Confianza

La confianza es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.

Autenticación

La autenticación es la medida por la cual cada interacción en el proceso está privilegiada.

No-repudio

El no-repudio provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.

Confidencialidad

La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.

Privacidad

La privacidad implica que el proceso es conocido únicamente por los sistemas o partes involucradas.

Autorización

La autorización es la certeza que el proceso tiene una razón o justificación de negocios y es administrado responsablemente dando acceso permitido a los sistemas.

Integridad

La integridad es la certeza que el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reversado sin el conocimiento de los sistemas o partes involucradas.

Seguridad

La seguridad son los medios por los cuales un proceso no puede dañar otros sistemas, o procesos incluso en caso de falla total del mismo.

Alarma

La alarma es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad. En la mayoría de violaciones de seguridad, la alarma es el único proceso que genera reacción

Mapa de Seguridad

Es una imagen de la presencia de Seguridad, compuesta por **6 secciones** las cuales son superpuestas entre si y contienen elementos de otras secciones. Un análisis apropiado de cada sección debe incluir ciertos elementos de las otras secciones. [21]

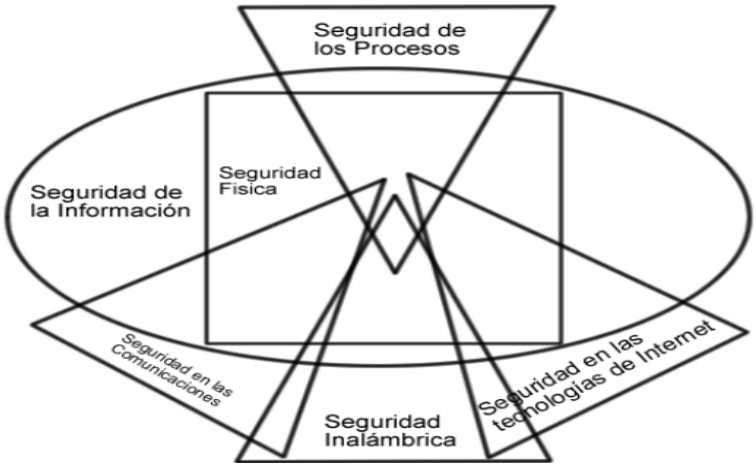


Figura N.- 8. Mapa de Seguridad definido por la OSSTMM

Lista de Módulos del Mapa de Seguridad

Son los principales elementos que contiene cada **sección,** los cuales deben incluir todas las dimensiones de seguridad aplicables con las tareas respectivas a ser ejecutadas y para los modulos que no son verificables o no exista infraestructura deberán declararse como NO APLICABLE en la documentación oficial del informe final OSSTMM.

La Metodología define además la seguridad operacional como una combinación entre separación y controles, donde la separación de una amenaza y el activo representan la seguridad total, y en el caso de no poder separar la amenaza del activo, es posible establecer controles para ofrecer protección.

En pocas palabras, la separación ofrece seguridad total y en los casos que no se pueda brindar separación, se aplican controles para aumentar la protección. A su vez, éstos cuentan con limitaciones, que disminuyen dicha protección. Cada una de estas características es medida de tal forma que se obtiene un valor que indica el estado de la seguridad operacional en un determinado momento. [21]

OSSTMM define diez tipos de controles (que abarcan todas las medidas de protección posibles) y también propone el análisis de las limitaciones que pueden encontrarse en dichos controles.

Cada una de estas características es medida de tal forma que se obtiene un valor que indica el estado de la seguridad operacional.

A continuación realizaremos un Análisis de la Seguridad de la Infraestructura propuesta mediante metodología OSSTMM, puntualmente sobre el servidor web de la organización que a su vez está conectado a la base de Datos.

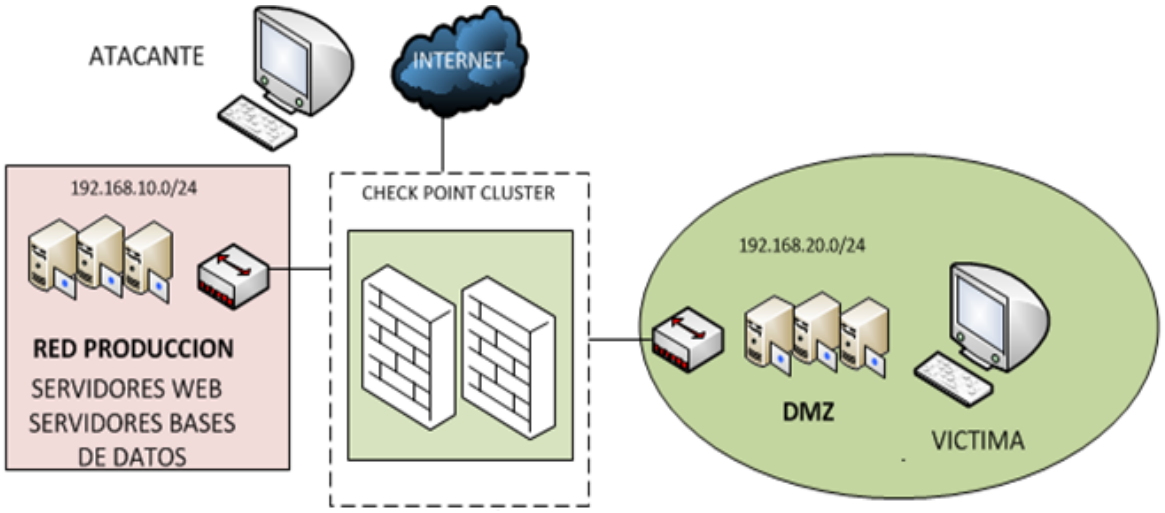


Figura N.-9. Esquema de Infraestructura propuesta para análisis OSSTMM.

El equipo Víctima corresponde a un Servidor Web el cual se accede mediante http y https y este a su vez se conecta a la base de Datos para consultas de trámites.

Visibilidad

Únicamente desde el Internet podemos ver un solo equipo que responde al puerto 443, además se tiene la posibilidad de hacer consultas por medio de una cadena de conexión en servidor web hacia la Base de Datos, por lo tanto en este caso particular se tiene una visibilidad de 2.

Accesos

En la infraestructura real, el servidor obedece al puerto 443 por tanto el valor de accesos es 1.

Confianza

Existe una relación de confianza entre el servidor Web y la Base de datos, este valor de confianza corresponde a 1. [21]

Controles

Controles sobre el Servidor Web.

(https) Confidencialidad = 1

(https) Integridad = 1

(https) No repudio = 1

Controles sobre el Servidor de Base de Datos.

(BD) Autenticación = 1

(BD) Subyugación = 1

Limitaciones

Preocupación

El servidor web acepta conexiones http (no seguro), valor 1 en limitaciones.

Resultados Seguridad Operacional.

Aplicamos la calculadora de RAV de OSSTMM con los datos obtenidos.

Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC	
Visibility	2
Access	1
Trust	1
Total (Porosity)	5

CONTROLS		
Class A		Missing
Authentication	1	4
Indemnification	0	5
Resilience	0	5
Subjugation	1	4
Continuity	0	5
Total Class A	2	23

Class B		Missing
Non-Repudiation	1	4
Confidentiality	1	4
Privacy	0	5
Integrity	1	4
Alarm	0	5
Total Class B	3	22

		True Missing
All Controls Total	5	45
Whole Coverage	10,00%	90,00%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	0	10,000000	0,000000
Weaknesses	0	5,600000	0,000000
Concerns	1	5,400000	5,400000
Exposures	0	0,920000	0,000000
Anomalies	0	0,380000	0,000000
Total # Limitations	1		5,4000

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC	7,289124
True Controls	2,915796
Full Controls	2,915796
True Coverage A	8,00%
True Coverage B	12,00%
Total True Coverage	10,00%
Limitations	7,470367
Security Δ	-11,84
True Protection	88,16

OSSTMM
Open Source Security Testing Methodology Manual
www.osstmm.org

Actual Security: 88,2705 ravs

Tabla N.- 6- Hola de cálculo para hallar el RAV de acuerdo con datos ingresados.

2.19 Infraestructura propuesta.

La infraestructura propuesta hace referencia a un modelo Real de una organización en la actualidad que se encuentra en producción y posee servidores críticos y contiene aproximadamente 800 usuarios.

En la topología presentada se distingue un enlace de internet conectado Directamente al equipo que cumple la función de firewall perimetral para toda la organización.

El firewall perimetral está formado por 2 equipos conocidos como Gateway de seguridad los cuales forman uno solo equipo virtual llamado clúster, los equipos Gateways se encuentran funcionando en modo activo-pasivo de manera que en una falla en cualquiera de estos 2 equipos, el clúster como tal seguirá funcionando y esta falla será imperceptible para el usuarios.

Adicionalmente a la Red de Internet se distinguen las siguientes redes.

- Red de Producción en donde se encuentran todos los servidores incluidos las Bases de Datos.
- Red DMZ en donde se encuentran el Servidor Web que se encuentra publicado al Internet que es un Proxy Reverso, encargado en redirigir el tráfico hacia los servidores de producción.
- Red de Usuarios.

Cada una de las redes indicadas tiene una conexión directa al cluster de Seguridad Perimetral (cada Gateway de seguridad tiene una interfaz conectado a cada red) con esto obtenemos un mayor control del tráfico dirigido desde y hacia

cada una de las redes mediantes reglas, es así como podemos configurar por ejemplo, que a la red DMZ solo ingresen desde el Exterior al puerto http y https del servidor y no desde la red de Usuarios ni tampoco de la Red de Producción, aislándolo de las redes por medio de reglas.

Es así como en la infraestructura real con la herramienta de seguridad propuesta se tiene implementado un esquema de seguridad compuesto por filtros.

En donde el primer filtro es el módulo de firewall que permite el paso únicamente de los puertos 80 y 443, si el tráfico pasa, es analizado por el segundo filtro que es el IPS, si el tráfico continua y no es detectado por los 2 modulos anteriores, continua con el siguiente filtro que es el modulo de Control de Aplicaciones web y URL Filtering, si el tráfico sigue, es analizado por el módulo de Antivirus y Antispam y luego de atravesar todos los filtros se dirige hacia el servidor.

Cuando el tráfico pasa todos los filtros de seguridad de la solución propuesta cual sale del perímetro de la solución sin embargo debemos tenerlo en constante análisis de vulnerabilidades y registrar constantemente el consumo de recursos en el servidor.

Adicionalmente en el servidor se debe actualizar el sistema operativo y aplicaciones de manera que actúen todos los parches conocidos para enfrentar ataques y exploits.

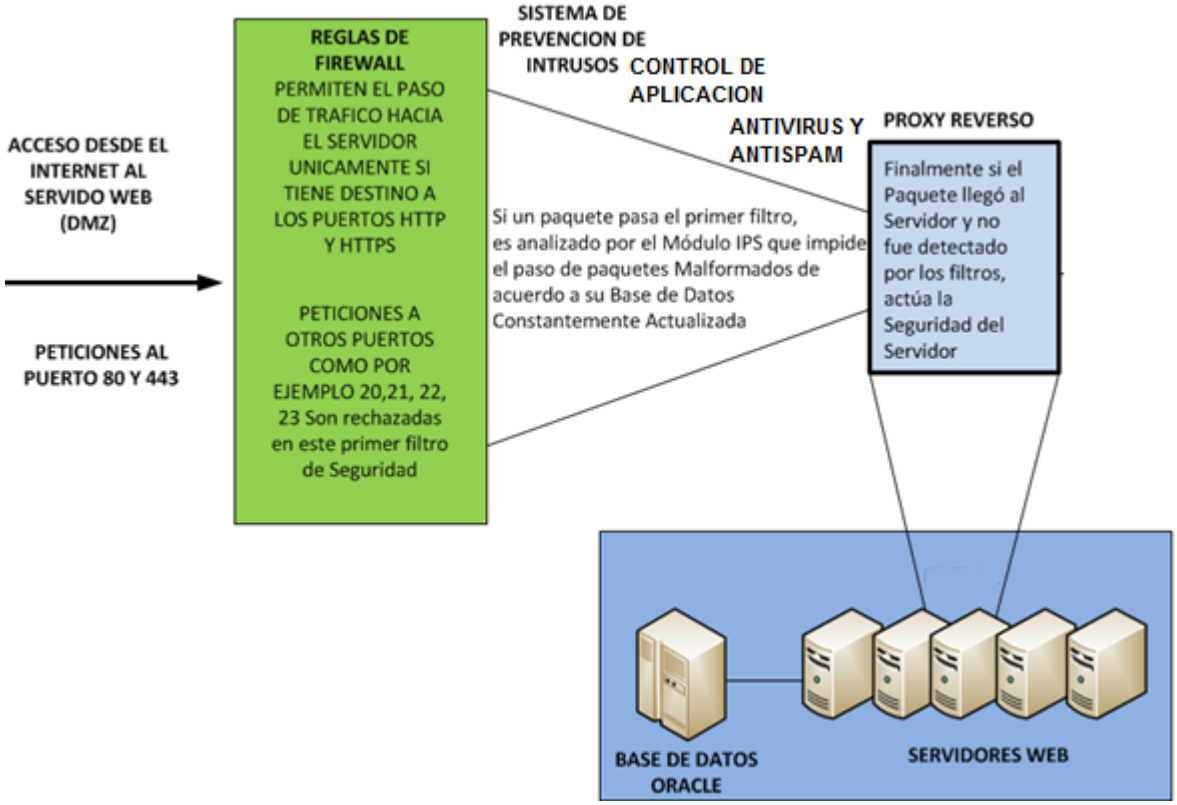


Figura N.- 10. Esquema de Seguridad Implementado en la Infraestructura Real Propuesta.

La comunicación entre el Proxy reverso y los Servidores Web de igual manera atraviesa los filtros y requieren autenticación, sin embardo este canal no es cifrado, este aspecto puede ser considerado para un futuro estudio.

La comunicación hacia la base de datos permite el acceso únicamente a un usuario autenticado en el dominio y autenticado en la base de Datos. Sin embargo esta comunicación tampoco es cifrada.

El escenario indicado en la figura N.- 7 representa el esquema actual compuesto por todos los filtros, sin embargo adicional al equipo proxy reverso se encuentra en la DMZ también un servidor con sistema operativo Windows el cual no ha podido ser migrado bajo este esquema por que posee unas aplicaciones de

índole financiera que permiten recaudación con un banco el particular, este equipo tiene una interfaz con una dirección pública lo cual lo vuelve vulnerable a ataques externos, a continuación se muestra el esquema de la plataforma web de la Infraestructura Propuesta.

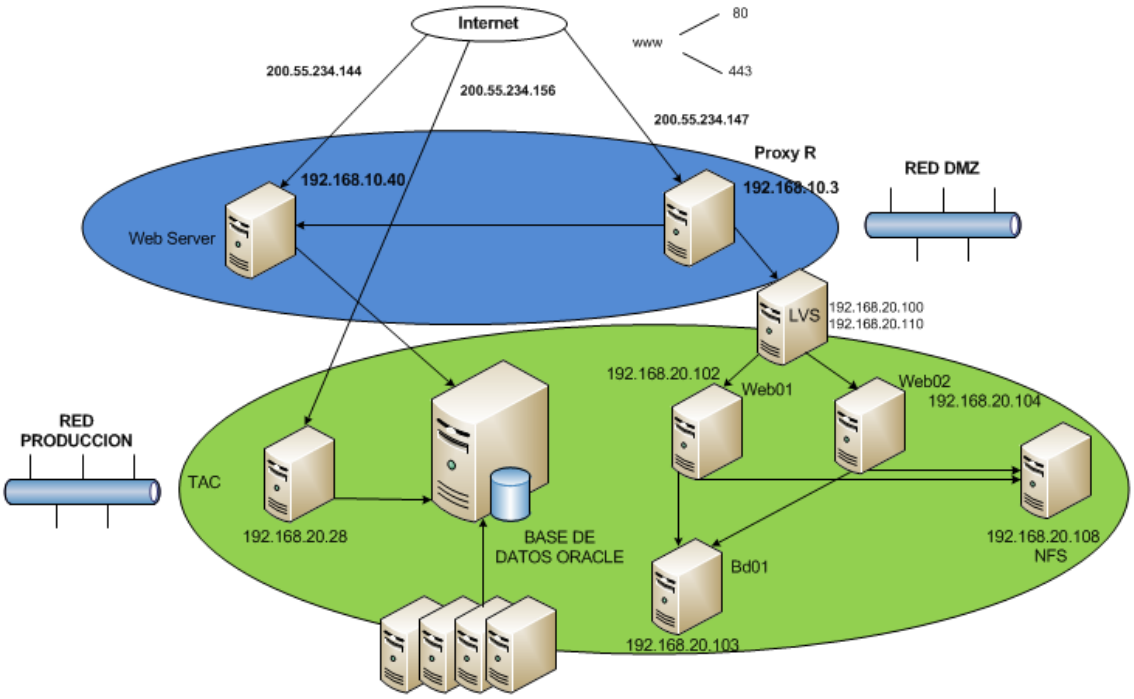


Figura N.-11. Plataforma Web de la Infraestructura Propuesta.

El equipo Web Server es el cual lo replicaremos en el escenario virtual y simularemos a un Atacante que envíe tráfico desde el internet y pondremos a prueba cada uno de los 2 primeros filtros de la solución de seguridad, que son el módulo de Firewall e IPS (Este último no actualizado por la versión demo utilizada). En este escenario no consideramos la Existencia del Proxy Reverso sino únicamente un servidor Windows como se muestra.

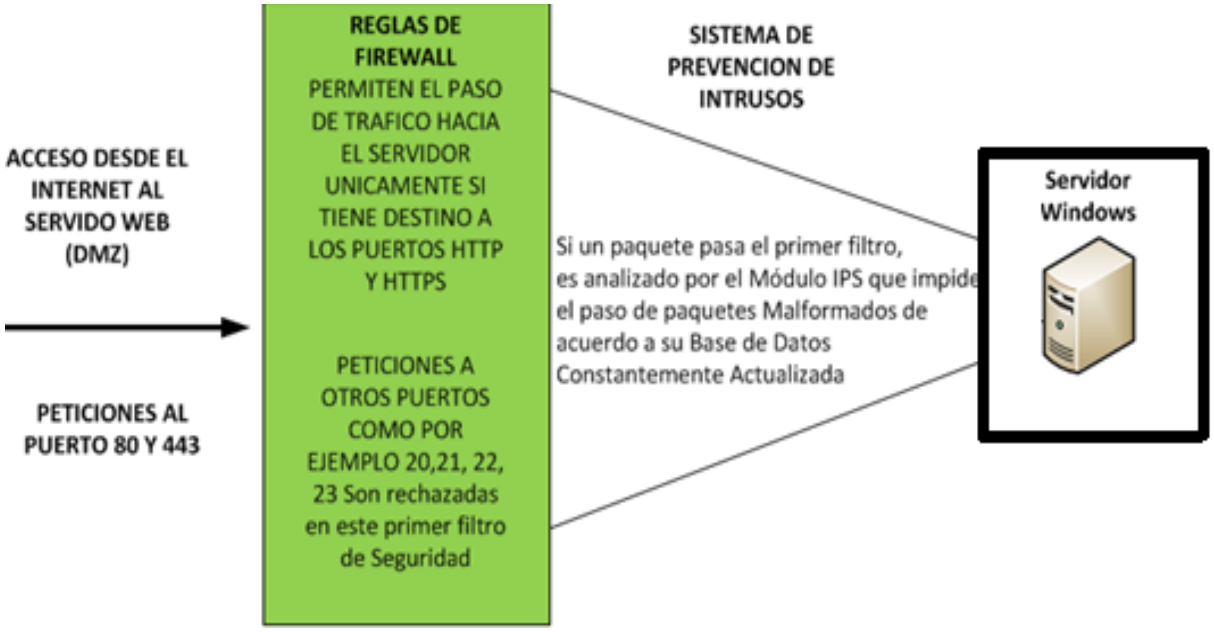


Figura N.12. Esquema Virtual sobre el cual se desarrollarán los ataques.

A continuación el diagrama lógico que muestra la infraestructura Real de la Organización en estudio la cual por motivos de seguridad no se revela la identidad.

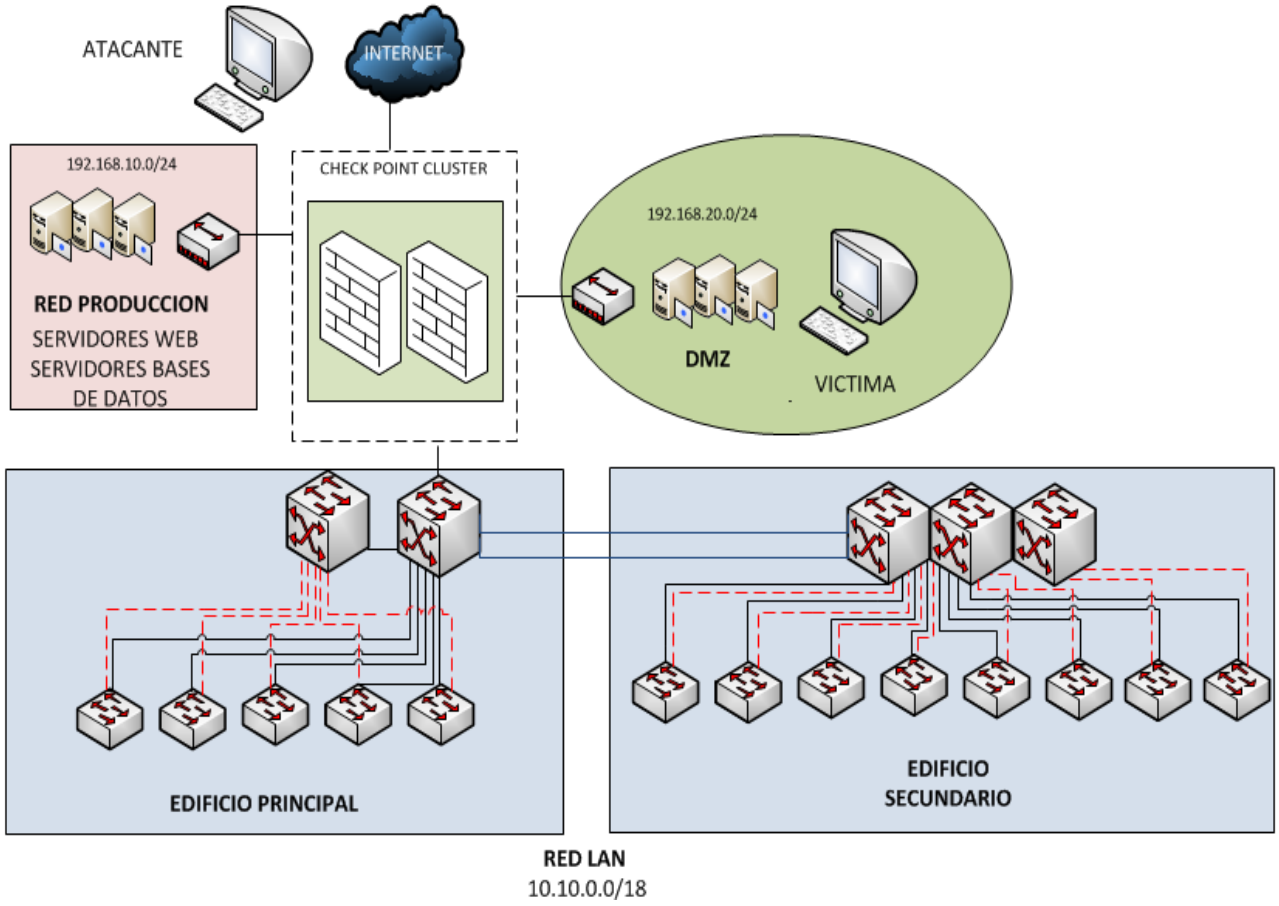


Figura N.- 13. Diagrama Lógico de la Infraestructura Propuesta para el Análisis y Evaluación de Seguridad Perimetral.

Debido a las ventajas que nos permite el trabajo sobre una infraestructura virtual, a manera de laboratorio, se recoge una parte del escenario real y se replicará en una plataforma de virtualización con la herramienta Vmware, Workstation.

Las principales características del Escenario Real que hemos recogido en el laboratorio Virtual son las siguientes.

1. Atacante Externo en la Red de Internet.
2. Equipo de Seguridad Perimetral. (Check Point Cluster)
3. Equipo Víctima en la Red DMZ.

Principalmente se determinará el comportamiento del Equipo de Seguridad Perimetral frente a ataques desde el Internet hacia la Red Desmilitarizada o DMZ. El siguiente Diagrama representa el esquema de Red Virtual.

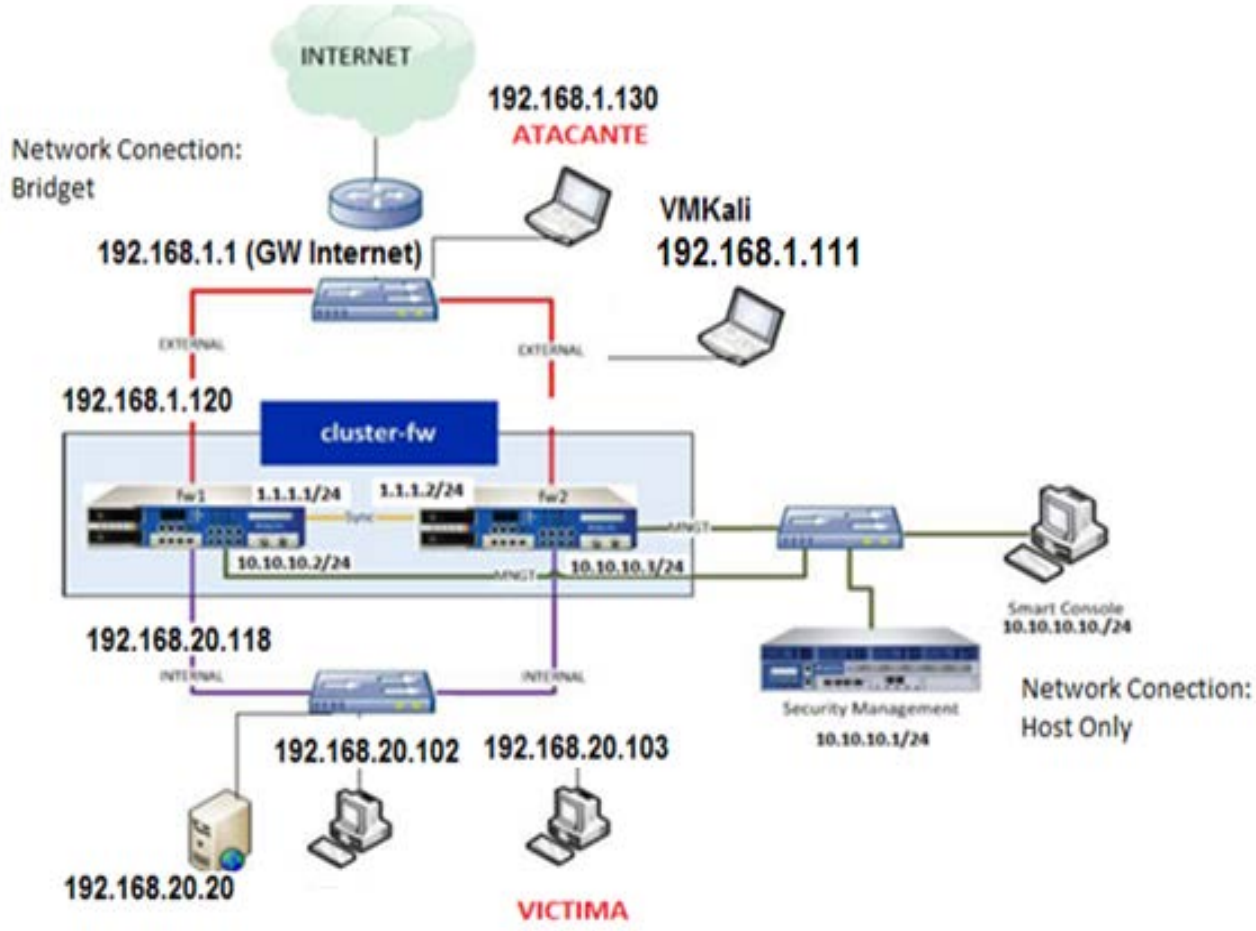


Figura N.-14. Escenario Virtual en donde se realizarán los Ataques desde el Internet hacia la red Interna.

2.20 Introducción a la Herramienta de Seguridad Propuesta.

La Herramienta de Seguridad propuesta para el análisis, representa un firewall en modo cluster mediante 2 equipos de Seguridad en modo Activo – Pasivo de la Empresa Check Point, proveedor de Soluciones de Seguridad de TI, líder mundial en Seguridad de Internet en sus productos de Firewall Perimetral

Empresarial y UTM según prestigiosas empresas consultoras como Gartner que lo ubica como líder durante 4 años consecutivos,

Desde sus inicios en 1993, fueron pioneros en la industria de Firewall patentando su tecnología de inspección del estado de red, su fábrica está ubicada en la República de Israel en la ciudad de Ramat-Gan. Sus equipos brindan protección garantizada contra todo tipo de Amenazas, minimiza los procesos complejos de manejo de seguridad y flexibiliza las soluciones orientadas a sus clientes pudiendo personalizarlas para satisfacer las necesidades puntuales en seguridad de las organizaciones, permitiéndoles implementar un plan de seguridad adaptado a sus necesidades.

Cada año presenta al mundo los resultados obtenidos en sus equipos a nivel mundial, entregando datos estadísticos con las principales amenazas y recomendaciones en General en sus reportes Check Point Security Report. La siguiente figura muestra su ubicación como líder en el Cuadrante de la Consultora Gartner en el año 2015, también se muestra otros productos.

Figura N.- 15. Cuadrante de Gartner que evalúa Firewalls Empresariales.

CAPITULO 3

Ejecución de Ataques

3.1 Objetivo del Escenario Virtual.

El objetivo es tomar una parte importante de la infraestructura propuesta para el análisis y plasmarlo en un escenario virtual de manera que refleje las condiciones reales del comportamiento de sus componentes.

3.2 Objetivo de la Solución de Seguridad Perimetral Propuesta.

Lo que se pretende conseguir es determinar el desempeño de la solución de Seguridad Perimetral Planteada frente a ataques externos originados desde el Internet.

3.3 Componentes de la Solución de Seguridad Perimetral Propuesta.

- Consola de Administración.
- Administrador del Equipo de Seguridad.
- Equipo de Seguridad.

Consola de Administración o Smartconsole.

Es un conjunto de herramientas gráficas, que se instala en un equipo con sistema operativo Windows, también conocido como GUI clientes (Unidad de Interfaz

gráfica), los cuales permiten conectarnos al Security Management para manipular diferentes aspectos de la configuración del firewall.

Administrador del Equipo de Seguridad o Security Management.

Se refiere a la consola de administración del o los firewalls. En esta consola se guardan las configuraciones, políticas y registros que están asociados a uno o dos Gateways o Firewall específico, se requiere instalación del Sistema Operativo GAIA.

Equipo de Seguridad o Security Gateway

Este término hace referencia a un equipo que hace funciones de Firewall o a veces también llamado Gateway, el cual se encuentra operando en la red y su objetivo es brindar seguridad en el perímetro, se requiere instalación del Sistema Operativo GAIA.

Existen dos tipos de instalación de este tipo de solución; Standalone y Distribuida.

Instalación Standalone es cuando el Security Gateway y el Security Management se encuentran instalados en la misma maquina generalmente este tipo de Instalación se da cuando se compra un solo equipo llamado Apliance.

Instalación Distribuida es cuando el Security Gateway y el Security Management son instalados en diferentes maquinas o appliance.

El tipo de instalación que realizaremos en nuestro escenario virtual será Distribuida ya que el equipo Firewall y el equipo Management están en diferentes equipos virtuales.

3.4 Implementación del Escenario virtual.

El diseño de la topología de la figura N.-9 fue implementado con la herramienta VMWare Workstation V9, sobre esta plataforma se puso en funcionamiento los diferentes segmentos de red.

Para la comunicación entre los equipos virtuales fue necesario configurar los adaptadores de red respectivos tomando en consideración que cada tarjeta de red tiene las siguientes opciones de configuración:

Modo Bridge en donde se le asigna a la tarjeta de red de la máquina virtual una dirección ip real visible desde la red.

Modo Nat en donde la maquina real actuará como un router NAT convirtiendo las direcciones internas en direcciones compatibles con el resto de red real.

Modo Host Only en donde se crea una red privada entre el ordenador anfitrión y la máquina virtual.

Modo Custom en donde se elige una red predefinida y finalmente Lan Segment que es cuando generamos un segmento de red interno con direccionamiento independiente únicamente visto desde las máquinas virtuales, la figura N.-9 indica la configuración de red de las máquinas virtuales.

Se puede concluir que se tiene 3 segmentos de red del en el escenario virtual, uno para la red lan de tipo Lan Segment, otro segmento de red para la comunicación entre el Gateway, el management y la consola (red de Gestión) de tipo host Only y otro para la salida el internet de tipo bridged.

A continuación se muestra un cuadro con las características de cada una de las máquinas virtuales que intervienen, en el cual no consta las características del equipo anfitrión, en donde se encuentra configurado la red de acceso a internet y configurado un adaptador de red de vmware con el direccionamiento de la red de Gestión, el cual debe tener sistema operativo Windows 7 u 8 para que soporte la instalación de la herramienta Smart Console y al menos 8Gb de memoria Ram.

Máquina Virtual	**Network Conection**	**Sistema Operativo**	**Dirección IP**	**Característica VM**
Check Point Firewall 1	Bridged - Lan Segment - Bridged (Lan Segment Sync)	GAIA R77.10	10.10.10.2/24	• 30 Gb de Disco Duro • 1 Gb en RAM • Al menos 3 tarjetas de red, para internet, para red lan y para red de gestión. • Si se instala en modo clúster se requiere de una tarjeta de red adicional para sincronización.
Security Management	Host Only	GAIA R77.10	10.10.10.1/24	• 30 Gb de Disco Duro • 1.5 Gb en RAM • Al menos una tarjeta de red para Gestión.
Windows XP1	Lan Segment Internal	WINDOWS XP	192.168.20.102/24	• 5 Gb de Disco Duro • 512 kb en RAM • Al menos una tarjeta de red para Gestión.
Domain Controler – DNS	Lan Segment Internal	WINDOWS SERVER 2003	192.168.20.20/24	• 10 Gb de Disco Duro • 512 kb en RAM • Al menos una tarjeta de red para Gestión.
Target Workstation (Victima)	Lan Segment Internal	LINUX	192.168.20.103/24	• 40 Gb de Disco Duro • 256 kb en RAM • Al menos una tarjeta de red para Gestión.
Attacker Workstation (Atacante)	Bridged	LINUX	192.168.1.130/24	• 40 Gb de Disco Duro • 256 kb en RAM • Al menos una tarjeta de red para Gestión.
VMKali	Bridged	LINUX	192.168.1.111/24	• 10 Gb de Disco Duro • 1 Gb en RAM • Al menos una tarjeta de red para Gestión.

Tabla N.-5. Configuración de Máquinas Virtuales del Escenario Virtual.

Una vez instalado el sistema operativo (GAIA) en el Gateway y el Management, se deberá ingresar vía web para ajustar la configuración,

posteriormente se debe instalar el software de Smart Console que permite gestionar las ordenes al management para que este a su vez envíe a los Gateways.

Finalmente se comprueba salida al internet de los equipos de la red lan para lo cual se crean las reglas necesarias que serán analizadas más adelante en este documento.

3.5 Implementación de Ataques y Análisis de Resultados.

Para la implementación de ataques seguiremos el procedimiento de Ethical Hacking indicado en la página 52, el cual en su primera fase recomienda realizar un reconocimiento del objetivo, luego en una Fase 2 escaneo y análisis de vulnerabilidades, posteriormente mediante herramientas de software se realizarán pruebas de penetración, no se pretende entrar en detalle en mantenimiento de acceso y eliminación de pruebas en la parte práctica del presente trabajo.

Fase 1.- Reconocimiento

Esta fase de reconocimiento consiste en obtener la mayor cantidad de información posible sobre nuestro objetivo, en primera instancia acudimos a sitios web que nos entregan información importante acerca de nuestro sitio web objetivo, como dirección ip, estado de puertos, entre otros detalles, algunos sitios que nos muestran esta información se muestran a continuación.

http://centralops.net/co/

http://www.yougetsignal.com/tools/open-ports/

Figura 16a. Obtención de la Dirección IP Pública de un servidor Web.

La figura 16a, muestra la Dirección IP pública como resultado de colocar la dirección del sitio web Real en el sitio http://centralops.net.

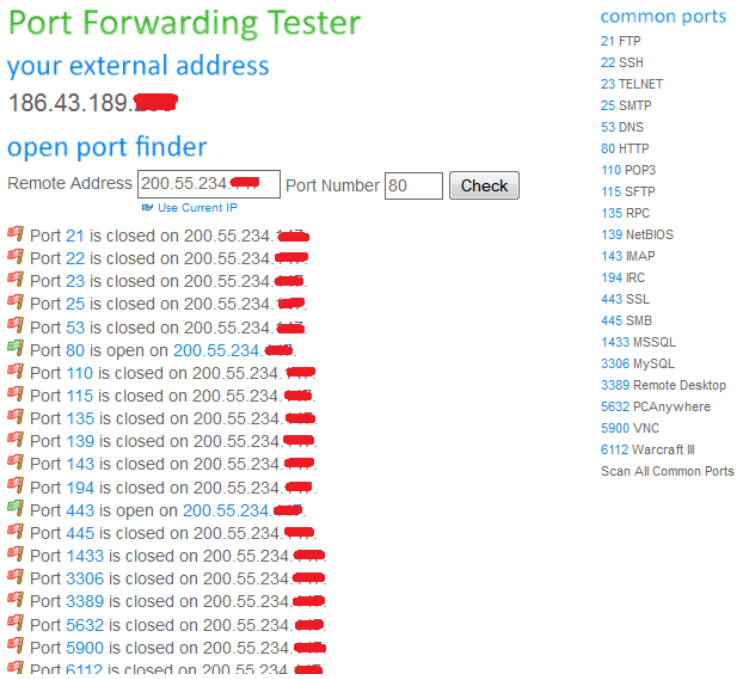


Figura N.-16b. Verificación de Puertos abiertos mediante web.

La figura 16b muestra el resultado de un analizador de puertos web que analiza el servidor web de producción de la Infraestructura Real, en donde se

observa que los puertos 80 y 443 se encuentran abiertos, lo cual coincide con la realidad.

No podemos hacer esta prueba en el escenario virtual por que no se tiene una dirección pública ni dominio registrado.

Adicional a conocer los puertos abiertos de un servidor al que pretendemos realizar el ataque, podemos investigar el sistema operativo de la víctima por medio del comando Nmap la directiva –O la cual pretendemos nos entregue esta información, al mismo tiempo que aplicamos el comando Nmap –O, ejecutamos paralelamente un sniffer en el origen y la herramienta de seguimiento “Tracker” que incluye el equipo de Seguridad Perimetral y observamos el resultado, cabe indicar que se ejecutó el comando con el IPS habilitado, los resultados se muestran en las Figuras 17a y 17b. Estas pruebas fueron realizadas en el escenario virtual.

La primera vez que ejecutamos el comando se obtiene el siguiente resultado:

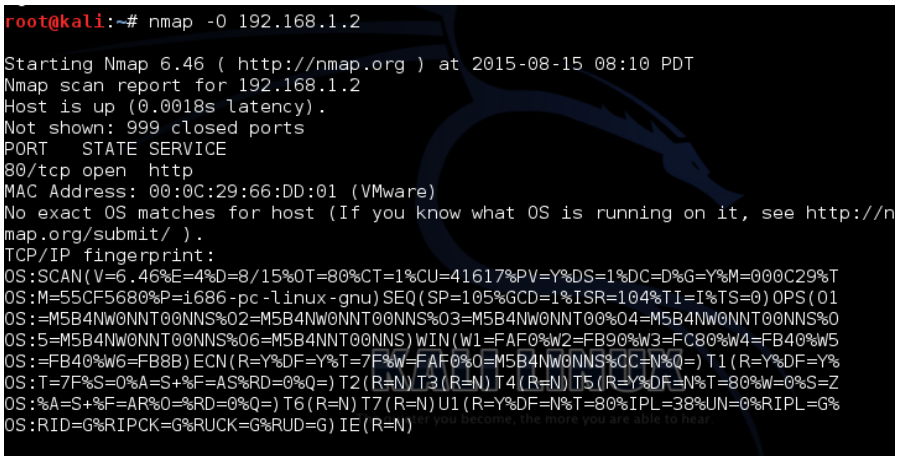


Figura N.-17a. Resultado del Comando Nmap -O para conocer el Sistema Operativo de un equipo, al primer intento.

La figura 17a, muestra el resultado al ejecutar por primera vez el comando para conocer el sistema operativo del equipo.

Para la segunda y tercera ocasión que ejecutamos el comando se obtuvo el resultado mostrado en la figura 12b, lo que demuestra que los ataques son más efectivos realizándolos más de una vez.

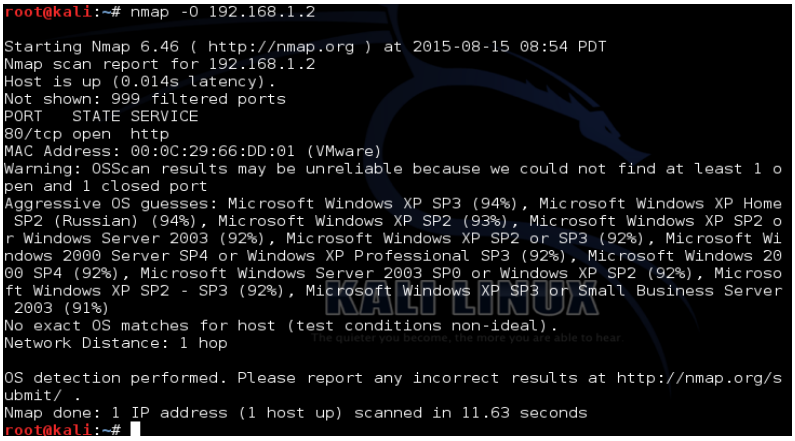


Figura N.-17b. Resultado del Comando Nmap -O para conocer el Sistema Operativo de un equipo, al 2do y 3er intento.

La figura 17b, muestra que el equipo victima tiene sistema operativo Microsoft Windows XP, luego de ejecutar el comando Nmap –O.

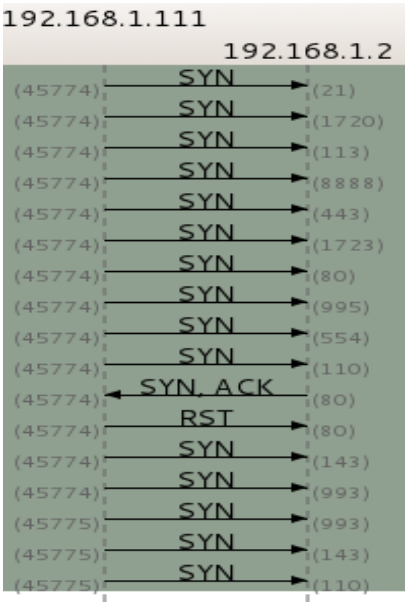


Figura N.-17c. Resultado de tráfico con Wireshark, mientras se ejecuta el comando Nmap –O en el equipo origen.

La figura 17c muestra el resultado del sniffer Wireshark en el equipo atacante, se muestra claramente que el receptor responde con un SYN, ACK únicamente a la petición realizada por el puerto 80 y de inmediato el atacante le devuelve la finalización de comunicación RST.

Finalmente en la figura 17d, observamos el resultado de la herramienta "Smart View Tracker" que incluye la herramienta de seguridad perimetral, que muestra los registros o logs marcados por los paquetes que en este caso tienen como origen el equipo atacante y como receptor el equipo víctima, que indica que únicamente los paquetes http son aceptados, el resto es dropeado.

49312	17Aug2015	0:23:55			SG1			poppassd	192.168.1.111	192.168.1.2	4	4-Standard
49313	17Aug2015	0:23:55			SG1			1022	192.168.1.111	192.168.1.2	4	4-Standard
49314	17Aug2015	0:23:55			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49315	17Aug2015	0:23:55			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49316	17Aug2015	0:23:56			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49317	17Aug2015	0:23:56			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49318	17Aug2015	0:23:56			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49319	17Aug2015	0:23:56			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49320	17Aug2015	0:23:56			SG1				192.168.1.111	192.168.1.2	4	4-Standard
49321	17Aug2015	0:23:56			SG1				192.168.1.111	192.168.1.2	4	4-Standard
49322	17Aug2015	0:23:56			SG1			32663	192.168.1.111	192.168.1.2	4	4-Standard
49323	17Aug2015	0:23:56			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49324	17Aug2015	0:23:56			SG1			http	192.168.1.111	192.168.1.2		
49325	17Aug2015	0:23:56			SG1			http	192.168.1.111	192.168.1.2		
49326	17Aug2015	0:23:56			SG1			35365	192.168.1.111	192.168.1.2	4	4-Standard
49327	17Aug2015	0:23:56			SG1			35365	192.168.1.111	192.168.1.2		
49328	17Aug2015	0:23:58			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49329	17Aug2015	0:23:58			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49330	17Aug2015	0:23:58			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49331	17Aug2015	0:23:58			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49332	17Aug2015	0:23:58			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49333	17Aug2015	0:23:59			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49334	17Aug2015	0:23:59			SG1				192.168.1.111	192.168.1.2	4	4-Standard
49335	17Aug2015	0:23:59			SG1				192.168.1.111	192.168.1.2	4	4-Standard
49336	17Aug2015	0:23:59			SG1			39868	192.168.1.111	192.168.1.2	4	4-Standard
49337	17Aug2015	0:23:59			SG1			http	192.168.1.111	192.168.1.2	3	3-Standard
49338	17Aug2015	0:23:59			SG1			35739	192.168.1.111	192.168.1.2	4	4-Standard
49339	17Aug2015	0:23:59			SG1			35739	192.168.1.111	192.168.1.2		
49351	17Aug2015	0:25:56			SG1			35739	192.168.1.111	192.168.1.2		

Figura N.-17d. Muestra los Registros desde el equipo Atacante hacia la víctima durante la ejecución del comando Nmap –O.

Y finalmente, la siguiente figura muestra la información que arroja el IPS.

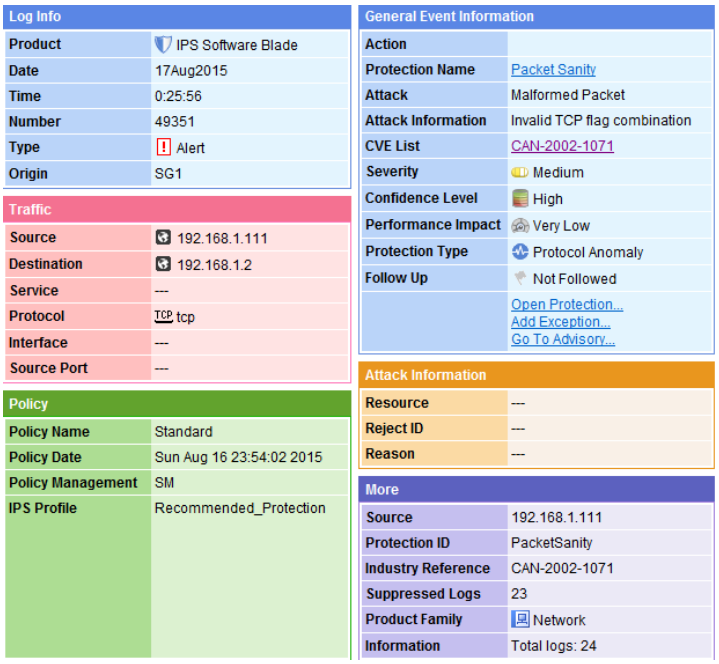


Figura N.- 17e. Muestra resultado de la Detección de IPS.

En la figura N.-17e, se puede observar el resultado del IPS, el cual detecta un ataque llamados Malformed Packet cuya vulnerabilidad tiene el código (CVE CAN-2002-1071).

Si bien se pudo observar que al ejecutar la herramienta Nmap en nuestro escenario de pruebas se indica que el sistema operativo de la víctima es Windows XP, el IPS detecta únicamente lo que existe en su base de datos (la cual debería estar actualizada), sin embargo el módulo de firewall también actúa bloqueando Paquetes.

Si deseamos conocer con exactitud el sistema operativo ya que el resultado de este análisis indica “Warning: Los resultados pueden no ser reales” se puede acudir a scripts internos que tiene la herramienta Nmap, para ello deben estar habilitados en la victima los puertos 445, 139 y 135 y ejecutar el comando #nmap –script smb-os-discovery.nse 192.168.1.2

Otra información importante es conocer la versión de los servicios que están corriendo, con la directiva –sV. A continuación el resultado de aplicarlo a nuestro escenario de pruebas.

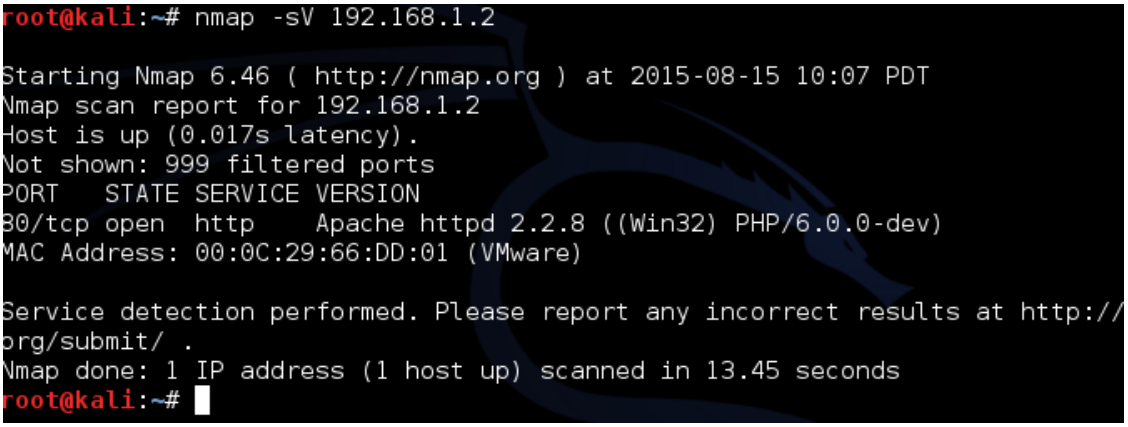


Figura 17f. Muestra claramente el nombre y la versión de la aplicación que corre sobre el puerto abierto.

Resultados de la Fase de Reconocimiento

En la primera parte de la práctica obtenemos la Dirección IP pública del sitio web como se muestra en la figura 11a, luego realizamos un escaneo de puertos abiertos del mismo sitio, esto nos arroja los resultados mostrados en la figura 11b; en ambos casos tanto en la obtención de la Dirección IP, así como la obtención de los puertos 80 y 443 en estado abierto los resultados coinciden con la realidad de la infraestructura propuesta ya que fueron ejecutados con los servidores reales.

Posteriormente realizamos las tareas de reconocimiento en nuestro escenario Virtual, en donde se observa que a pesar de que el IPS detecta al paquete que contiene una Vulnerabilidad CVE List CAN-2002-1071 mostrado en la figura 17e, se obtiene el resultado esperado del ataque que es obtener el Sistema Operativo como

se muestra en la figura 17b. Sin embargo se debe indicar que para obtener el resultado fue necesario realizar el test en más de una ocasión.

Adicionalmente se ejecuta el comando Nmap –sV el cual también arrojó resultados correctos acerca de la versión de la aplicación que está corriendo sobre el puerto habilitado como se muestra en la figura 17f. Estos resultados obedecen a que el IPS se encuentra en el momento del ataque en estado de Detección por Defecto y desactualizado que únicamente detecta los malwares pero no los bloquea, si cambiamos la configuración del IPS a estado de Detección Recomendada y actualizamos el módulo de IPS, el paquete es efectivamente rechazado, para comprobarlo se muestra los mismos ataques realizados en el escenario virtual sobre el escenario real en la figura 17g.

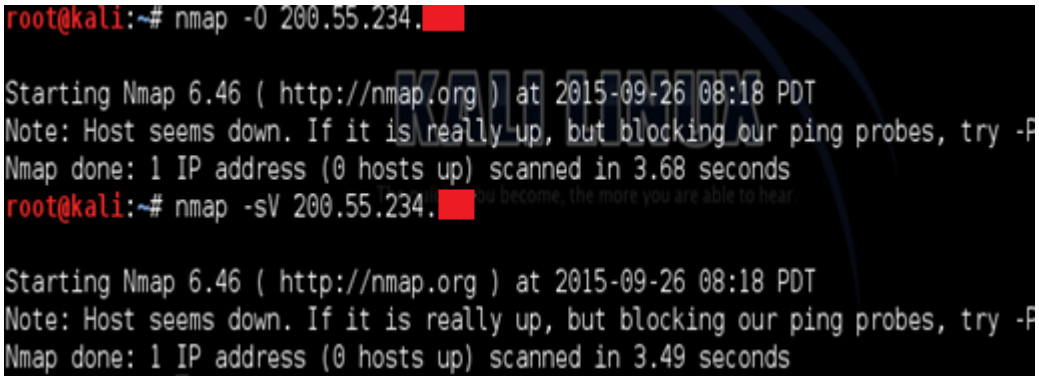


Figura 17g. Ataques a la infraestructura Real.

La figura 17g muestra claramente los resultados de los comandos realizados ya no sobre el escenario virtual si no sobre el escenario real, en donde se encuentra actualizado el IPS.

Fase 2.- Escaneo y análisis de vulnerabilidades.

Esta fase consiste en analizar puertos y formas que permitan ingresar a la red y sistemas objetivos, esta es la etapa previa a la ejecución del ataque, para ello una

vez que conocemos la dirección IP (publica de nuestro servidor Web) entre otros detalles conseguidos, realizamos un tipo de “ataque” de escaneo de puertos, en donde la víctima es nuestro servidor web de pruebas, el cual debe permitir conexiones entrantes desde el exterior en el puerto 80 http, con esta premisa generamos nuestro escenario virtual y realizamos configuraciones como se muestra en la siguiente figura.18.

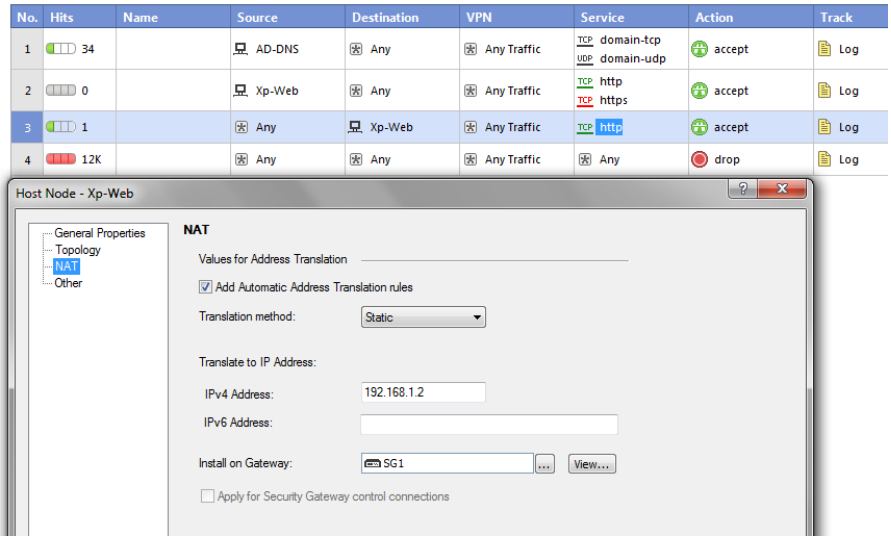


Figura N.-18. Simulación del Escenario Real mediante Virtualización.

La figura 18 muestra claramente los equipos protegidos por la solución de seguridad perimetral en donde se muestran las reglas específicas para cada servidor, se observa en la regla N.-1 el permiso desde el servidor DNS hacia cualquier lugar el tráfico en el puerto 53 para protocolo Tcp y Udp. La regla N.-2 permite el tráfico desde el servidor web víctima hacia cualquier lado en los puertos http y https, esto le permite al servidor poder navegar en estos puertos.

La regla N.-3 permite el tráfico http desde cualquier lado incluido el internet acceder al equipo web víctima. Finalmente la regla N.-4 elimina todo paquete que ingrese y que no sea declarado.

Con estas configuraciones se procede a realizar el escaneo de puertos mediante herramientas dedicadas para el efecto como por ejemplo Nmap.

Escaneo de Puertos con Nmap

Nmap (Network Mapper) es una herramienta de software de código abierto dedicada para exploración (rastreo) de red y auditorías de seguridad el cual ha sido diseñado para escanear redes como también host únicos, tiene varias opciones de configuración que usadas de manera adecuada se puede evitar dejar huellas y permite el encubrimiento de dirección ip lo que no es posible con otras herramientas.

Las técnicas de escaneo pueden ser clasificadas en función del grado de conexión realizada contra la maquina destino y en función de los paquetes enviados, las cuales se describen a continuación:

1. Escaneo Abierto.
2. Escaneo a medio abrir.
3. Escaneo Sigiloso.

1.- El escaneo de puertos de tipo Abierto nos proporciona un alto nivel de fiabilidad sin embargo quedan almacenados los registros y sería detectado por cualquier sistema IDS haciéndose visible el escaneo, por tanto es usado en auditorías internas y durante escaneo de equipos propios. Este tipo de escaneo realiza una conexión Full TCP Conection que significa abrir una conexión completa con el equipo remoto con el modo de conexión normal, conocido como three-way TCP/IP Handshake que consiste en que al inicio la máquina origen o cliente envía un paquete con el flag SYN activado a la máquina destino o servidor, el servidor responde con los flags SYN/ACK activados que significa que el puerto al que se realizó el intento de conexión se encuentra abierto, una vez que el cliente envía el

ack de confirmación se completa el three-way TCP/IP Handshake y la conexión es terminada por el cliente, pudiéndose repetir el proceso para el resto de puertos que se desee escanear.

Figura N.-19. Full TCP Conection de Puerto Abierto (Izquierda). Full TCP Conection de Puerto Cerrado (Derecha).

Por su parte si el puerto que intentamos escanear se encuentra cerrado, el servidor en lugar de responder con el flag activado SYN/ACK, lo hace con RST/ACK informando al cliente que debe terminar la conexión con un RST ya que el puerto se encuentra cerrado.

En nuestro ejemplo práctico, a continuación observamos los resultados al aplicar un escaneo abierto para un puerto abierto y para uno cerrado, se muestra el análisis con Wireshark así como la herramienta de registros de logs de Check Point, a continuación las capturas que muestran los resultados.

Policy

Search for IP, object, action, ... Query Syntax

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	670		AD-DNS	Any	Any Traffic	TCP domain-tcp UDP domain-udp	accept	Log
2	127		Xp-Web	Any	Any Traffic	TCP http TCP https	accept	Log
3	75		Any	Xp-Web	Any Traffic	TCP http	accept	Log
4	235K		Any	Any	Any Traffic	Any	reject	Log

Figura N.- 20a. Muestra que la Regla N.-4 rechaza todos los paquetes que no son declarados en las reglas 1, 2 y 3.

```
root@kali:~# nmap -sT 192.168.1.2 -p 80,21

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-13 05:19 PDT
Nmap scan report for 192.168.1.2
Host is up (0.0012s latency).
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp open   http
MAC Address: 00:0C:29:66:DD:01 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
root@kali:~#
```

Figura N.-20b. Muestra el resultado de ejecutar Nmap –sT en el servidor web (victima), en donde se pretende obtener el estado de los puertos 80 y 21.

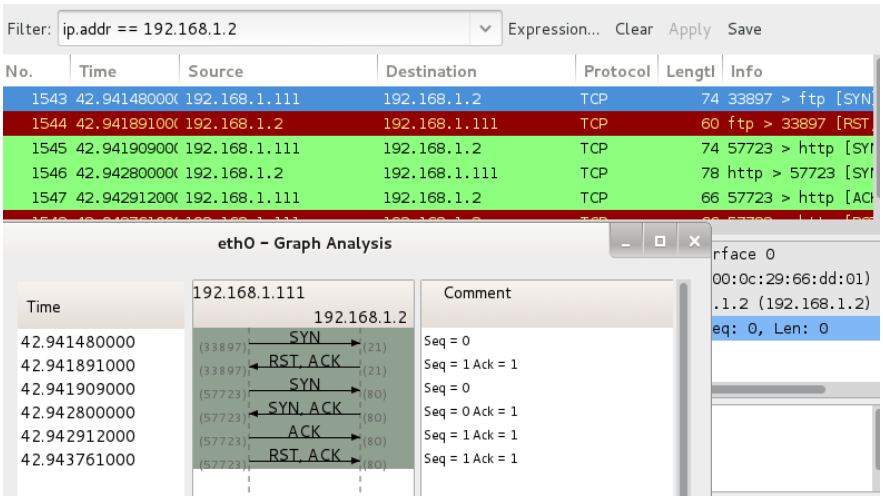


Figura N.-20c. Muestra gráficamente el tráfico de las conexiones TCP realizadas hacia los puertos 80 y 21 desde el equipo atacante, aplicando la herramienta Wireshark.

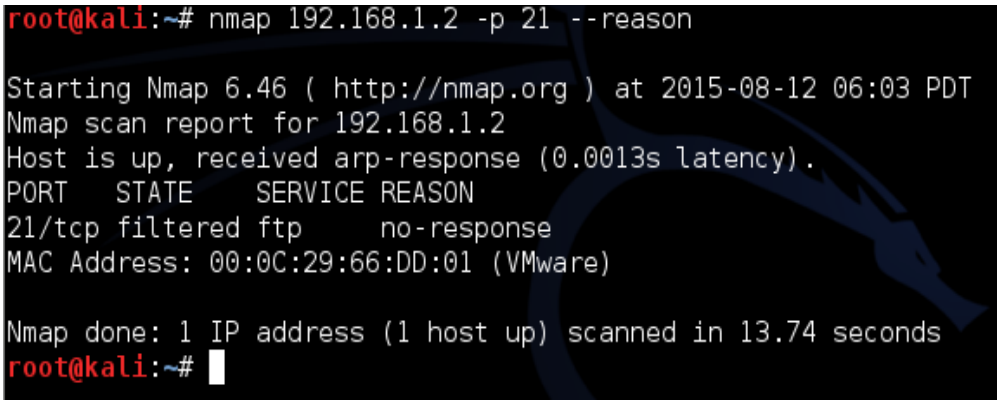
Figura N.- 20d. Muestra que únicamente es aceptado el tráfico en el puerto http dirigido hacia la víctima y el tráfico en el puerto 21 es rechazado.

Un puerto también puede estar en estado filtered cuando se envía SYNCs pero no responde ni con un RESET ni con un SYNC, este comportamiento suele

indicar que se ha establecido una política de DROP en un firewall como se muestra en la figura 21a y 21b.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	34		AD-DNS	Any	Any Traffic	domain-tcp domain-udp	accept	Log
2	0		Xp-Web	Any	Any Traffic	http https	accept	Log
3	1		Any	Xp-Web	Any Traffic	http	accept	Log
4	12K		Any	Any	Any Traffic	Any	drop	Log

Figura N.- 21a. Muestra la regla N.-4 en Drop en lugar de reject, esto lo que hace es informar que está filtrado por el firewall.



```
root@kali:~# nmap 192.168.1.2 -p 21 --reason

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-12 06:03 PDT
Nmap scan report for 192.168.1.2
Host is up, received arp-response (0.0013s latency).
PORT   STATE    SERVICE REASON
21/tcp filtered ftp     no-response
MAC Address: 00:0C:29:66:DD:01 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
root@kali:~#
```

Figura N.-21b. Indica que el puerto 21 se encuentra detrás de un firewall de seguridad.

Resultados Obtenidos por escaneo de Puertos de tipo Abierto.

Las directivas para ejecutar este tipo de escaneo son de tipo -sT (Sondeo TCP).

De acuerdo a las pruebas realizadas en el escenario práctico se observa que si el puerto está abierto y el firewall permite el paso de tráfico que en el caso práctico es el 80 y a pesar de estar el IPS habilitado en la opción recomendada, se obtienen los mismos resultados al no estar habilitado el IPS, es decir se realizaron las

pruebas tanto con el IPS deshabilitado y con el IPS habilitado; se ha logrado determinar según los datos arrojados de las pruebas que con esta metodología para el firewall e IPS son intentos de conexión que no son detectados como amenaza debido a la no actualización del IPS, ante esto se ha logrado vulnerar los filtros 1 y 2.

Usualmente cuando encontramos un puerto en estado de filtrado esto implica que el servidor se encuentra detrás de un firewall con una política de drop (comúnmente utilizada).

2.- El escaneo de puertos a medio abrir por su parte sucede cuando el cliente termina la conexión antes de que se complete el proceso de intercambio Three-way TCP/IP handshake. Mediante esta metodología para reconocer si un puerto del servidor está abierto o cerrado no necesita establecer realmente una conexión sino es suficiente enviar un único paquete SYN y si recibe como respuesta un paquete ACK es porque ha detectado un puerto activo (figura 17), después de esto el cliente envía un RST para terminar de forma abrupta la comunicación; si el cliente en lugar de un ACK recibe un RST significa que el puerto se encuentra inactivo. La directiva utilizada para este tipo de escaneo es –sS (sondeo SYN o Half Open).

Ésta metodología de sondeo es igual a la de sondeo de puerto de tipo abierto, excepto en el último paso en donde en lugar del envío del ACK por parte de la máquina cliente no se lleva a cabo y en su lugar, el cliente termina la conexión mediante el envío de un RST.

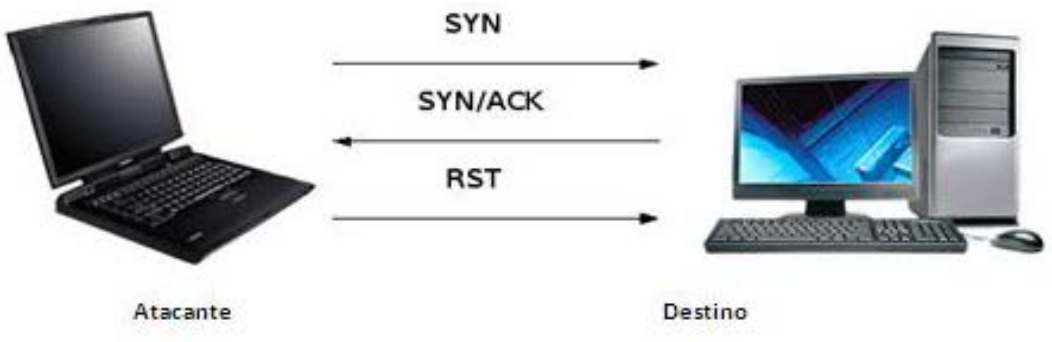


Figura N.- 22. Escaneo de puerto a medio abrir, puerto abierto.

En nuestro ejemplo práctico, a continuación observamos los resultados al aplicar un escaneo a medio abrir para un puerto abierto y para uno cerrado, a continuación las capturas que muestran los resultados.

```
root@kali:~# nmap -sS 192.168.1.2 -p 80,22

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-13 05:39 PDT
Nmap scan report for 192.168.1.2
Host is up (0.0046s latency).
PORT   STATE  SERVICE
22/tcp closed ssh
80/tcp open   http
MAC Address: 00:0C:29:66:DD:01 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
root@kali:~#
```

Figura N.- 22a. Indica el puerto 22 como cerrado y el puerto 80 abierto, luego de la ejecución del comando Nmap –sS.

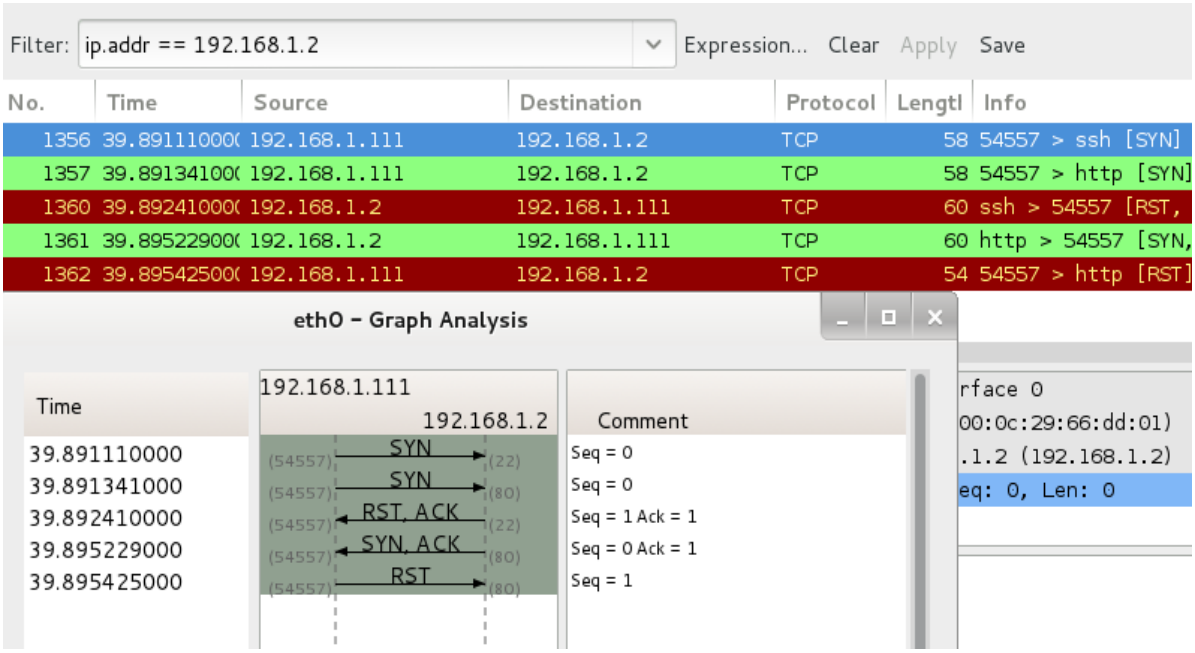


Figura N.- 22b. Muestra el tráfico de las conexiones TCP realizadas hacia los puertos 80 y 22 desde el equipo atacante, aplicando la herramienta Wireshark, luego de aplicar el comando Nmap –sS. Se observa que el 3er paso del Tree way hand shake en lugar de responder el atacante con un ACK, responde con un RST.

Figura N.- 22c. Muestra el registro en el equipo de Seguridad, en donde solo pasa lo permitido que es el puerto http, rechazando ssh.

Resultados Obtenidos por escaneo de Puertos a medio abrir

De igual manera que con las pruebas de escaneo de puertos de tipo abierto, de acuerdo a las pruebas realizadas en la práctica se observa que si el puerto está abierto y el firewall permite el paso de tráfico a pesar de estar el IPS habilitado en la opción recomendada, se obtienen los mismos resultados al no estar habilitado el IPS, es decir se realizaron las pruebas tanto con el IPS deshabilitado y con el IPS habilitado; se ha logrado determinar según los datos arrojados de las pruebas que

por más que se tenga habilitado el IPS si no se encuentra actualizado el mismo como en este caso, el equipo de seguridad no brinda seguridad. En este caso particular el ataque traspasó los filtros 1 y 2.

3.- El escaneo de puertos Sigiloso se relaciona con técnicas que permiten el uso de determinadas banderas, técnicas de sobrepasar filtros, firewalls, routers, entre otras.

En nuestro escenario práctico realizamos en **Sondeo con bandera FIN** con la directiva –sF, se espera que al enviar un paquete con el flag FIN activo, un puerto cerrado responderá con un RST, mientras que los puertos abiertos se quedarán "callados". A continuación verificamos los resultados en el escenario práctico.

Con IPS habilitado.

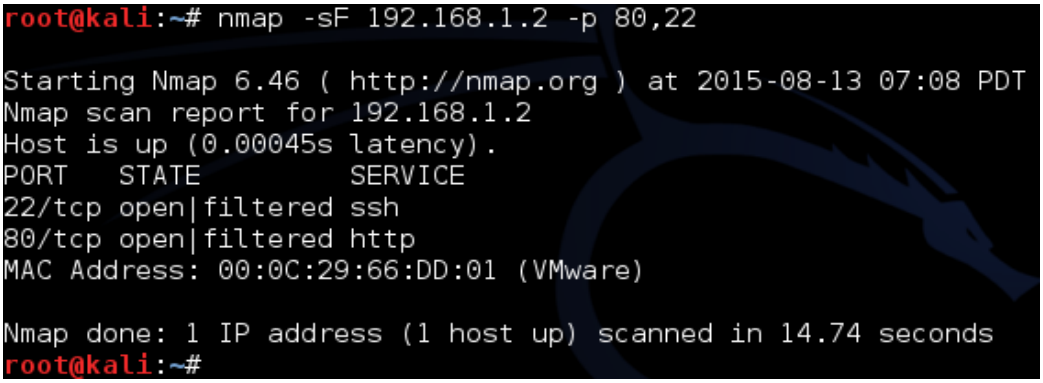


Figura N.-23a. Muestra el resultado de Rastreo Sigiloso Nmap con bandera FIN a los puertos 80 y 22 a la dirección IP 192.168.1.2, se observan los resultados open y filtrados, claramente se observa que el equipo se encuentra detrás de un firewall (filtrados) y la información de los puertos lo toma como open por no recibir respuesta sin embargo, no se recibe respuesta debido a que actúa el módulo IPS impidiendo el paso de tráfico.

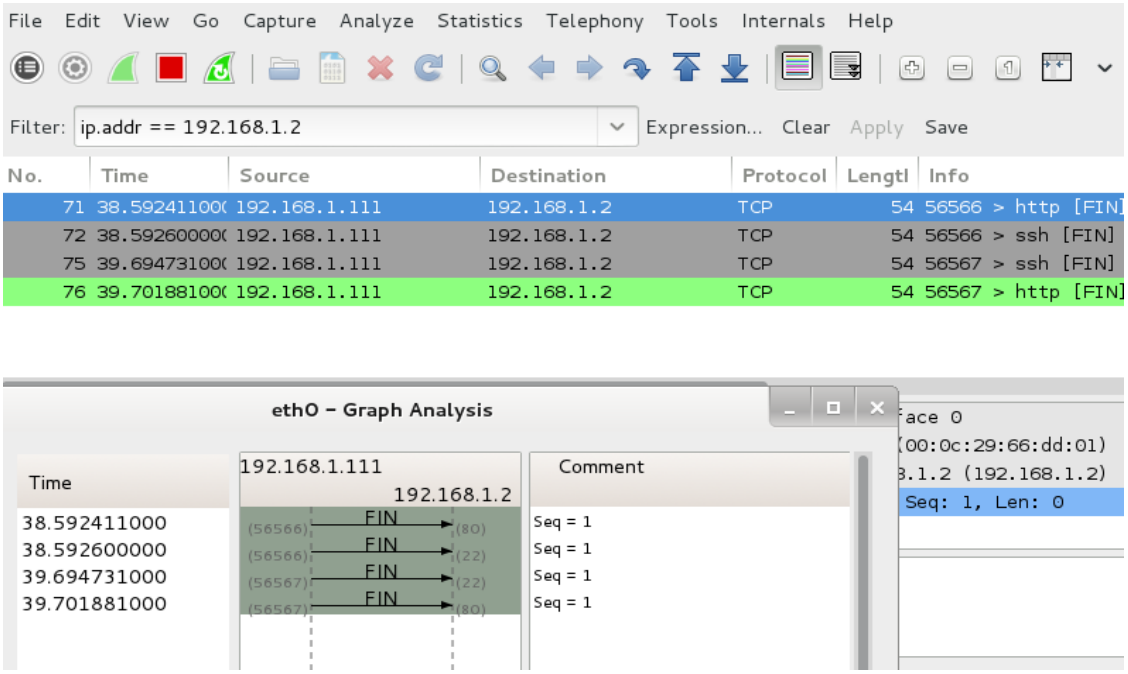


Figura N.-23b. Resultado del Sniffer Wireshark ante rastreo Nmap –sF sobre servidor web, se observa que no se tiene respuesta por parte del servidor.

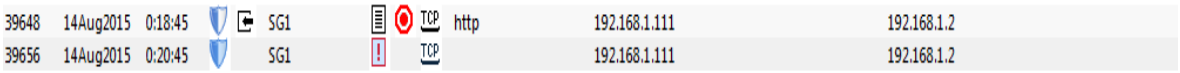


Figura N.-23c. Registros del Firewall en donde no permite el paso de los paquetes debido a que el módulo de IPS lo impide.

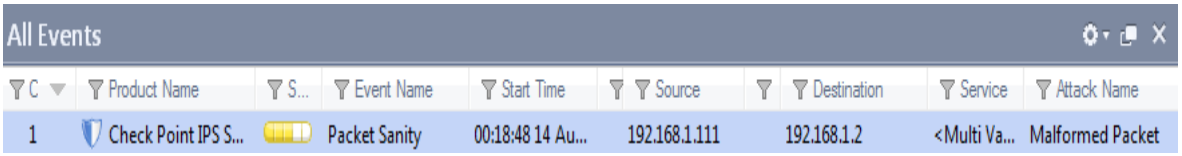


Figura N.-23d. Registro del Módulo Smart Event en donde se reporta actividad del IPS, origen, destino, fecha y hora, nombre de evento y nombre del "Ataque"

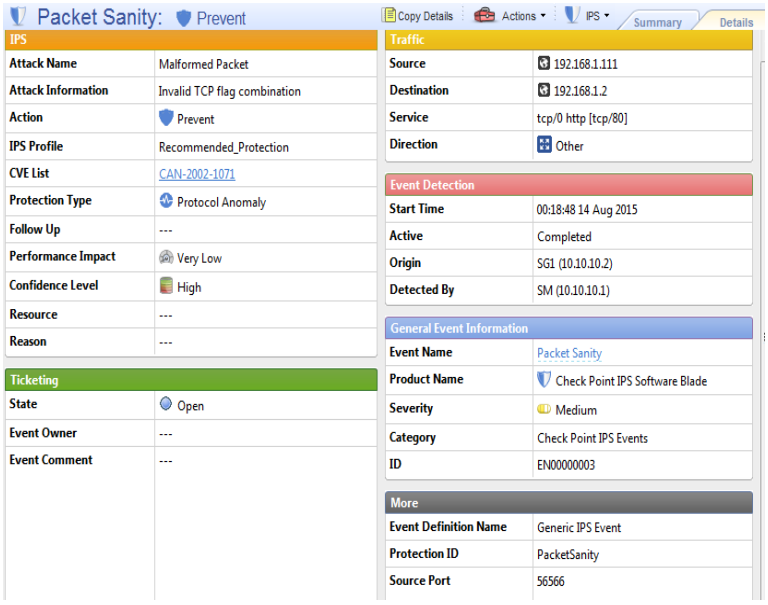


Figura N.-23e. Información sobre la detección escaneo Nmap -sF, reportado por el módulo IPS de Check Point el cual lo considera como ataque de malformación de paquete TCP.

Con IPS deshabilitado.

Al deshabilitar por completo el IPS únicamente las políticas del firewall serán las encargadas en filtrar el tráfico, observemos los resultados de estas pruebas.

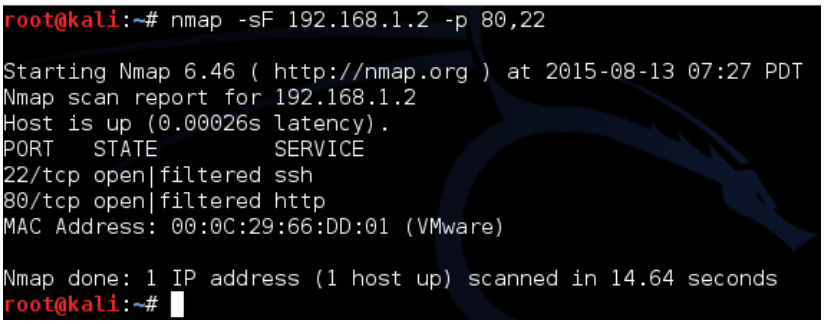


Figura N.- 24a. Resultado del escaneo Nmap a los puertos 80 y 22, aplicado al servidor 192.168.1.2. Con IPS deshabilitado, se observan los mismos resultados que con el IPS habilitado, en esta ocasión no actúa el IPS si no únicamente el módulo de Firewall.

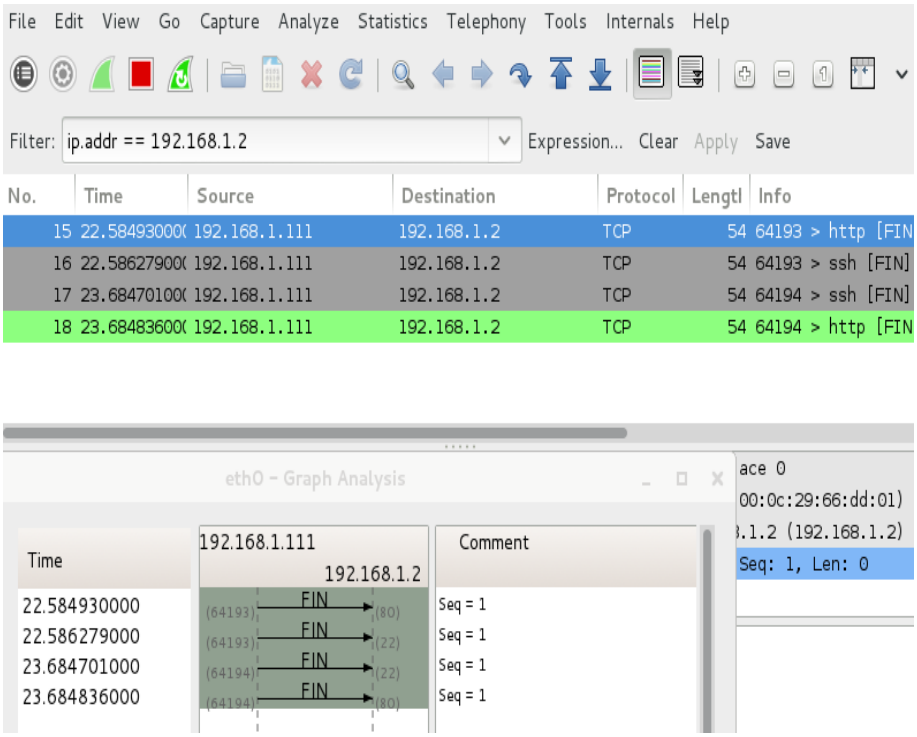


Figura N.-24b. Resultado del Sniffer Wireshark en el equipo atacante cuando se ejecuta escaneo con banderas tipo fin, sin IPS. Se observa que no se tiene respuesta por este motivo el comando Nmap interpreta como open.

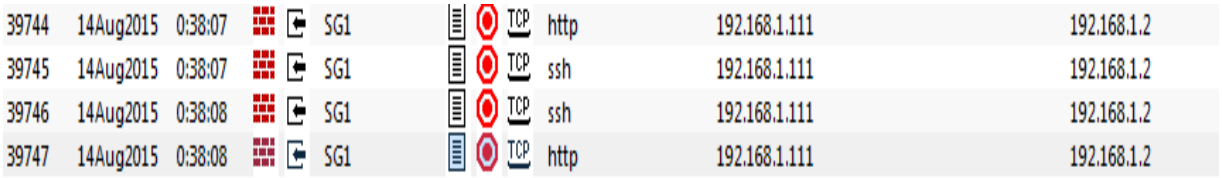


Figura N.-24c. Muestra la actividad en el firewall ante la ejecución del comando Nmap –SF, con el módulo IPS deshabilitado, se observa que no existe tráfico atravesando el firewall debido a que es bloqueado por el equipo de seguridad a pesar de no existir IPS.

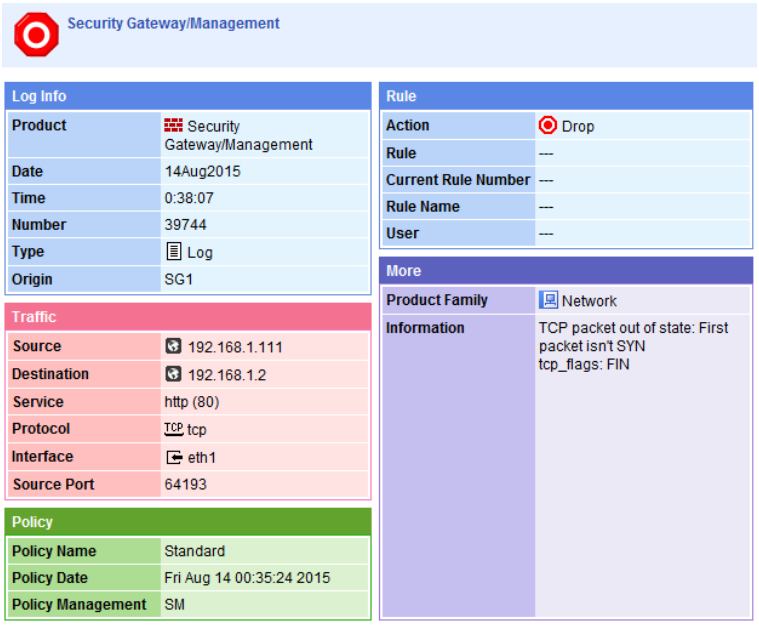


Figura N.-24d. Resultado del equipo de Seguridad Perimetral (modulo firewall), ante un Paquete TCP, se observa que reconoce que el primer paquete no es SYN sino un TCP con bandera FIN activa motivo por el cual es bloqueado.

Si no tuviéramos equipo de Seguridad Perimetral o si tuviéramos otro firewall tipo de firewall el resultado de un puerto cerrado sería:

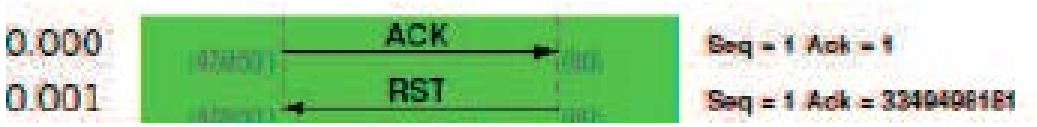


Figura N.-24e. Resultado de escaneo con bandera FIN.

A continuación realizamos una última prueba de rastreo de puertos con Nmap mediante el **Sondeo con bandera ACK**, con este método se pretende analizar el equipo de seguridad perimetral, el objetivo no es conocer si un puerto está abierto o cerrado sino más bien puertos filtrados o no filtrados por un cortafuegos, si el puerto no está protegido por un equipo de seguridad es “no filtrado” por tanto devolverá un rst, a continuación observamos los resultados sobre nuestro escenario práctico.

Con IPS habilitado y deshabilitado tenemos los mismos resultados.

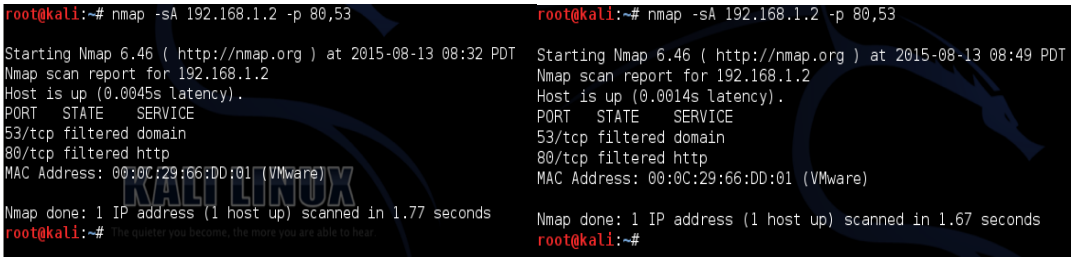


Figura N.-25a. Resultado de escaneo de puertos 80 y 53, de tipo Sigiloso con bandera ACK con y sin IPS, se observa que el resultado indica que se tienen los puertos “filtrados”

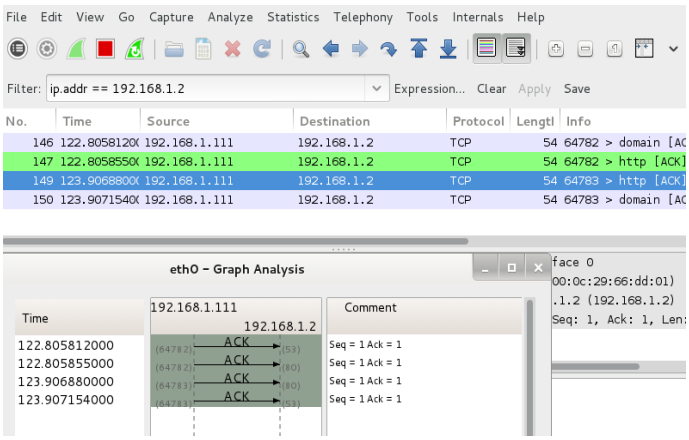


Figura N.-25b. Muestra el resultado de Aplicar un Sniffer Wireshark durante el Escaneo de puertos 80 y 53, de tipo Sigiloso con bandera ACK con y sin IPS. Se observa que no se tiene respuesta de la víctima por tanto son puertos filtrados.

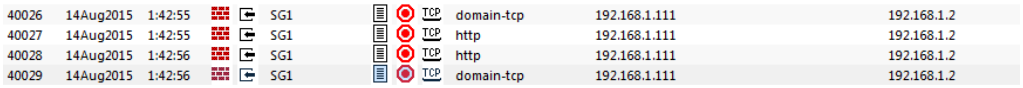


Figura N.-25c. Resultados del análisis de registros en el equipo de Seguridad Perimetral en donde se observa que se impide el tráfico que cursa tanto para el puerto 80 y 53.

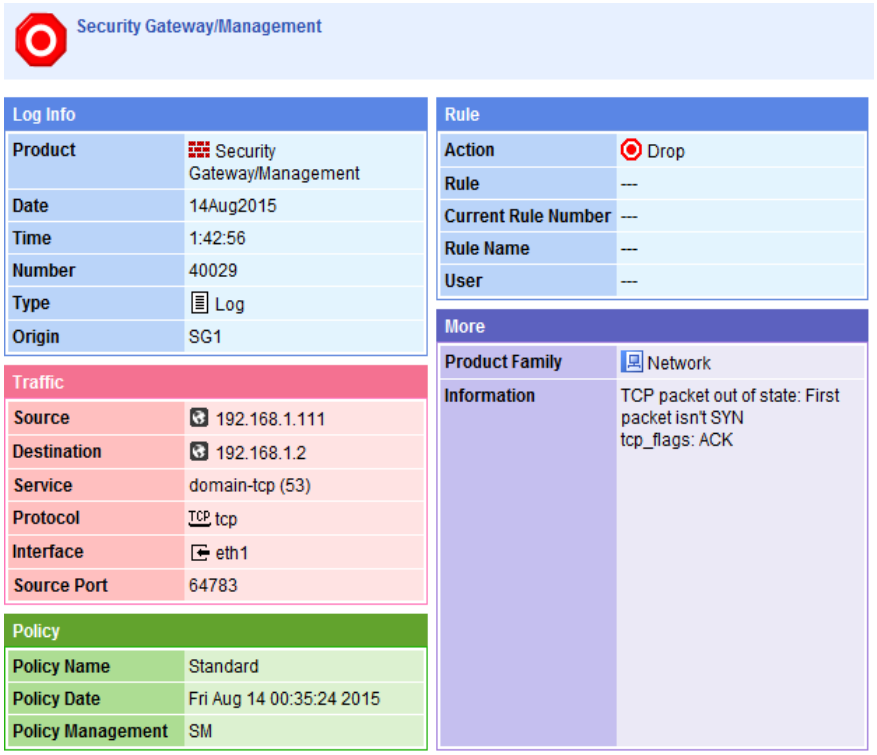


Figura N.-25d. Muestra el resultado del bloqueo del firewall debido a que el primer paquete TCP recibido no es SYN y es ACK.

Resultados Obtenidos por Escaneo de Puertos de Tipo Sigiloso.

Podemos observar que el módulo de firewall trabaja correctamente cuando recibe paquetes TCP a pesar de no estar habilitado el IPS, verificando las banderas activas y en caso de recibir un paquete TCP que no sea inicial SYN de inmediato bloquea el tráfico.

Resumen de pruebas con Nmap

A continuación se muestra un resumen de las pruebas Nmap realizadas.

Análisis y Escaneo de Puertos				
ITEM	DESCRIPCION	ESCANEO REALIZADO	PUERTOS ANALIZADOS	RESULTADO
1	ESCANEO DE TIPO ABIERTO O FULL	nmap -St	80,21	PUERTO 80 ABIERTO, 21 CERRADO - CON Y SIN IPS LOS MISMOS RESULTADOS
2	ESCANEO A MEDIO ABRIR	nmap -Ss	80,22	PUERTO 80 ABIERTO, 21 CERRADO - CON Y SIN IPS LOS MISMOS RESULTADOS
3	ESCANERO SIGILOSO	nmap -Sf	80,22	IPS DETECTA,
		nmap -Sa	80,53	IPS NO DETECTA . FIREWALL DETECTA

Tabla N.-6. Resultado de Pruebas de puertos con Nmap.

Análisis de Vulnerabilidades con herramientas dedicadas.

Un analizador de vulnerabilidad es una aplicación que permite efectuar una comprobación de seguridad mediante el análisis de puertos abiertos en los equipos que forman parte de la red , dentro del proceso de análisis se emplean mecanismos que permiten determinar qué servicios se están ejecutando e identificar los riesgos de seguridad de acuerdo a su base de datos de vulnerabilidades, existen varias herramientas dedicadas cuyo objetivo es entregarnos una serie de resultados de vulnerabilidades obtenidas y recomendaciones, entre los escáneres de vulnerabilidades más conocidos podemos nombrar a Nessus, Openvas, Nikto, Qualys, Uniscan, etc.

Cada una ofrece ciertas ventajas frente a las otras, en nuestro escenario práctico realizaremos un análisis de nuestro servidor web con herramientas Nessus, Nikto, y uniscan.

Inicialmente procedemos con la instalación de la herramienta Nessus en una versión demo, teniendo en cuenta nuestro objetivo que es la dirección ip 192.168.1.2 que es la dirección pública (escenario virtual) a continuación se muestran los resultados obtenidos.

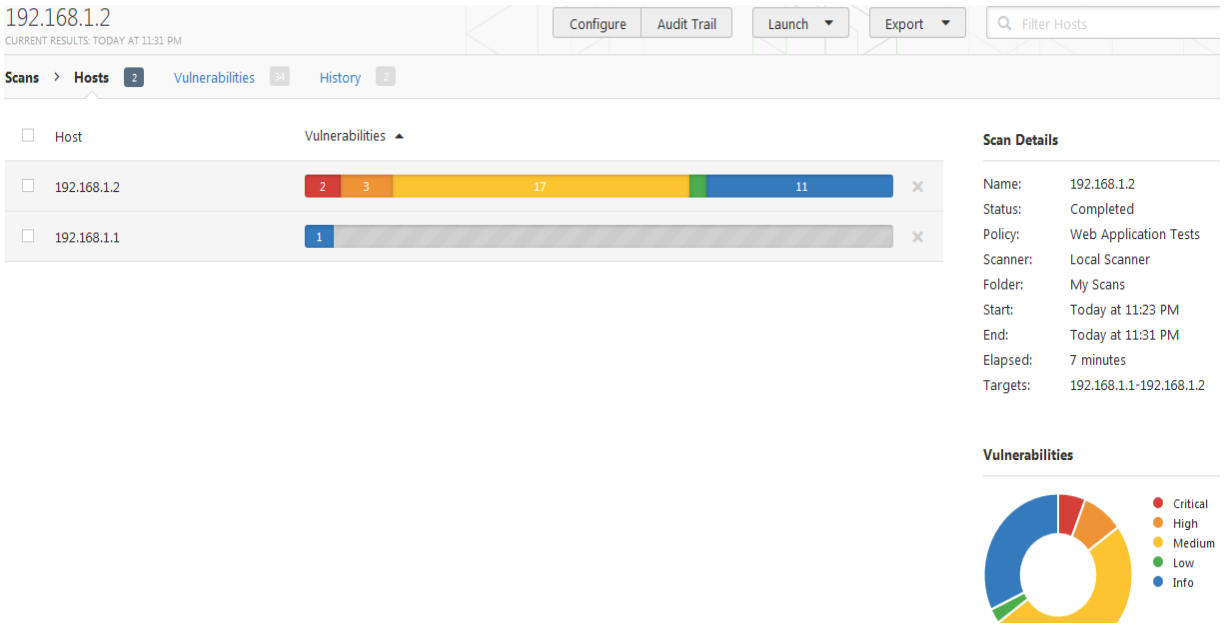
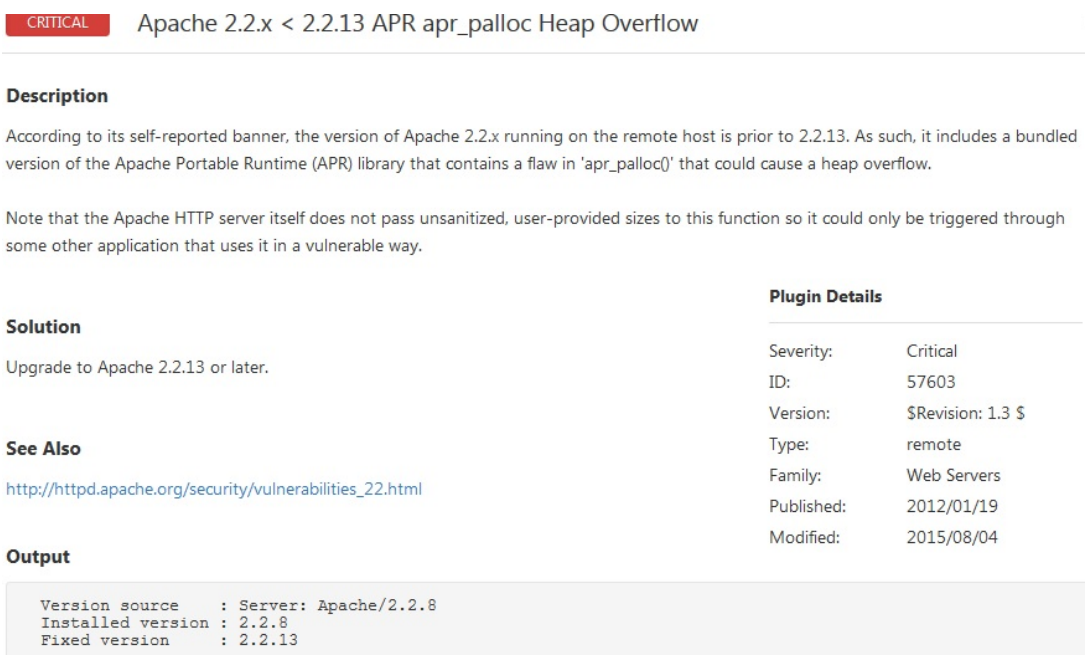


Figura N.-26. Muestra los Resultados gráficos del Análisis de Vulnerabilidad sobre del Servidor Web con la herramienta Nesus, se observa 34 vulnerabilidades en el servidor víctima del Escenario Virtual.

La herramienta Nessus nos permite exportar el reporte de vulnerabilidades de Nessus el cual es bastante completo, que en nuestro escenario práctico arrojó 48 páginas con 34 vulnerabilidades (recogidas del reporte)

Figura N.-27. Vulnerabilidades encontradas en Servidor Web del escenario de Pruebas, en orden desde la más crítica hasta la más leve de acuerdo con la herramienta Nessus. Se muestra 2 vulnerabilidades críticas, las cuales se muestran a detalle en las siguientes figuras.



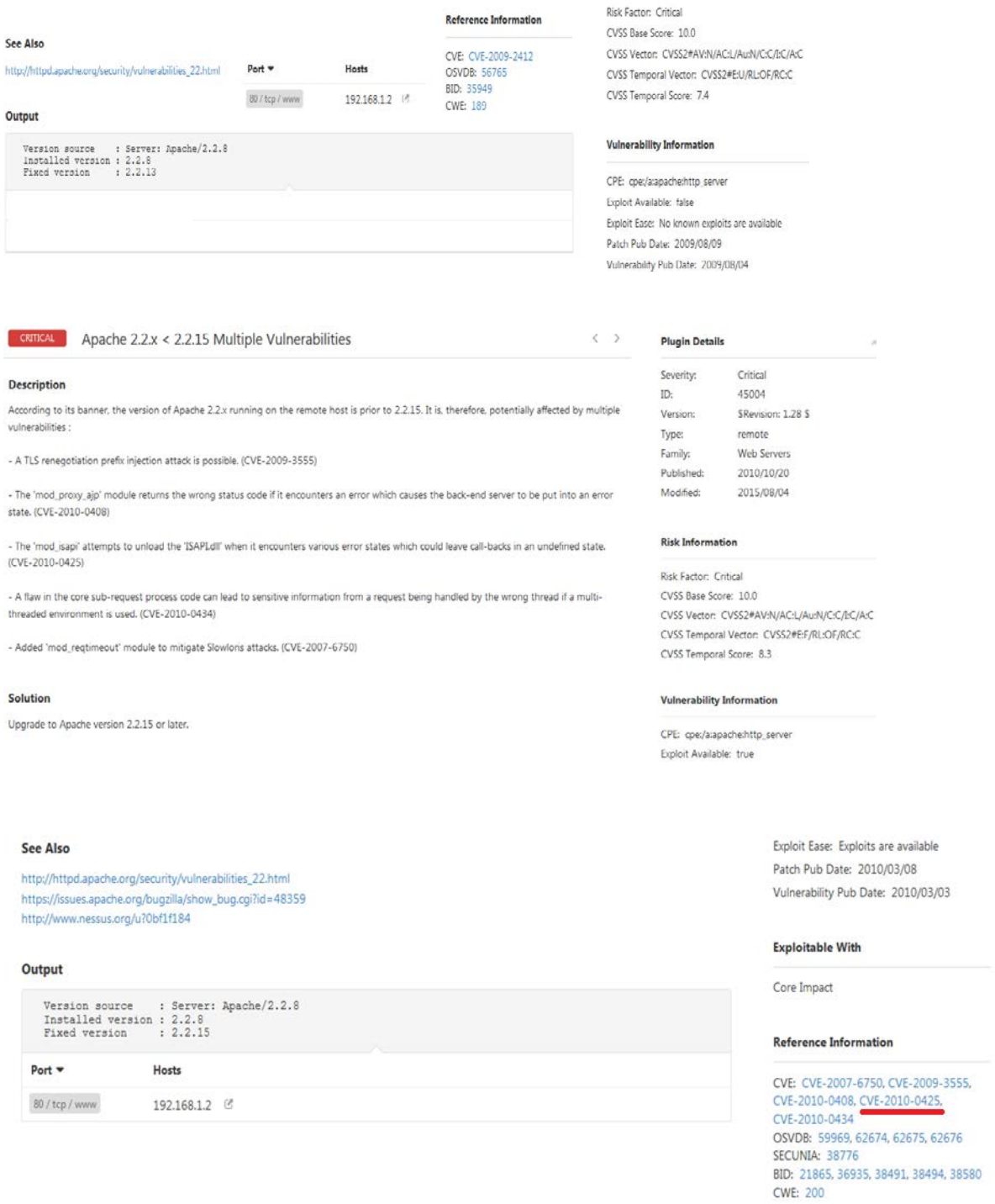


Figura N.-28. Muestra las vulnerabilidades de Nivel Critico reportadas por la herramienta Nessus. Se observa varios códigos CVE uno de los cuales vamos a elegir para desarrollar un exploit.

A manera de comprobación, mostramos otro analizador de vulnerabilidades llamado Nikto que está incluido en la herramienta Kali.

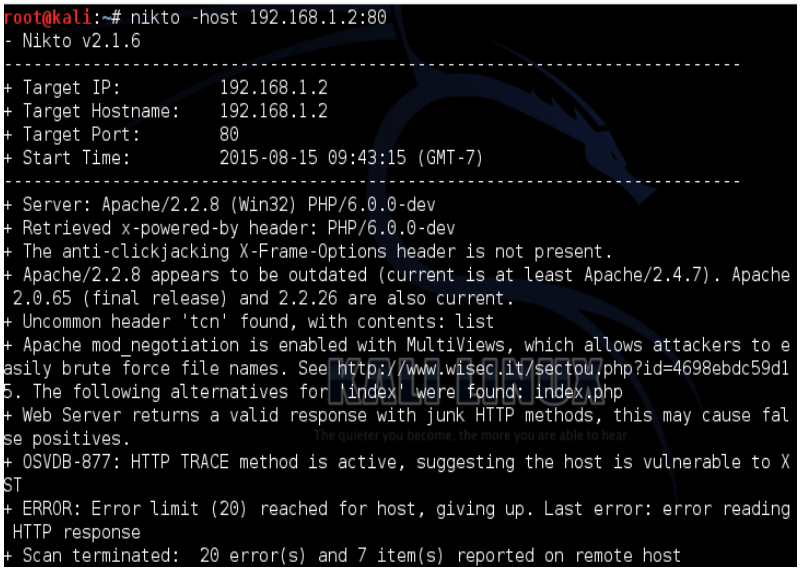


Figura N.-29. Vulnerabilidades reportadas por la herramienta de Software Nikto, sus resultados hacen mención que la versión de apache esta desactualizada.

Finalmente utilizamos otra herramienta incluida en Kali Linux llamada Uniscan, que nos entrega los siguientes resultados.

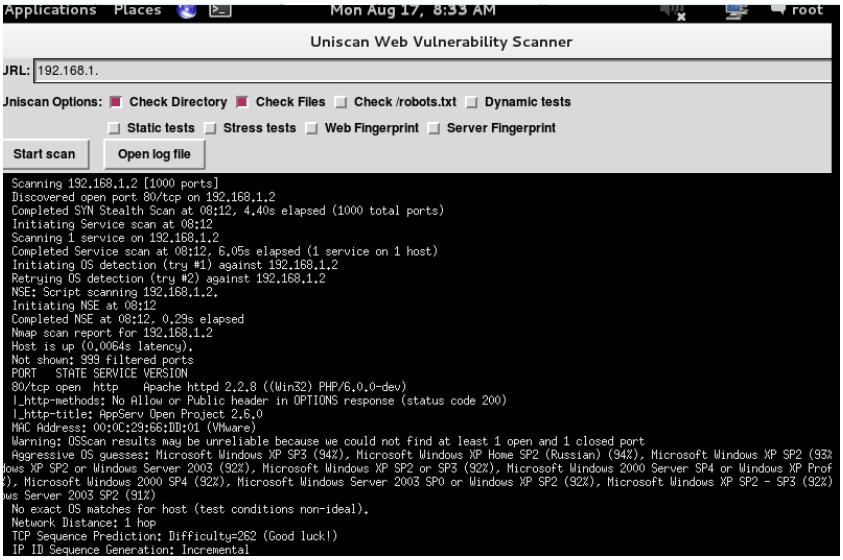


Figura N.-30. Muestra los resultados del scanner de vulnerabilidades Uniscan, se observa que arroja resultados de puertos abiertos y sistema operativo.

Escaneo de Vulnerabilidades en el Servidor Real.

Tomando las consideraciones anteriores en la cual ejecutamos el análisis de vulnerabilidades sobre el servidor web virtual, realizamos el mismo procedimiento con el servidor Real (Proxy Reverso) y con el Servidor Windows con la herramienta Nessus y en el primer caso obtuvimos 51 vulnerabilidades, con estos resultados se procedió a realizar una actualización del sistema operativo con el comando yum update y se redujeron las vulnerabilidades a 9; adicionalmente se realizó un cambio de contraseña por una más fuerte, en la realidad, aparte de reducir las vulnerabilidades, se redujo el consumo del procesador al 50%.

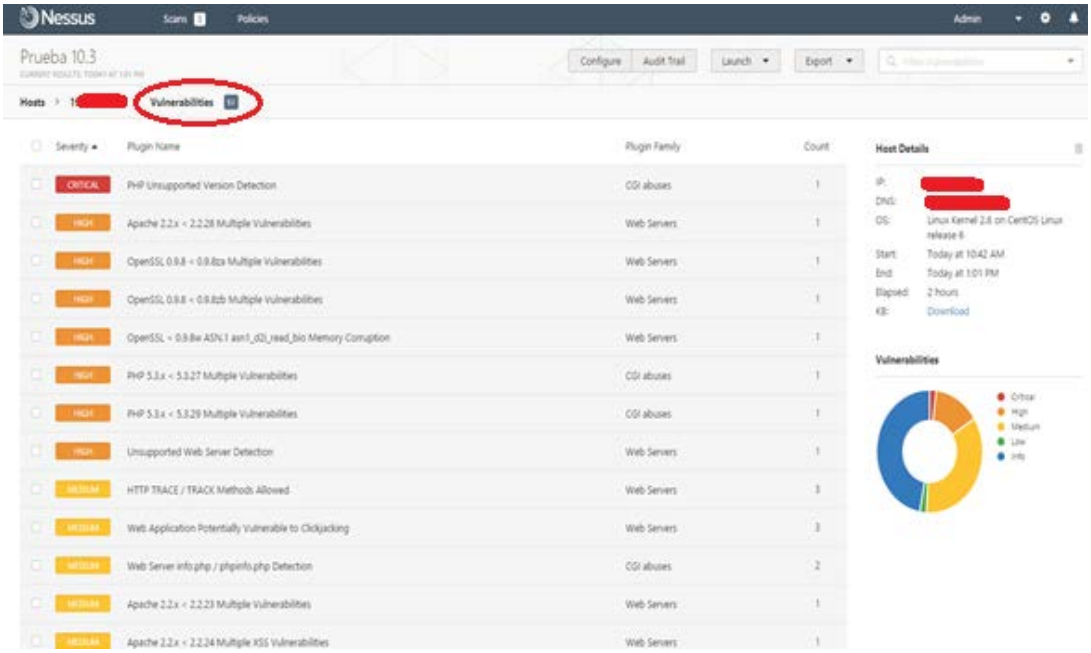


Figura N.- 31. Muestra el resultado del análisis de vulnerabilidades sobre el sitio web real con la Herramienta Nessus. El resultado arroja 51 vulnerabilidades, de las cuales una es considerada crítica.

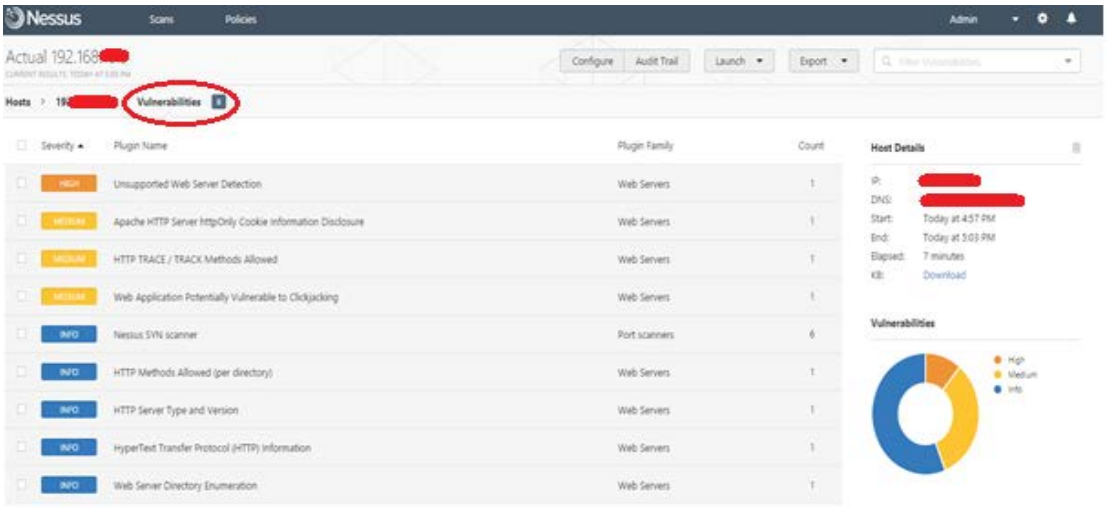


Figura N.-32. Muestra el resultado del análisis de vulnerabilidades sobre el sitio web real con la Herramienta Nessus. El resultado arroja luego de la actualización del sistema operativo 9 vulnerabilidades, ninguna considerada crítica.

Para el caso del servidor Windows, se tuvieron 41 vulnerabilidades las cuales 1 es crítica y se mantiene en continuo análisis para disminuir la cantidad de vulnerabilidades actuales.

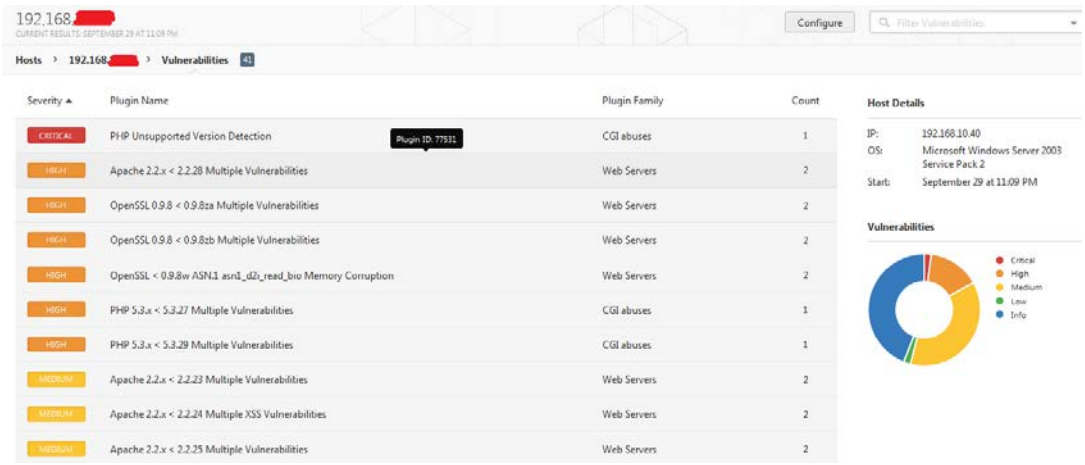


Figura N.-33. Cantidad de Vulnerabilidades reportadas sobre el servidor Windows Actual de la Infraestructura real.

Ataques a la Red Propuesta (Objetivo Servidor Web)

De acuerdo con la definición citada en la pag.53, “se considera ataque al proceso de acceder a un equipo objetivo y la manipulación de este sin consentimiento” además como se indicó también en la página 33 “Las pruebas de penetración pueden realizarse utilizando herramientas de software de ataque automatizadas o manualmente”

Lo indicado en líneas anteriores, junto a la información obtenida hasta el momento (resultado del análisis de puertos y vulnerabilidades) llamado también vector de ataque se procede a realizar una serie de ataques iniciando con la explotación de una de las vulnerabilidades sacadas a la luz por el analizador Nessus.

En nuestro escenario práctico realizaremos un exploit que ataque la vulnerabilidad CVE-2010-0425 visible. Para esto requerimos de una herramienta llamada Metaexploit, en donde se requiere ejecutar un conjunto de comandos desde su consola que nos permite Generar el Exploit y posteriormente configuramos los parámetros necesarios para vulnerar el servidor web, como se muestra en las figuras 27 y 28 mostradas a continuación.

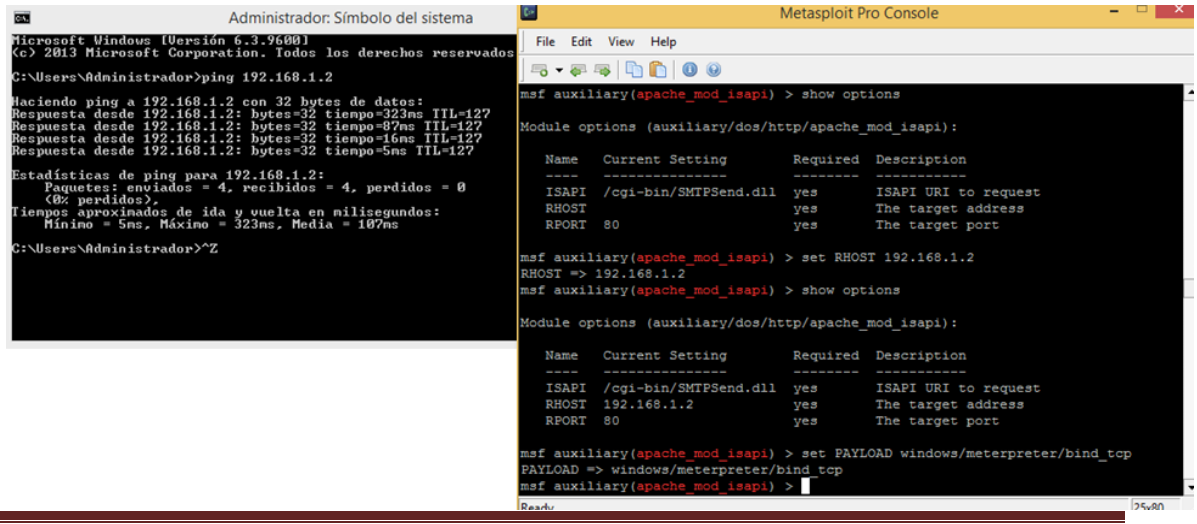


Figura N.-34. En la parte izquierda nos aseguramos mediante ICMP que tenemos comunicación con el servidor web víctima. En la parte derecha observamos una serie de comandos ejecutados en la consola de la herramienta Metaexploit necesarios para explotar la vulnerabilidad CVE-2010-0425.

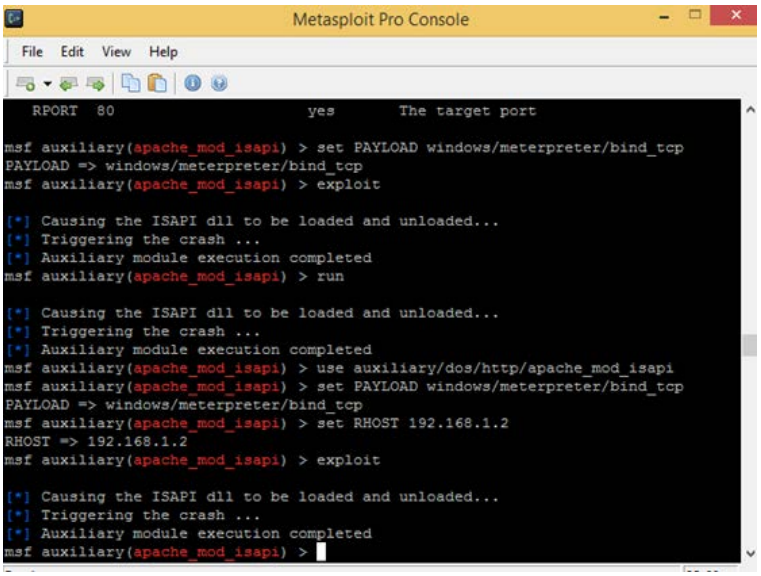


Figura N.-35. Muestra los resultados de la ejecución de comandos necesarios para explotar la vulnerabilidad.

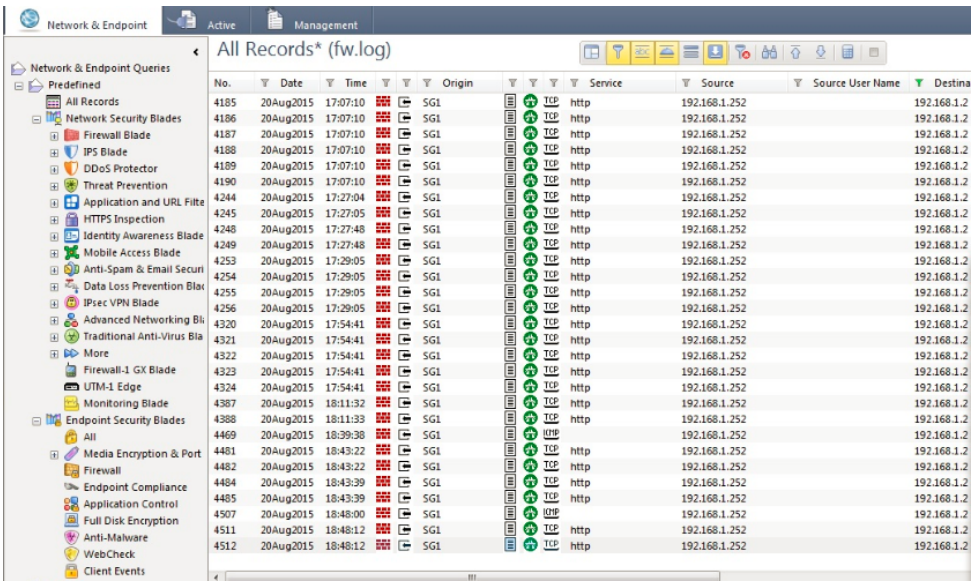


Figura N.-36. Muestra el tráfico registrado en el Firewall mientras se ejecuta el exploit. Se observa que únicamente pasa el tráfico permitido que es https, el cual es el suficiente para obtener el resultado de explotación de la vulnerabilidad.

Para eliminar esta vulnerabilidad se deberá actualizar la versión de apache de acuerdo con el diccionario de vulnerabilidades, a continuación se muestra la vulnerabilidad reportada.

Figura N.-37. Información acerca de la vulnerabilidad Explotada Código CVE-2010-0425 escogida para el análisis.

Herramienta metaexploitable2.

Existen disponibles herramientas con fines académicos que poseen varias vulnerabilidades que permiten ser explotadas y por ejemplo observar los resultados previos a realizar las pruebas de penetración sobre equipos que se encuentren en producción, su interfaz web se muestra en la siguiente figura.

Figura N.- 38. Muestra la Herramienta Metaexploitable 2, en la parte izquierda se observa la consola web una vez instalada la herramienta. En la parte derecha se observa que agregando (?-s) al final de la ruta http, se ejecutó un ataque de inyección de código.

Ataque de Denegación de Servicio.

Objetivo.

Consiste en dar de baja el servidor web, por medio de saturación del servicio, hacia la dirección pública del servidor.

Proceso

En nuestro escenario práctico usaremos un script llamado slowloris hecho en Perl (parecido a C) que implementa una potente e inteligente manera de generar una denegación de servicio sobre un servidor web, para esto se basa en la cantidad de peticiones que es capaz de mantener un servidor web de manera concurrente, la forma de saturar el pool de servicios es mediante la creación de “request” a http (también funciona con https) de manera que se empiezan a enviar muchas cabeceras al servidor web de manera de forzar a mantener abierta las conexiones por parte del servidor, por lo general los servidores tienen configurado un

determinado número máximo de sokets permitidos en los archivos de configuración, de manera que el servidor llega a su límite, se satura y no es más accesible.

Que se va a atacar.

El servidor web que en nuestro caso es el 192.168.1.2

Pruebas a Ejecutar (Sin Firewall y con Firewall)

Antes de Ejecutar ningún ataque se comprueba el acceso al servidor web mostrado a continuación.

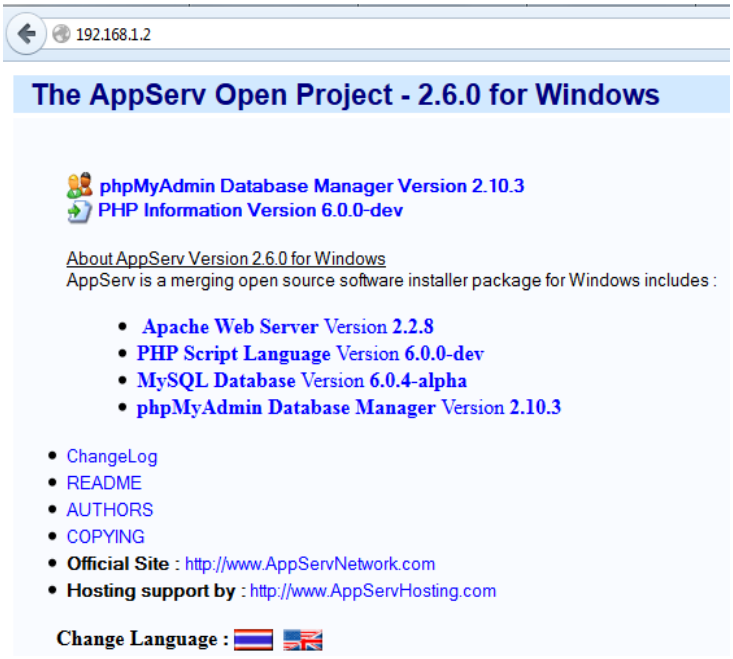


Figura N.-39. Muestra el contenido de la aplicación Web del equipo víctima.

Posteriormente se procede a ejecutar el archivo solowloris.pl (script hecho en Pearl) desde Kali hacia el servidor web por medio del siguiente comando desde el equipo Kali Linux:

```
root@kali:~/Desktop# perl ./slowloris.pl -dns 192.168.1.2 -port 80
```

Resultados sin IPS.

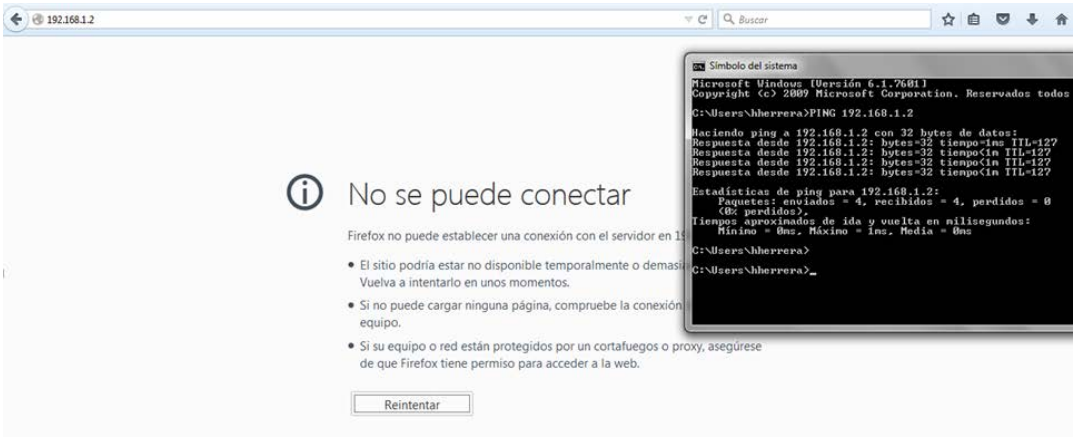


Figura N.- 40. Muestra el resultado de ejecutar el ataque de denegación de servicios, se muestra que el sitio web publicado está caído.

13193	23Aug2015	2:37:56	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13194	23Aug2015	2:37:56	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13195	23Aug2015	2:37:57	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13196	23Aug2015	2:37:57	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13197	23Aug2015	2:37:57	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13198	23Aug2015	2:37:57	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13199	23Aug2015	2:37:57	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13200	23Aug2015	2:37:57	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13201	23Aug2015	2:37:58	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard
13202	23Aug2015	2:37:58	SG1	TCP	http	192.168.1.102	192.168.1.2	3	3-Standard

Figura N.- 41. Muestra el tráfico registrado en el firewall mientras se ejecuta el ataque de denegación de servicio.

Resultados con IPS.

Los mismos resultados.

Formas de Contrarestar este tipo de ataque

1. Limitar la tasa de tráfico proveniente de un único host.
2. Limitar el número de conexiones concurrentes al servidor.
3. Restringir el uso del ancho de banda por aquellos hosts que cometan violaciones.
4. Realizar un monitoreo de las conexiones TCP/UDP que se llevan a cabo en el servidor (permite identificar patrones de ataque).

Ataque de hombre en el medio (MIM). Suplantación de Identidad o Arp Spoofing

Objetivo.

Consiste en interceptar la conexión o la comunicación que se establece entre un equipo (víctima) y su Gateway (router) usurpando la identidad del router haciendo que los paquetes que envíe la victima al router sean vistos o pasen primero por el atacante.

Proceso

Para realizar este ataque requerimos de un sniffer, en nuestro escenario práctico usamos ethercap-graphic incluido en la herramienta Kali Linux, la siguiente figura muestra la detección de la lista de host conectados en la red incluida el router.

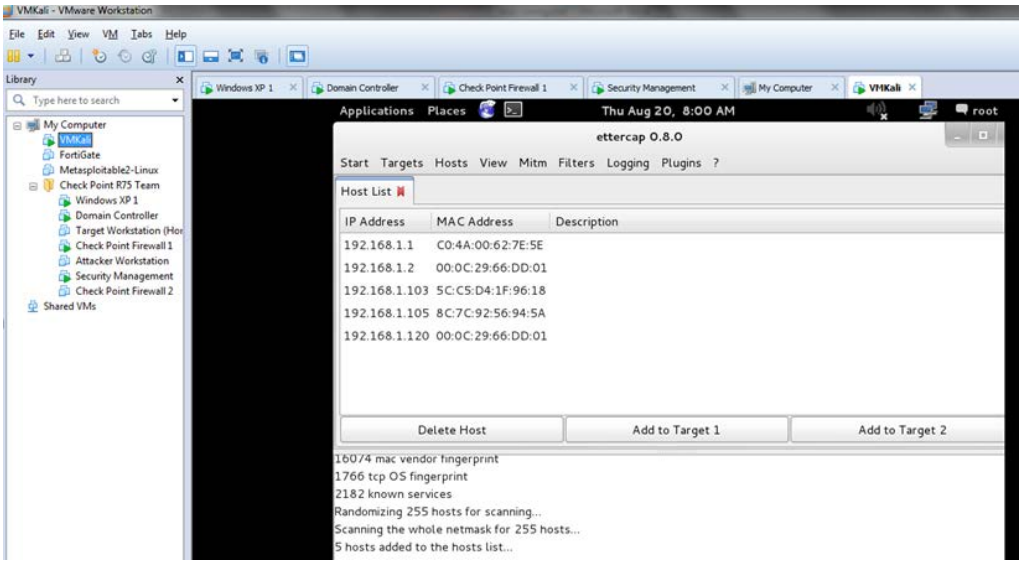


Figura N.-42. Direcciones IP que muestra el sniffer Ethercap necesarios para ejecutar el ataque de hombre en el medio.

Que se va a atacar

Los equipos que se encuentran en la red de laboratorio, el objetivo es conocer una contraseña que un equipo victima envía al internet por medio de un router, interceptando la comunicación.

Pruebas a Ejecutar (Sin Firewall y con Firewall)

Sin firewall.

Ejecutamos lo indicado a continuación con la herramienta Ethercap.

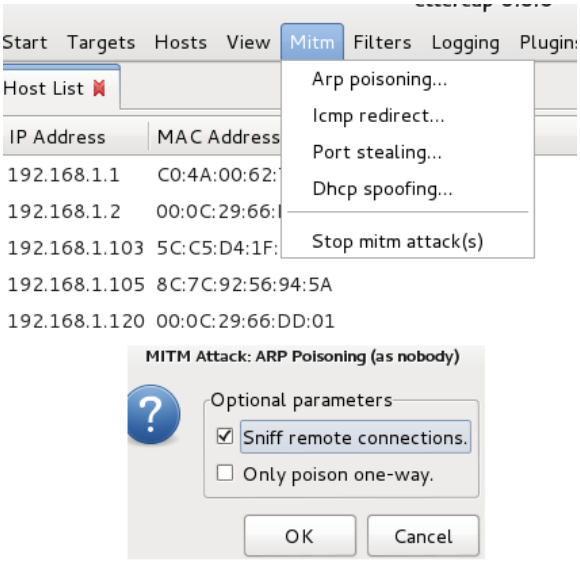


Figura N.-43. Configuración para envenenamiento ARP, mediante Ethercap, para el ataque de hombre en el medio MIM.

A continuación ejecutamos los comandos que nos permiten redirigir el tráfico del puerto 80 hacia el puerto 10000 e iniciar el servicio sslstrip para poder capturar credenciales https.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat-A PREROUTING -p tcp --destination-port 80 -j REDIRE
CT --to-port 10000
Bad argument `PREROUTING'
Try `iptables -h' or 'iptables --help' for more information.
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 10000
root@kali:~# locate sslstrip.py
/usr/share/sslstrip/sslstrip.py
root@kali:~# pwd
/root
root@kali:~# cd ..
root@kali:/# cd /usr/share/sslstrip
root@kali:/usr/share/sslstrip# python sslstrip.py -l 10000

sslstrip 0.9 by Moxie Marlinspike running...
```

Figura N.-44. Configuración para reenvío de tráfico del puerto 80 al puerto 10000 y modificación de archivo sslstrip para que se escuche en el puerto 10000.

A continuación realizaremos una prueba verificando con el sniffer ethercap que escuche el tráfico de la red y nos entregue resultados.

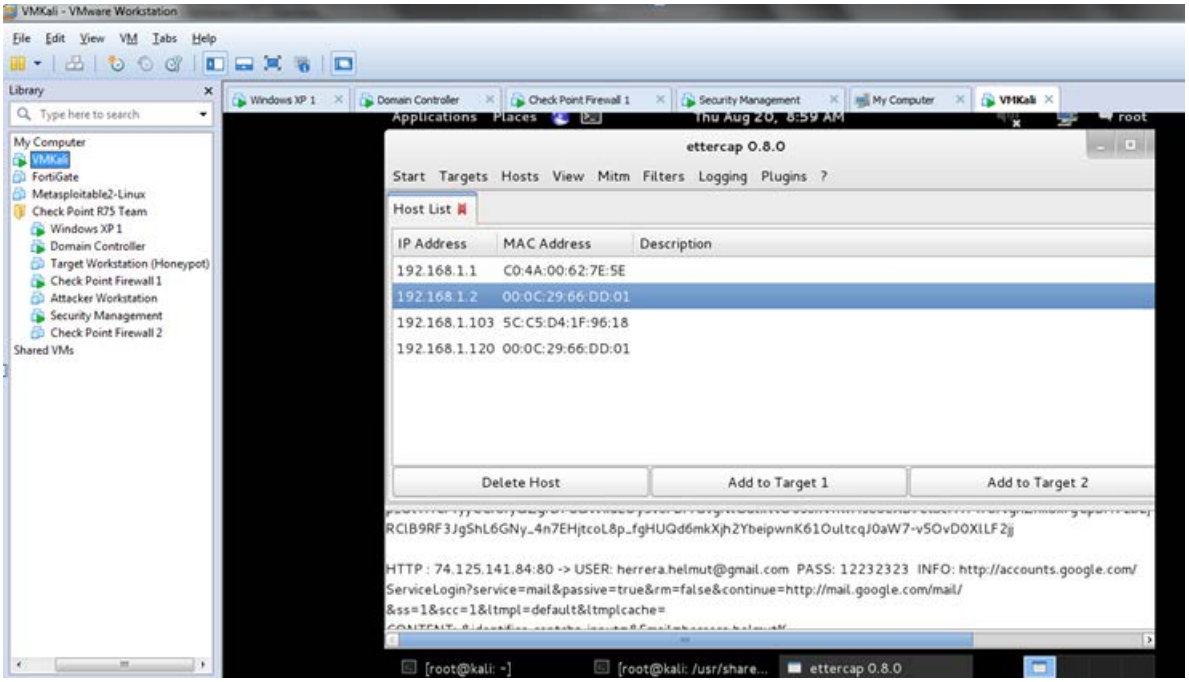


Figura N.- 45. Resultados del ataque de Hombre en el medio, se observa la contraseña ingresada.

Con IPS activado, se observan los mismos resultados.

Formas de Contrarestar este tipo de ataque

- Descargar la última versión del navegador.
- Adoptar EV SSL y eduque a usuarios del significado del brillo o color verde en la barra de navegación.
- Usar credenciales de autenticación tales como tokens (autenticación de dos factores) para acceso.

Ataque de Ingeniería Social o Phishing

Objetivo

Este tipo de ataque intenta inducir o influenciar a un usuario a revelar su información sensible como claves de acceso y de esta forma obtener credenciales de la víctima. Las credenciales más comunes y fáciles de obtener son de correos electrónicos, redes sociales, banca en línea en donde se puede obtener sin ningún problema contraseñas, PIN de seguridad, etc.

Proceso

El medio por el cual se ejecuta el ataque es el envío de información y solicitudes al correo electrónico de la víctima. Estos correos electrónicos contienen un comunicado que de alguna forma llama la atención del usuario mediante una advertencia, una promoción o la explotación de su curiosidad y lo obliga a acceder a un link que supuestamente lo llevará al sitio web perteneciente a su banco, cuenta de correo electrónico personal o red social, sin embargo la página web a la que es dirigido es una página Clonada muy parecida a la original y es utilizada para capturar la información otorgada por el usuario atacado. Vamos a utilizar el ejemplo de

Facebook que es el más sencillo para una demostración, cualquier otra página tendría el mismo principio.

Ahora bien, la página desarrollada en este ataque es exactamente igual a la original, y con la herramienta Kali Linux se genera automáticamente una copia de la original, la pregunta ahora es, como llegar al usuario?, en este caso lo realizaremos por el correo electrónico, esto se consigue fácilmente gracias a las millones de cadenas y SPAM que ofrecen dar suerte en el dinero y suerte en el amor, los atacantes llegan a tener millones de cuentas de correo en su poder.

Que se va atacar

En la siguiente figura se muestra una prueba de correo electrónico fraudulento, en donde el atacante se hace pasar por Facebook y se solicita al usuario que actualice sus datos inmediatamente, por tanto la victima puede ser cualquier usuario.

Figura N.-46 Muestra el resultado de un Ataque de Phishing mediante email.

Este correo fraudulento se puede enviar fácilmente desde cualquier servidor de correo que no tenga implementadas las respectivas protecciones, en este caso se trata de uno de pruebas. El remitente puede engañar al usuario que recibe el

correo porque el dominio indica que proviene de Facebook.com que hace muy convincente el correo, el mensaje utilizado (por el atacante) utilizaría un mensaje que incite al usuario que de click en el link adjunto y que supuestamente lo llevara a la página de Facebook para actualizar sus credenciales, sin embargo link adjunto como se puede ver, no redirecciona a Facebook.com si no a un servidor web que puede estar en Internet o en la red interna y alberga una página muy similar a Facebook.

Si todo marcha bien y el usuario es engañado, se ingresará al link enviado y pasará a ser uno más de los millones de usuarios engañados anualmente, solo en américa latina en el 2014 el promedio de usuarios afectados por phishing supera los 100 millones (Kaspersky, 2014).

Pruebas a Ejecutar

Como se mencionó anteriormente, la página en cuestión puede ser clonada con herramientas libres, o desarrolladas con un editor HTML, en este caso se ha utilizado Kali para clonar la página de Facebook.

Figura N.-47. Clonación de Pagina

Las credenciales ingresadas se muestran en la Figura N.-44 y es un intento exitoso de robo de credenciales con ingeniería social Phishing mediante la herramienta Kali. Ahora bien, este ejemplo es exactamente igual para otros sistemas, como correos electrónicos, bancos, etc., cualquier sistema que el usuario deba ingresar credenciales u otorgar información sensible.

Es muy común que los firewalls actuales sean tan sofisticados que mantengan una lista actualizada de IPs de riesgo o talvez países que estén dentro de las listas negras como países con mayor índice de ataques informáticos (Demidova, 2014), sin embargo los especialistas de seguridad informática no deben olvidar de la existencia de la red TOR, que si bien es cierto fue creada para mantener el anonimato y es ampliamente utilizada por WikiLeaks, también puede ser utilizada ocultar la dirección pública por lo tanto las listas negras publicadas por estos antivirus no sería de mucha ayuda.

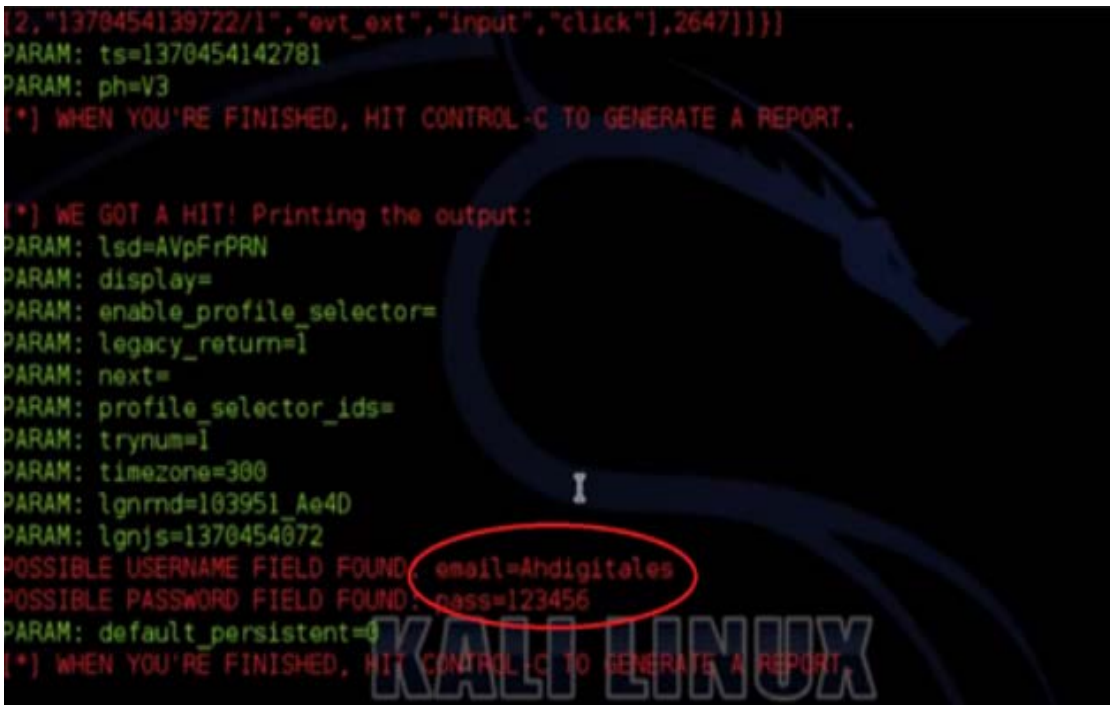


Figura N.-48. Obtención de Credenciales con Kali

Formas de Contrarestar ataques de phishing.

- Identificar correos electrónicos sospechosos
- Verificar el origen de los correos electrónicos recibidos.
- Nunca ingresar al sitio web de un banco mediante links de acceso.
- Introducir datos únicamente en sitios web seguros https:// y con un candado.
- Asegurar el computador con antivirus y antimalware.
- Revisar continuamente las cuentas para estar prevenido.
- El phishing no solo trabaja a nivel de banca on line sino de otros sitios que manejan de dinero.
- Ante una mínima duda, es mejor no abrir un correo dudoso.

Ataque mediante Herramienta de Generación Automática Aleatoria de Ataques.

Objetivo

El objetivo de esta generación aleatoria de ataques es comprobar el funcionamiento del equipo de seguridad perimetral propuesto y verificar el funcionamiento del IPS en el caso que exista una regla que permita el pasó de paquetes en ciertos puertos.

Proceso

Para la consecución del objetivo planteado debemos habilitar la opción recomendada en el IPS y generar en el equipo de seguridad perimetral un escenario con reglas permisivas es decir que cualquier origen llegue a cualquier destino y

viceversa, es decir una regla any to any, que deja pasar todo tipo de tráfico como se muestra.

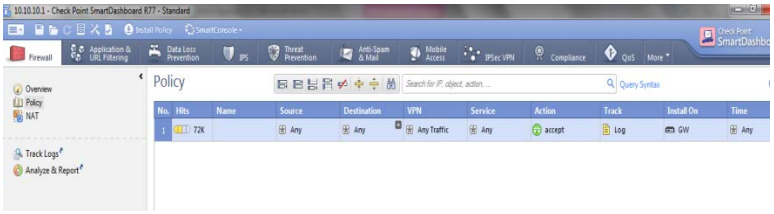


Figura N.-49. Muestra un Regla permisivas que permite todo tipo de tráfico desde cualquier origen a cualquier destino.

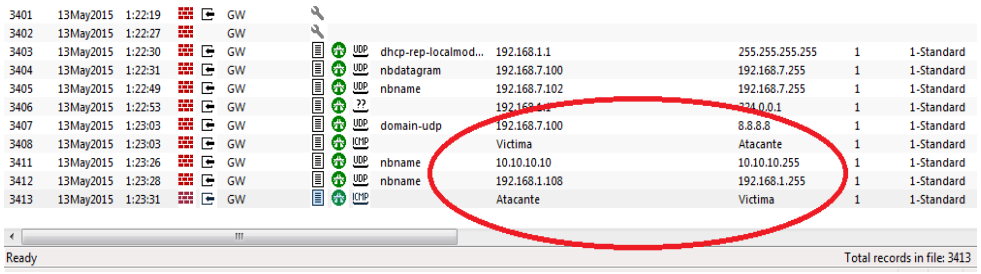
La herramienta para la ejecución de estos ataques es descargable del siguiente link: https://www.checkpoint.com/forms/lead.htm?formId=000001.

Una vez que instalamos la máquina virtual (tanto para el atacante como en la victima) debemos realizar las configuraciones pertinentes que permitan establecer un equipo como atacante y al otro como víctima, configurando entre otras opciones la red en la que se encuentra cada uno.

Que se va a atacar

La víctima en este caso es un equipo dentro de la red LAN configurada como víctima (similar a un Metaexploitable 2).

A continuación procedemos a probar la comunicación entre el equipo atacante y el equipo víctima con una herramienta de Check Point que visualiza los registros como se muestra:



3401	13May2015	1:22:19		GW						
3402	13May2015	1:22:27		GW						
3403	13May2015	1:22:30		GW	UDP	dhcp-rep-localmod...	192.168.1.1	255.255.255.255	1	1-Standard
3404	13May2015	1:22:31		GW	UDP	nbdatagram	192.168.7.100	192.168.7.255	1	1-Standard
3405	13May2015	1:22:49		GW	UDP	nbname	192.168.7.102	192.168.7.255	1	1-Standard
3406	13May2015	1:22:53		GW	??		192.168.1.1	224.0.0.1	1	1-Standard
3407	13May2015	1:23:03		GW	UDP	domain-udp	192.168.7.100	8.8.8.8	1	1-Standard
3408	13May2015	1:23:03		GW	ICMP		Victima	Atacante	1	1-Standard
3411	13May2015	1:23:26		GW	UDP	nbname	10.10.10.10	10.10.10.255	1	1-Standard
3412	13May2015	1:23:28		GW	UDP	nbname	192.168.1.108	192.168.1.255	1	1-Standard
3413	13May2015	1:23:31		GW	ICMP		Atacante	Victima	1	1-Standard

Ready — Total records in file: 3413

Figura N.-50. Muestra el resultado del registro de tráfico entre el computador atacante y la víctima, se confirma una Comunicación exitosa necesaria para el ataque.

A continuación podemos ejecutar la herramienta, la misma que en sus opciones de configuración nos presenta un menú principal en donde podemos realizar varias pruebas de manera independiente o también una sola corrida de que genere todos los ataques que contiene la herramienta. En nuestro caso realizamos una serie de ataques independientes y finalmente en la página de manera aleatoria opción 0. La siguiente figura muestra una parte de las configuraciones de esta herramienta.

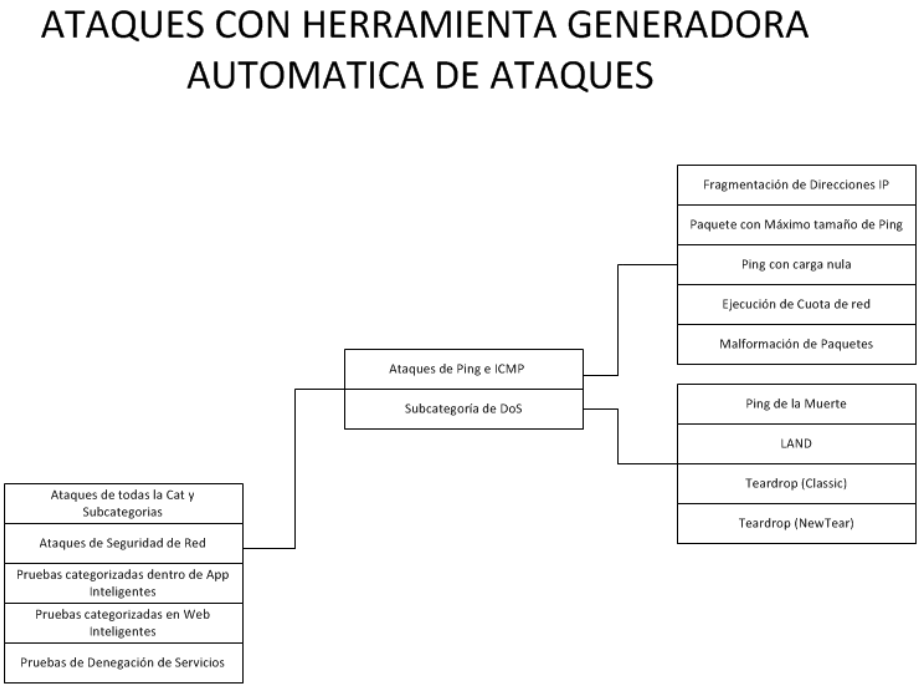


Figura N.-51. Opciones de Configuración de la Herramienta Automática de Ataques.

Pruebas Ejecutadas.

Ataques de Ping e ICMP

- Fragmentación de Direcciones IP.
- Ataque de envío de ping con tamaño máximo.
- Ataque con carga nula de Ping.
- Ataque de cuota de red.
- Ataque de malformación de paquetes

Ataques de Denegación de Servicios.

- Ping de la Muerte.

Fragmentación de Direcciones IP.

El ataque de Fragmentación de paquetes IP intenta agotar recursos de CPU hasta llegar a producir un ataque de denegación de servicio. Un atacante puede enviar el primer fragmento y el último fragmento de un paquete IP, sin necesidad de enviar los fragmentos intermedios o enviar en el intermedio paquetes con contenidos especiales. Ese fragmento de almohadilla en la pila IP se mantiene abierta hasta que el temporizador expira, aprovechando el hecho de que algunos sistemas operativos establecen sus tiempos de espera de para re ensamblaje del fragmento por encima del rango de 2 minutos. Este ataque no requiere una respuesta del sistema de destino, la dirección IP de origen puede ser falsa para ocultar la verdadera ubicación del atacante. El Puerto y destino no son validados, lo que significa que los dispositivos aceptan los paquetes no importa qué puerto se utiliza.

Un equipo de destino bajo ataque podría descartar paquetes legítimamente fragmentados, normalmente experimentan agotamiento de los recursos de la CPU y otros comportamiento inesperados.

Una vez ejecutado el ataque con la herramienta, se ejecutan las tareas necesarias para el ataque y podemos observar los registros en tiempo real que nos presenta la herramienta Smartview Tracker, en donde claramente el módulo de IPS nos informa lo ocurrido como se muestra.

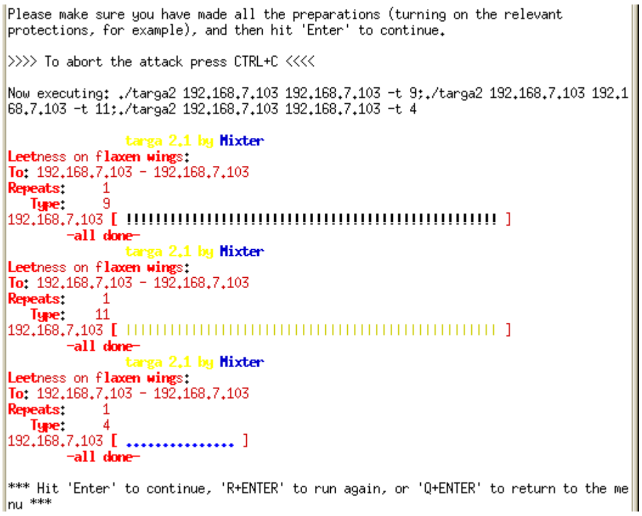


Figura N.- 52. Pantalla en donde se muestra la generación de Ataque de Fragmentación de Direcciones IP por medio de la Herramienta.

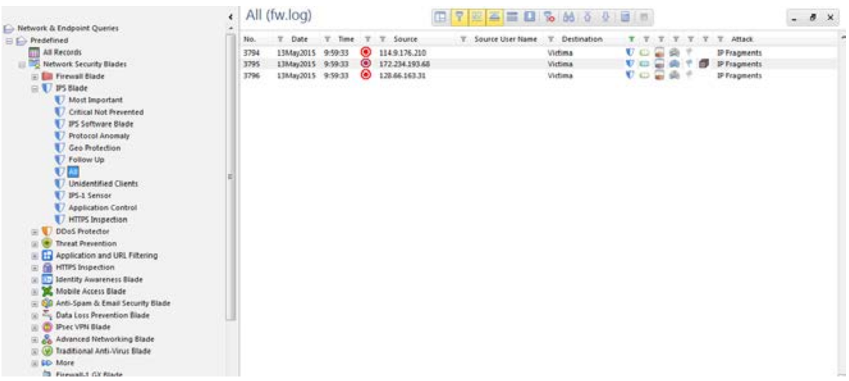


Figura N.-53 Pantalla en donde se muestra la visualización de los registros del módulo IPS.

Al ingresar a cada uno de los registros nos entrega información del tipo de Ataque como se muestra:

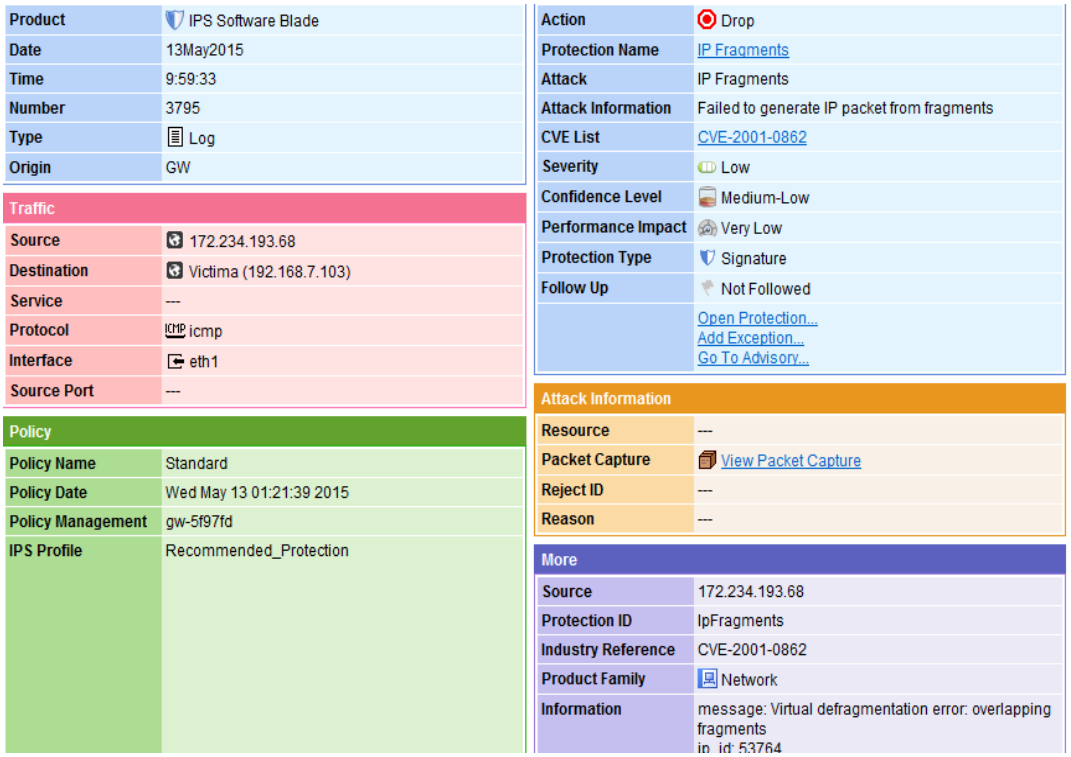


Figura N.-54. Pantalla que muestra la información registrada del tipo de ataque detectado.

Como podemos observar en la pantalla, se tiene información de la fecha y hora del ataque, el modulo que actuó frente al ataque, dirección IP origen, destino, el protocolo utilizado, la interface por donde se generó, característica del IPS que actuó, acción realizada, nombre de la protección (en donde genera un link para mayor información), nombre e información del ataque, numero de listado en el Organismo CVE (Common Vulnerabilities and Expousures) entre otras.

El enlace que hace referencia al nombre de la protección nos entrega información adicional.

Ataque con Ping de máximo tamaño.

Este tipo de ataque pretende bajar al equipo victima haciéndole un ping con alta carga, la cual es configurada con 65000 bytes de datos, este ataque no tiene registro ni tampoco alcanza a ser recibido por el equipo víctima, es desechada por el firewall.

Ataque de carga nula de ping.

Este tipo de ataque pretende volver loco al equipo haciendo un ping con carga nula, la cual es configurada con 1 byte de datos, se muestra la ejecución del ataque.

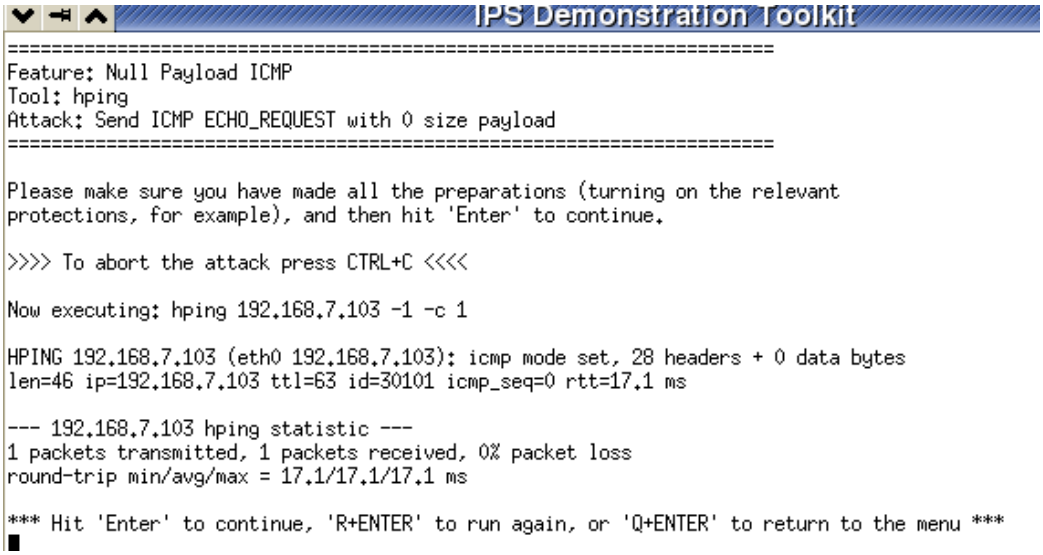


Figura N.-55 Pantalla que muestra la ejecución del ataque de ping con carga nula.

El registro en línea del IPS detecta a este ataque como Fragmento de Ip y no le deja pasar.

Ejecución de Ataque de Cuota de Red.

Este tipo de ataque pretende conseguir recursos del CPU, ya que envía un ping con conteo de 5000 luego le solicita hacer un intervalo de 10 seg e inmediatamente enviar un syn con puerto de destino 80. A continuación la ejecución del ataque, este ataque no tiene registro ni tampoco alcanza a ser recibido por el equipo víctima, es desechada por el firewall.

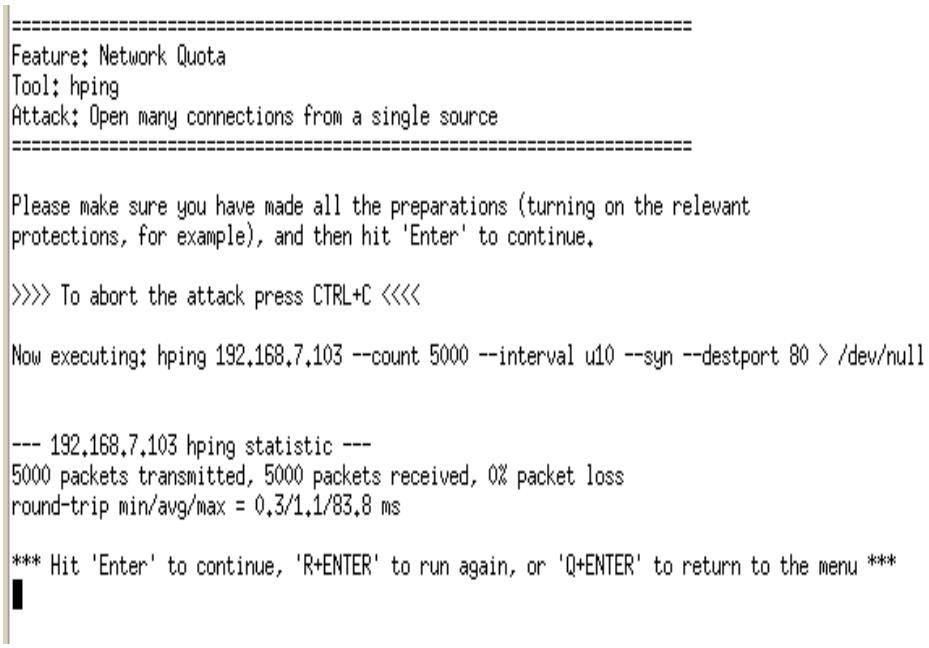
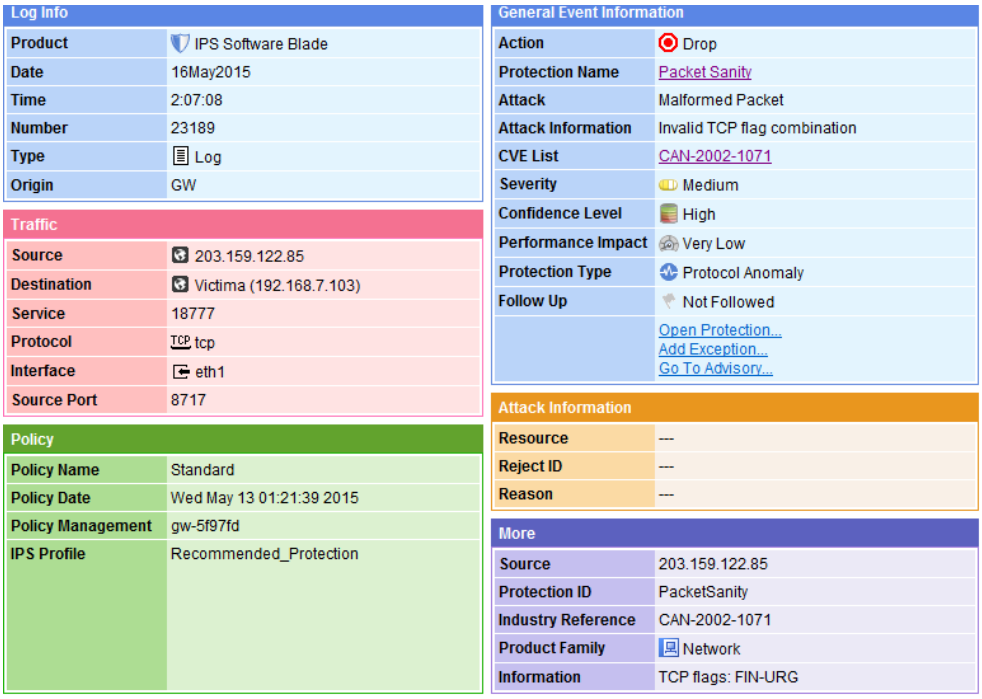


Figura N.-56. Pantalla que muestra la ejecución del ataque de cuota de Red.

Ataque de Malformación de Paquetes.

Esta opción realiza comprobaciones de estado de Capa 3 y Capa 4. Incluye la verificación de tamaño del paquete, UDP y longitudes de cabeceras TCP, opciones de direcciones IP eliminadas y verifica los indicadores TCP.



Log Info	
Product	IPS Software Blade
Date	16May2015
Time	2:07:08
Number	23189
Type	Log
Origin	GW

Traffic	
Source	203.159.122.85
Destination	Victima (192.168.7.103)
Service	18777
Protocol	tcp
Interface	eth1
Source Port	8717

Policy	
Policy Name	Standard
Policy Date	Wed May 13 01:21:39 2015
Policy Management	gw-5f97fd
IPS Profile	Recommended_Protection

General Event Information	
Action	Drop
Protection Name	Packet Sanity
Attack	Malformed Packet
Attack Information	Invalid TCP flag combination
CVE List	CAN-2002-1071
Severity	Medium
Confidence Level	High
Performance Impact	Very Low
Protection Type	Protocol Anomaly
Follow Up	Not Followed
	Open Protection... Add Exception... Go To Advisory...

Attack Information	
Resource	---
Reject ID	---
Reason	---

More	
Source	203.159.122.85
Protection ID	PacketSanity
Industry Reference	CAN-2002-1071
Product Family	Network
Information	TCP flags: FIN-URG

Figura N.-57. Pantalla que muestra la información registrada del tipo de ataque detectado.

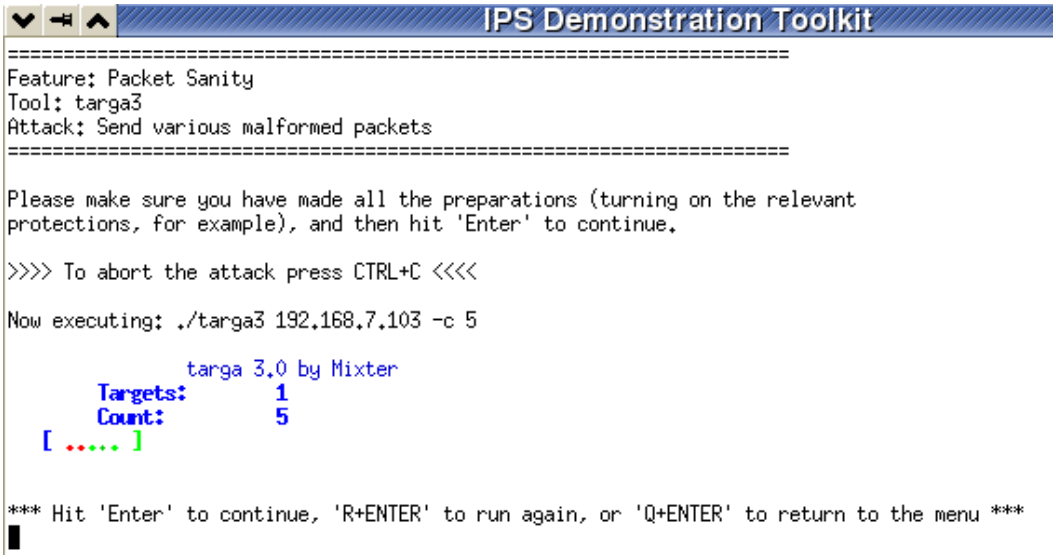


Figura N.-58. Pantalla que muestra la ejecución del Ataque Packet Sanity.

Ataque de Denegación de Servicio

La primera opción de este menú “Denegación de Servicio” nos permite hacer la prueba del ping de la muerte, a continuación de analiza los requerimientos.

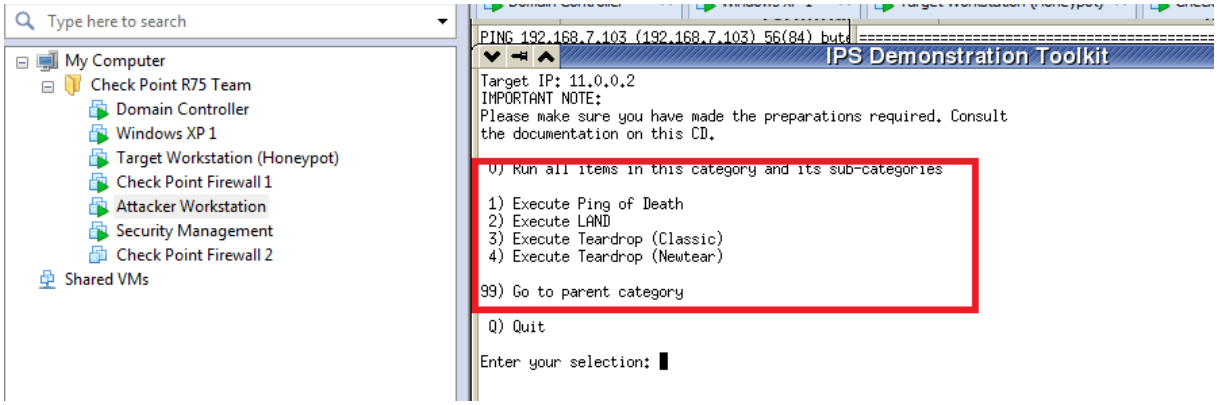


Figura N.-59 Pantalla que muestra las opciones de ataques.

Ping de la Muerte

Al ejecutar la herramienta de visualización de registros nos presenta la pantalla de detección del ataque similar a las pantallas mostradas anteriormente, aquí, el atacante envía una solicitud PING fragmentado en formato incorrecto que busca bloquear el equipo destino, que supera el tamaño máximo de paquete IP (64 KB). Algunos sistemas operativos no son capaces de manejar este tipo de peticiones.

Implementación de Ataques de Forma Aleatoria

Al igual que los ataques que hemos analizado hasta el momento de manera individual los cuales han sido detectados ya sea por el IPS o por el firewall, se presenta a continuación los resultados de ejecutar la opción que permite ejecutar

todos los ataques de forma aleatoria; para que los ataques en la realidad sean detectados, se deberá mantener actualizadas las bases de datos del IPS.

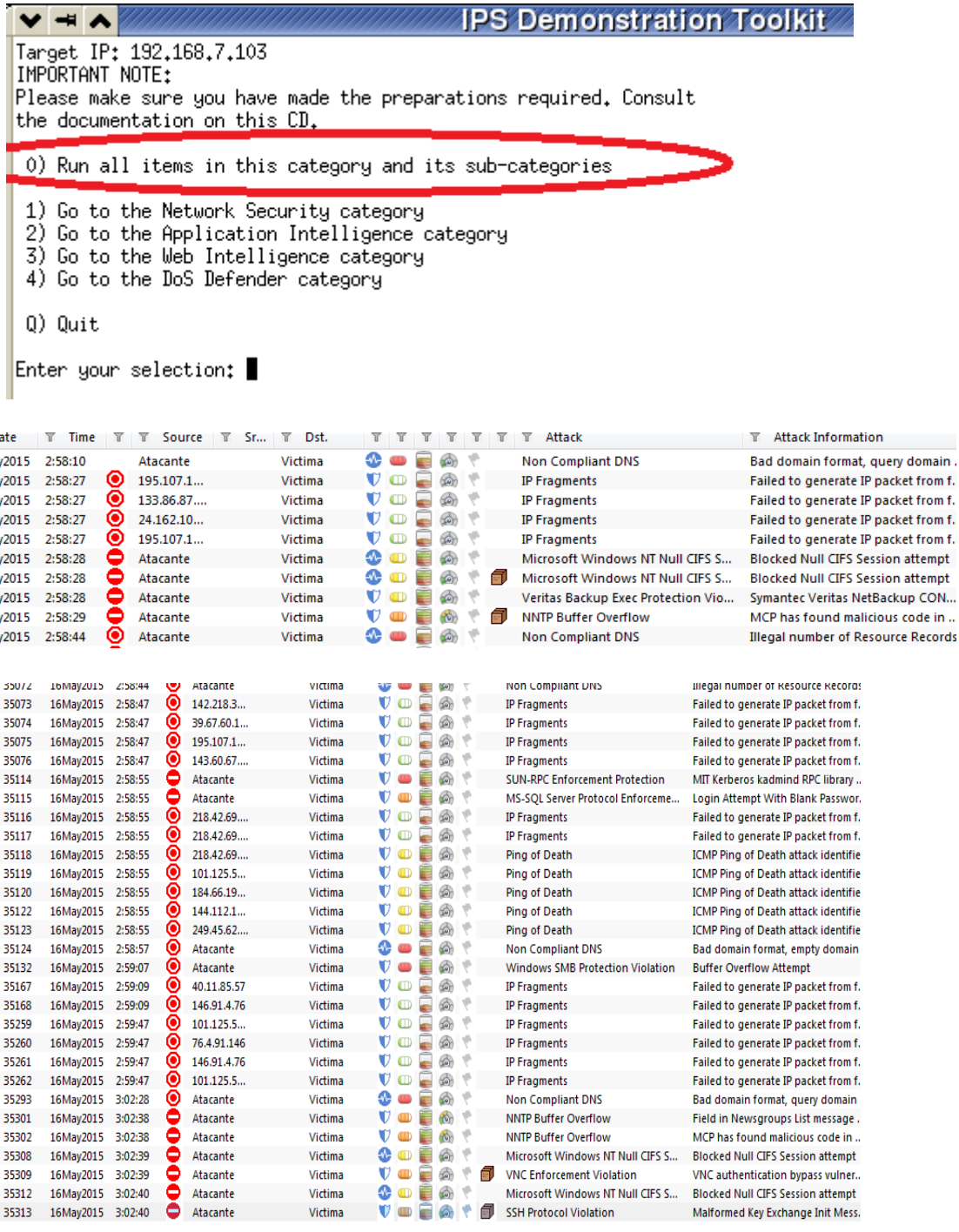


Figura N.-60. Pantallas que muestran los registros de ataques enviados de forma aleatoria.

Resultados de Ejecutar la Herramienta de Generación Automática de Ataques.

Como es de esperarse, la herramienta de comprobación de IPS de Check point que es la utilizada para esta prueba funciona para todas las pruebas realizadas, es decir el IPS realiza su tarea, sin embargo para lograr comprobar esto en el escenario práctico se ha colocado una regla any to any la cual no se dá en la práctica, lo que nos permitiría concluir que si dejaríamos todos los puertos abiertos de un equipo expuestos al internet, bajo las condiciones de la herramienta el IPS actuaría impidiendo el paso de este tipo de ataques.

Resumen de Ataques realizados

La siguiente tabla representa un resumen de todos los ataques realizados hasta el momento.

<table>
<tr><th colspan="7">Implementacion de Ataques a la Infraestructura Propuesta</th></tr>
<tr><th colspan="7">Fase 1. Reconocimiento</th></tr>
<tr><th colspan="2">Puertos Abiertos</th><th colspan="2">Sistema Operativo</th><th>Versión del Servicio</th><th colspan="2">Observaciones</th></tr>
<tr><td colspan="2">Herramientas Web</td><td colspan="2">Herramienta Nmap</td><td>Herramienta Nmap</td><td colspan="2"></td></tr>
<tr><td>http://centralops.net/co/</td><td>http://www.yougetsignal.com/tools/open-ports/</td><td>#nmap -O [Obtetivo]</td><td>nmap –script smb-os-discovery.nse 192.168.1.2</td><td>#nmap -sV [Objetivo]</td><td colspan="2"></td></tr>
<tr><th colspan="6">Fase 2. Escaneo de Puertos y Análisis de Vulnerabilidades</th><td></td></tr>
<tr><th colspan="7">Escaneo de Puertos con NMAP</th></tr>
<tr><th colspan="2">Escaneo de Puertos Abiertos</th><th colspan="2">Escaneo de Puertos a Medio Abrir</th><th>Escaneo Sigiloso</th><th colspan="2"></th></tr>
<tr><td colspan="2">#nmap -sT [objetivo] -p (puertos)</td><td colspan="2">#nmap -sS [objetivo] -p (puertos)</td><td>#nmap -sF [objetivo] -p (puertos)
#nmap -sA [objetivo] -p (puertos)</td><td colspan="2">Unicamente el IPS Detectó el Escaneo Sigiloso</td></tr>
<tr><th colspan="7">Analisis de Vulnerabilidades con Herramientas Dedicadas</th></tr>
<tr><td colspan="2">Herramienta Nessus</td><td colspan="2">Herramienta Nicto</td><td>Herramienta Uniscan</td><td colspan="2">Se determina que todos los paquetes dirigidos hacia el puerto 80 pasan, por tanto las herramientas coniciden en ciertos valores, sin embargo la Opción Nessus hasta el momento es el que mejores</td></tr>
<tr><th colspan="7">Herramienta Metaexploitable2 (EQUIPO CON TODAS LAS VULNERABIIDADES CONOCIDAS</th></tr>
<tr><th colspan="7">Ataque de Denegación de Servicio.</th></tr>
<tr><th colspan="7">Ataque de Hombre en el medio</th></tr>
<tr><th colspan="7">Ataque de Ingeniería Social o Phishing</th></tr>
<tr><th colspan="7">Ataque con Herramienta Generadora de Ataques que se propone.</th></tr>
<tr><td>Ataque 1</td><td>Ataque 2</td><td>Ataque 3</td><td>Ataque 4</td><td>Ataque 5</td><td>Ataque 6</td><td></td></tr>
<tr><td>Fragentacion de Direcciones IP</td><td>Ping de máximo tamaño.</td><td>Ping con carga Nula</td><td>Cuota de Red.</td><td>Maformación de Paqutes</td><td>Ping de la Muerte.</td><td>Estos ataques intentan comprobar el estado del IPS.</td></tr>
</table>

Tabla N.-7. Resumen de Análisis de Vulnerabilidades.

El resultado de cada una de los ataques y medidas para Contrarrestarlos ha sido analizado en cada caso previamente estudiado.

CAPITULO 4

Conclusiones y Recomendaciones

4.1 Conclusiones.

Si bien en el presente trabajo se ha desarrollado un esquema de ataques desde el exterior hasta la red interna y en ciertos ataques basados en escaneo de puertos lo cual frente crecimiento tecnológico en los últimos años ha pasado a ser algo antiguo o mejor dicho menos frecuente en la actualidad y casi controlado en su totalidad con las sofisticadas herramientas de seguridad como la propuesta en el presente trabajo, se plantea como estudio futuro realizar un análisis del comportamiento de los nuevos malwares que surgen en la actualidad los cuales presentan un formato diferente en donde probablemente no ingresan desde el exterior sino internamente y que generalmente no son detectados fácilmente.

Se concluye además que debe tomarse la iniciativa de incluir mecanismos de seguridad desde el origen de cada proyecto y no cuando este se encuentre en ejecución o en etapas finales ya que no se atacaría el origen de los requerimientos de seguridad, para el caso del departamento de desarrollo se debe implementar seguridades desde el diseño del software e implementada durante todo el proceso hasta entrar en producción.

Se concluye en la importancia de realizar un monitoreo constante de uso de recursos, análisis de vulnerabilidades y test de penetración sobre los servidores críticos y actuar inmediatamente sobre ellos ya que de no hacerlo tenemos el riesgo de ser vulnerables (en cualquiera de los tipos estudiados) lo cual puede provocar desde intercepción de Información hasta denegación del servicio, etc.

Actualmente el Organismo que se ha tomado como referencia de estudio, no dispone de políticas claras de Seguridad; esto hace necesario que se tomen medidas para que el personal encargado trabaje en este punto; además se deberá buscar apoyo Directivo para que el cumplimiento de las mismas sea obligatorio puesto que deben estar orientado al beneficio de todos los usuarios.

En el presente trabajo no se ha considerado seguridad de acceso físico, redundancia eléctrica, aire acondicionado, sistemas de replicación de datos, etc, donde se encuentran los equipos informáticos, sin embargo es un punto muy importante que deberá tomarse en cuenta en la elaboración de EGSI y queda planteado para futuros estudios.

El presente trabajo ha permitido ejecutar mediante virtualización Vmware un escenario similar a la realidad, la cual en la realidad tendría un costo elevado, sin embargo debe tomarse en cuenta que no se tiene una similitud del 100% como es un caso real.

Si se realizaran todos los ataques indicados en este documento en el escenario real con los equipos en producción podría llevarlos a la inactividad, como sería por ejemplo el ataque de denegación del servicio Web lo cual sería crítico para la empresa si mencionado servidor no pudiera arrancar enseguida (debido a consecuencias de un ataque), ante esto se ha procedido con equipos similares y se tiene un marco de actividades a seguir que se podrían ejecutar sobre clones de los equipos en producción.

Se ha escogido la herramienta de protección así como para la gestión de los ataques Check Point debido a ser el firewall mejor ranqueado en firmas consultoras

internacionales como Gartner, así como por ser una herramienta de fácil manejo debido a su interfaz gráfica.

Se concluye que los objetivos planteados fueron cubiertos, pues se tiene un documento con escenarios prácticos en donde se indica los ataques realizados y sus resultados, se ha procedido a realizar el test de penetración en base al procedimiento del Ethical Hacking sin embargo puede ser ajustado dentro de una metodología como la OSSTM.

Con el fin de evitar ataques informáticos basados en ingeniería social, cada usuario deberá manejar buenas costumbres de seguridad y acceso y dejar de confiar tanto en redes públicas y correos sospechosos, para esto se deberá generar una campaña de información al respecto, no obstante se tiene que asumir ese riesgo.

No es analizado en el presente documento el hacking de correo electrónico debido a que la infraestructura propuesta para el análisis dispone de un servidor de correo externo que no está presente en la red local.

Actualmente una opción que puede ser un diferencial para evitar ser víctimas de phishing en Instituciones Financieras y eCommerce es adoptar certificados SSL EV que pintan de color verde la barra de direcciones. SSL EV garantiza autenticidad aparte del clásico cifrado en transmisión. Hay que insistir con los usuarios en esa característica.

En base al trabajo realizado se puede aportar con lo siguiente:

- El entorno de un laboratorio como el realizado en el presente trabajo, destaca de manera aislada el comportamiento de la herramienta de seguridad con respecto a los ataques realizados hacia un único servidor, esto ha permitido establecer que aspectos particulares como la precisión en las reglas del firewall así como la habilitación del módulo IPS, el continuo análisis de vulnerabilidad de los servidores y la actualización del sistema operativo de los mismos, son los principales factores a tomar en cuenta en un esquema de Seguridad, que aplicándolos en el escenario real se redujo el consumo del procesador del Servidor en un 50% y la cantidad de vulnerabilidades en un 80%.
- De la experiencia del presente trabajo se destaca que el escenario virtual tiene una gran utilidad para realizar pruebas que nos permita disminuir la cantidad de vulnerabilidades, por medio de la ejecución de exploits y otras herramientas para el efecto.
- No todos los ataques es posible realizarse en el escenario real propuesto debido al riesgo existente de dejar sin servicio web como por ejemplo con el ataque de denegación de servicio; este aspecto ha sido tomado en cuenta en el presente trabajo de tesis, sin embargo los ataques que fueron realizados desde el Internet a la infraestructura real como por ejemplo escaneo de puertos fueron evitados en el escenario real en un 100%.
- Para realizar este tipo de ataques en una infraestructura en producción se deberán considerar varios aspectos que van desde el horario, el cual tendría que ser fuera de horarios de oficina para no entorpecer las labores de los usuarios, así como también la cantidad de veces de

cada ataque hasta que tengamos un único resultado, ya que en la práctica se ha demostrado que no es suficiente realizar una sola vez un ataque si no al segundo y tercer intento se obtienen los resultados estables, al hacerlo dentro de un escenario en producción, se puede entorpecer los sistemas.

- El licenciamiento utilizado en la Herramienta de Seguridad Perimetral propuesta para el análisis en nuestro escenario virtual tiene una duración de 15 días, esto es lo que normalmente se puede conseguir sin costo, por tanto para efectos del presente trabajo se tuvieron que realizar varias instalaciones del sistema operativo GAIA. Este tipo de licenciamiento permite conocer un poco más a detalle la herramienta sin embargo no permite una actualización del módulo IPS, con estas limitantes se ha conseguido realizar el 100% de los ataques propuestos y observar el comportamiento de la solución con estas limitaciones.
- El presente trabajo puede ser replicado con la herramienta de Seguridad de Check Point sin licenciamiento o también solicitando a los diferentes canales una demo que permita una actualización del IPS y trabajar con servidor web víctima equipos con otros sistemas operativos y aplicaciones web, esto permitirá ejecutar ataques, exploits, etc y observar el comportamiento de la solución y sus resultados.
- También se puede replicar el escenario virtual con otra herramienta de seguridad de otros fabricantes, esto puede ser crucial en el momento de tomar una decisión de compra de una herramienta de seguridad.
- La herramienta de Seguridad Propuesta tiene un alto costo por tanto es una limitante para ser aplicado en entornos pequeños sin embargo es

una excelente opción para entornos medianos y grandes; ya que se tienen varios modulos de seguridad adicionales como Correlacionador de Eventos llamado Smart Event, Antivirus, Antispam, etc.

- Es importante ejecutar constantemente análisis de vulnerabilidades de los Servidores Críticos en nuestro caso real trabajamos con la Herramienta Nessus, lo cual nos ha permitido obtener importantes resultados. En la práctica se deben validar varias herramientas de este tipo.
- Los ataques realizados nos ha permitido determinar que efectivamente un malware puede llegar a pasar los filtros de la herramienta de seguridad propuesta y de cualquier otra herramienta, por tanto la labor del Oficial de Seguridad no solo está en gestionar el Equipo de Seguridad Perimetral sino también gestionar la seguridad de los Servidores, actualizando sus sistemas operativos, así como también cambiando y reforzando constantemente las contraseñas de acceso entre otras opciones.
- Muchos ataques son detectados y descartados en el primer filtro (Reglas) si estas están correctamente implementadas.
- El módulo IPS colabora con la seguridad siendo un segundo filtro siempre y cuando también se encuentre habilitado, correctamente configurado y actualizado, sin embargo en la realidad el afinamiento es bastante complejo debido a los falsos positivos que se presentan. Para esto es necesario un constante análisis de los registros de tráfico que nos permitan excluir del IPS ciertos tráficos internos válidos, la herramienta de seguridad propuesta permite al Módulo de IPS trabajar

en modo Default, protegiendo (siempre y cuando se encuentre actualizado) de las amenazas de malware recientemente detectadas y las más comunes.

4.2 Propuestas de Mejora.

Luego de realizar los diferentes tipos de ataques a nuestro escenario virtual, replica del escenario real, podemos realizar las siguientes propuestas de mejora para la Infraestructura real.

- Se debe realizar un estudio de las otras variables que no se han tomado en cuenta en el presente documento relativo a la seguridad, como por ejemplo seguridad física, ambiental, etc.
- Estudiar y evaluar mecanismos de cifrado y control de acceso que permitan reducir ataques por sniffer hacia los servidores, aplicaciones y Bases de Datos.
- Estudiar y evaluar otras herramientas de análisis de vulnerabilidades que sean una alternativa a las que actualmente se las utiliza.
- Programar un cronograma continuo de actualización de Sistemas Operativos tanto Linux por medio del comando yum update y en el caso de Windows, descargar los últimos parches o actualizaciones.
- Instruir a los usuarios que eviten el abrir los mails en cadena.
- Estudiar y evaluar una solución NAC que permita que únicamente los equipos autorizados obtengan acceso a Red.

4.3 Recomendaciones

Se recomienda a corto plazo realizar un cambio en la plataforma web actual, en donde el servidor web Windows no tenga direccionamiento público sino únicamente privado y trabaje detrás del proxy de manera similar a los demás servidores web como se muestra en el siguiente gráfico.

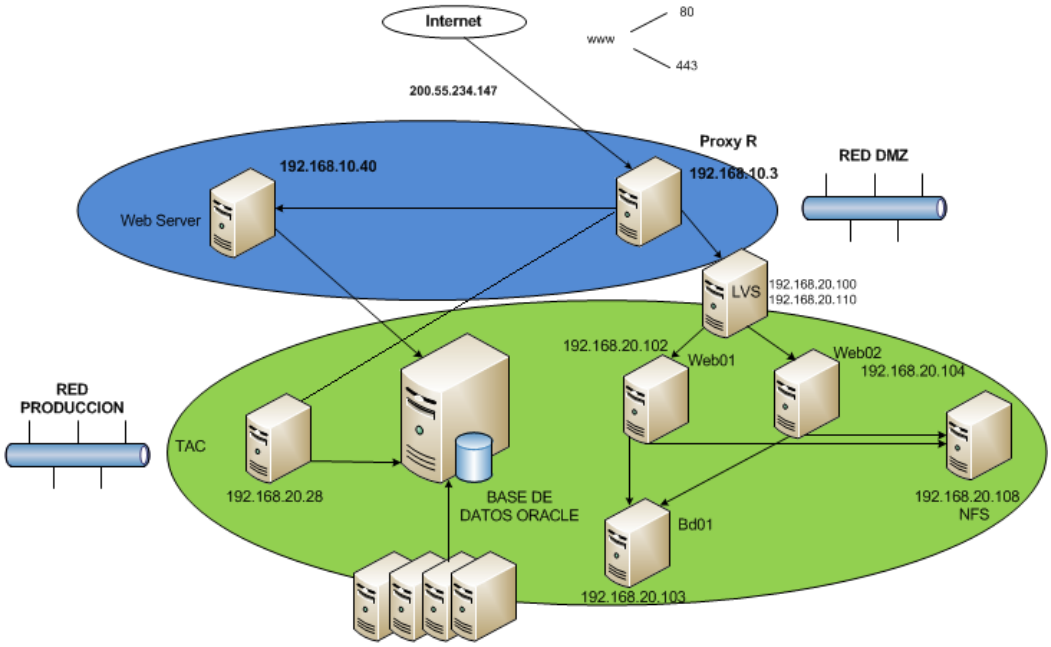


Figura N.-61. Cambios Realizados a nivel de Infraestructura.

Se recomienda a mediano plazo implementar canales cifrados de comunicación entre el proxy reverso y los servidores web así como también entre estos y las bases de datos, ya sean por medio de vpn o cifrados directos a través del sistema operativo (nac).

Se recomienda realizar constantes análisis y verificación de reglas del firewall de manera de evitar que se expongan equipos con más puertos de los necesarios, así como determinar los usuarios, redes y vlans autorizados a que accedan a los servidores.

Se recomienda Actualización periódica de Sistema Operativo y Aplicaciones (parches de seguridad) en todos los servidores.

Dentro del punto anterior, se destaca que en la realidad al realizar una actualización a través del comando yum update se descargan muchos paquetes que en realidad no son necesarios, por tanto deberá verificarse los procesos que conrren antes y después de la actualización.

Se recomienda que el Departamento de Desarrollo aplique las recomendaciones OWASP (Open Web Aplication Security Project Top 10) para el desarrollo web seguro, el cual en su guía de pruebas intenta que el desarrollador entienda que, porque, cuando y como probar sus aplicaciones web. Si bien esta parte es de suma importancia en el aspecto de Seguridad no se lo ha profundizado en el presente documento sin embargo queda planteado para que el lector tome estas consideraciones en su esquema de Seguridad.

Se recomienda además profundizar el tema de control de acceso a Red ya que si bien ha sido tratado brevemente en el presente documento, es una implementación que debe contemplarse en toda organización, debido a su implementación que si bien no es compleja pero consta de varios procesos y no ha sido abordad de manera profunda sin embargo también queda planteado para que el lector profundice y aplique a medida de sus necesidades.

Mantener un escenario similar al de producción a manera de un laboratorio de pruebas (como el desarrollado en el presente documento) para ejecutar análisis de vulnerabilidades, exploits y ataques periódicos que permitan hacer varias pruebas para reducir vulnerabilidades.

Se recomienda mantener actualizado el módulo de IPS y revisión constante del módulo de la herramienta que identifica amenazas en la red mediante correlación de Eventos (Smart Event en el caso de Check Point). Al tratarse de situaciones

críticas como afinamiento del IPS se recomienda realizar pruebas dentro de un escenario de pruebas como el planteado antes de colocar configuraciones en el escenario en producción ya que pueden darse muchos falsos positivos (datos errados que bloqueen accesos legales permitidos)

Se recomienda disponer de respaldos de servidores así como realizar una verificación constante del estado de los mismos de manera de que se garantice la existencia y recuperación ante desastres.

Se recomienda el uso de certificados para las aplicaciones web debido a la información que se maneja, ya que sin este mecanismo de seguridad, la información viaja en texto plano. Es necesario educar a los usuarios finales sobre la importancia de conocer e identificar el origen y la autenticidad de los mismos para no ser víctimas de ataques con certificados digitales falsos.

Se recomienda implementar un EGSI de manera de estar alineados con una estrategia de Seguridad Informática estandarizada y también cumplir con el acuerdo Ministerial 166 tomando como referencia lo realizado en el presente trabajo.

Se recomienda realizar tareas de Aseguramiento del Sistema Operativo que consiste en:

- Deshabilitar carpetas compartidas.
- Usar contraseñas fuertes.
- No usuarios Administrativos.
- Deshabilitar puertos USB mediante GPO.
- Actualización de SO.

- Visualizar archivos ocultos.
- Configuración visualización de extensiones de archivos.

Se recomienda tomar medidas de Seguridad en la Navegación como por ejemplo no descargar barras de herramientas, no abrir banca on line o Redes Sociales desde redes públicas. Tener cuidado con las descargas de tipo P2P, considerar la seguridad en medios removibles.

Se recomienda estar al tanto de los nuevos malwares y actividades en contra de la seguridad, una opción es http://cybermap.kaspersky.com/

Se recomienda considerar las recomendaciones de Seguridad para Entornos virtuales, se tiene guías de Seguridad recomendadas por cada fabricante, en el caso de VMWare se dan recomendaciones de seguridad para su plataforma, por ejemplo cambiar periódicamente el password del equipo vcenter, asignar usuarios para acceso web client, etc. [10]

REFERENCIAS BIBLIOGRAFICAS

[1] V. Pacheco F, "The Need for Formal Education on Information Security" Vol 11, 2013.

[2] M. R. S. W. F. D. D. M. Karla Tandazo Jiménez, «PREVENCIÓN, DETECCIÓN Y REDUCCIÓN DE RIESGOS DE ATAQUES POR ESCANEO DE PUERTOS USANDO TECNOLOGÍAS DE VIRTUALIZACIÓN,» Paper, ESPE.

[3] P. Z. M. S. P. G. Walter Fuertes, «Alternative Engine to Detect and Block Port Scan Attacks using,» *IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.11, November 2011* , vol. 11, nº 11, p. 10, 2011.

[4] R. N. J. Keller, «A Collaborative Virtual Computer Security Lab,» *e-science, In Proc. Second IEEE International Conference on e-Science and Grid Computing,* nº 12, p. 126, 2006.

[5] T. M. P. Li, «Integration of Virtualization Technology into Network Security Laboratory,» *In Proc. 38th ASEE/IEEE Frontiers in Education Conference,* Saratoga, NY, Oct. 2008.

[6] R. H. F. Abbasi, “Experiences with a Generation III virtual Honeynet”, Camberra, ACT Australia: ISBN: 978-1-4244-7323-6, 2009.

[7] D. F. Fermín Galán, «"Use of VNUML in Virtual Honeynets Deployment",» *IX Reunión Española sobre criptología y Seguridad de la Información (RECSI), Barcelona (Spain),* nº ISBN: 84-9788-502-3, p. 15, 2006.

[8] F. F. D. R. E. Damiani, «The open source virtual lab : a case study,» *In proceedings of the workshop on free and open source learning environments and tools, hosted by: FOSLET 2006;,* nº 5-12, p. 7, 2006.

[9] P. Ferrie, «Attacks on Virtual Machine Emulators,,» *Symantec White Paper,,* 2008.

[10] P. Z. L. A. M. M. Walter Fuertes, «Plataforma de Experimentación de Ataques Reales a Redes IP utilizando tecnologías de Virtualización.,» *Dirección de Postgrados de la Universidad Politécnica del Ejercito,* p. 17.

[11] J. Aguilar, , “Estado del Arte de la Cyberseguridad”, IN Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Dic, 2010, en Cuadernos de Estrategia, Instituto Español de Estudios Estrategicos. Instituto Universitario “General Gutierrez Mellado, 2010.

[12] S. I. d. Bancos, «//www.sbs.gob.ec,» [En línea]. Available: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2090.pdf.

[13] C.-O.-I.-P. 2014, «www.desarrolloamazonico.gob.ec,» [En línea]. Available: http://www.desarrolloamazonico.gob.ec/wp-content/uploads/downloads/2014/05/CODIGO-ORGANICO-INTEGRAL-PENAL-act.pdf.

[14] A. Tonenbaum, Redes de Computadoras 5ta Edicion.

[15] ArcCert, «Manual de la Seguridad de las Redes,» [En línea].

[16] E. T. M. C. James Michael Stewart, «Study Guide to Certified Information Systems,» 3rd Edition, San Francisco • London.

[17] J. R. Yáguez, *PROYECTO FIN DE GRADO,* 2014.

[18] C. P. Labs, «http://www.checkpoint.com,» 2015. [En línea]. Available: http://www.checkpoint.com/resources/2014-security-report/.

[19] O. ORG, «owasp.org,» [En línea]. Available: www.owasp.org/images/f/ff/3.OWASP_Day_Costa_Rica_Mario.pdf.

[20] «http://www.dragonjar.org,» [En línea]. Available: http://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml.

[21] «http://isecom.securenetltd.com,» [En línea]. Available: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf.

[22] E. P. D. EJÉRCITO, *ANÁLISIS Y DISEÑO DEL SISTEMA DE SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS (COMACO),* Sangolqui, 2005.

[23] D. Antuna, «diazantuna.es,» [En línea]. Available: http://www.diazantuna.es/certificados-digitales/.

[24] «www.reydes.com,» [En línea]. Available: http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf.

[25] J. Burgos Salazar y P. Campos G, «Modelo Para Seguridad de la Información en TIC. http://ceur-ws.org/Vol-488/paper13.pdf,» de *EIG2008 2do Encuentro de Informática y Gestión*, Temuco, Chile, Noviembre 20-21, 2008., 2008.

[26] H. Tipton y M. Krause, «Information Security Handbook».

[27] «Tesis de Grado. Plataforma de Experimentación de ataques reales a redes IP utilizando tecnologías de Virtualización,» 2012. [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/6057/1/AC-RIC-ESPE-034343.pdf.

[28] ArCert, «Manual de Seguridad de Redes,» [En línea].

[29] «reydes.com,» [En línea]. Available: http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf.