UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

DEPARTAMENTO DE CIENCIAS DE ELÉCTRICA Y ELECTRÓNICA

MAESTRÍA EN REDES DE INFORMACIÓN Y CONECTIVIDAD SEGUNDA PROMOCIÓN

IMPLEMENTAR UNA RED HONEYPOTS PARA DETECCIÓN Y CLASIFICACIÓN DE INTRUSOS MEDIANTE MÁQUINAS VIRTUALES EN EL MINISTERIO DE DEFENSA NACIONAL.

AUTOR: ING. REBECA SOLEDAD TORRES QUEZADA

DIRECTOR: ING. MAURICIO CAMPAÑA

Sangolquí, 21 de enero del 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

MAESTRÍA EN REDES DE INFORMACIÓN Y CONECTIVIDAD

CERTIFICO

Que el trabajo titulado "**IMPLEMENTAR UNA RED HONEYPOTS PARA DETECCIÓN Y CLASIFICACIÓN DE INTRUSOS MEDIANTE MÁQUINAS VIRTUALES EN EL MINISTERIO DE DEFENSA NACIONAL**", realizado por la Ing. Rebeca Soledad Torres Quezada, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la Universidad, en el reglamento de estudiantes de Universidad de las Fuerzas Armadas.

Sangolquí, 21 de enero del 2014

_____

ING. MAURICIO CAMPAÑA
DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

MAESTRÍA EN REDES DE INFORMACION Y CONECTIVIDAD

DECLARACIÓN DE RESPONSABILIDAD

Yo, **TORRES QUEZADA REBECA SOLEDAD**
DECLARO QUE:

El proyecto de grado denominado "**IMPLEMENTAR UNA RED HONEYPOTS PARA DETECCIÓN Y CLASIFICACIÓN DE INTRUSOS MEDIANTE MÁQUINAS VIRTUALES EN EL MINISTERIO DE DEFENSA NACIONAL**", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

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

Sangolquí, 21 de enero del 2014

_____
Ing. Rebeca Soledad Torres Quezada

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

MAESTRÍA EN REDES DE INFORMACION Y CONECTIVIDAD

Yo, **REBECA SOLEDAD TORRES QUEZADA**

Autorizo a la **Universidad de las Fuerzas Armadas-ESPE**, la publicación, en la Biblioteca Virtual de la Institución del trabajo "**IMPLEMENTAR UNA RED HONEYPOTS PARA DETECCIÓN Y CLASIFICACIÓN DE INTRUSOS MEDIANTE MÁQUINAS VIRTUALES EN EL MINISTERIO DE DEFENSA NACIONAL**", cuyo contenido, ideas y criterio son de mi exclusiva responsabilidad y autoría.

Sangolquí, 21 de enero del 2014

_____

Ing. Rebeca Soledad Torres Quezada

AGRADECIMIENTO

Mi agradecimiento a Dios por todas las bondades que ha puesto a mi vida, ya que con su fortaleza espiritual ayudo a que se culmine este proceso en mi etapa profesional.

Mi agradecimiento profundo a mi familia, especialmente a mi madre, que con amor y paciencia me apoyado en este camino de la vida y junto con mis hermanos, han sido mis pilares para seguir adelante.

Un agradecimiento especial al Ing. Mauricio Campaña, por su dedicación y apoyo al presente proyecto de tesis, ya que con sus lineamientos y consejos me ha permitido culminar esta meta en mi vida, y porque además de ser mi tutor es mi amigo.

DEDICATORIA

Esta etapa de mi vida, la dedico a una persona especial, mi padre, que aunque no está físicamente a mi lado, se que desde el cielo estará contento de verme culminar mi carrera profesional, quien con su ejemplo y fuerza influyó en mi vida para ser cada día una persona mejor para la sociedad.

INDICE

INDICE DE GRÁFICOS

INDICE DE CUADROS

RESUMEN DE LA TESIS

IMPLEMENTAR UNA RED HONEYPOTS PARA DETECCIÓN Y CLASIFICACIÓN DE INTRUSOS MEDIANTE MÁQUINAS VIRTUALES EN EL MINISTERIO DE DEFENSA NACIONAL

En la actualidad las redes informáticas se encuentran expuestas a ataques y robos de información generando grandes daños económicos y problemas en el funcionamiento de la red. La presente investigación analiza la implementación de una herramienta de seguridad informática denominada Honeypost, utilizando plataformas de virtualización. Esta herramienta permite realizar el control, captura y análisis de los datos recolectados, lo cual permite establecer las formas de ataque, de dónde se realiza la intrusión y los mecanismos para poder disminuir dichos ataques. Para la ejecución de esta investigación se instaló el honeynet virtual autocontenida de tercera generación, se implementó tres honeypost con diferentes sistemas operativos y servicios, los mismos que presentaban vulnerabilidades para atraer a los intrusos. La máquina fuente se conectó directamente al router de la empresa, con el fin de evitar daños en la red de producción. Además se realizaron pruebas de escaneo, fuerza bruta y denegación de servicio. El Honeynet registró las intrucciones a la red y el comportamiento de los atacantes, lo que ayudó a establecer mecanismos de mejora en la seguridad requerida.

Palabras claves: ataques, vulnerabilidad, redes de información, virtualización, honeypots.

Abstract

Nowadays the computer networks are not only exposed to attacks, but also to information theft which have been generating huge economics damages, and troubles in the network working. This research analyzes the implementation of a security computer tool called "Honeypost", using virtualization platforms. What this tool allows is to monitor, capture and analyze a group of collected data through which permit to establish the different forms of attack, from which is the intrusión performed and the mechanics to reduce such attacks. In order to run this computer research, the third generation of self-contained virtual was installed. Besides, it was implemented three honeypost with different operanting systems and services. these have showed vulnerabilities to attrack intruders. The source machine was directly connected to the router of the company in order to avoid damages in the production network. It was therefore done scanning tests, brute force and rejection of the service. Finally, the Honeynet registered the intrusions to the network and behavior of the attackers what helped to establish the mechanics for improving the required security.

Keywords : attack, vulnerability , information networks , virtualization, honeypots.

CAPÍTULO 1: PROBLEMA DE INVESTIGACIÓN

1.1 Introducción

En este capítulo, se realizará la descripción del perfil de tesis, en el cual se detalla los motivos que impulsaron a realizar esta investigación, los problemas que se presentan en la institución donde se implementará el producto resultado de la tesis (Ministerio de Defensa Nacional), además se establecen los objetivos, el cronograma de trabajo, presupuesto y la hipótesis que permitirá determinar si lo que se está realizando se cumple o no.

1.2 Motivación y contexto

"El fenómeno informático es la expresión de un crecimiento acelerado de la capacidad de procesar información por parte del género humano. Esta capacidad de procesamiento es la que convierte a la información en conocimiento. Es por ello que la Revolución informática es sólo la cobertura tecnológica de un proceso mucho más amplio definitorio: el desplazamiento de la humanidad hacia el concepto de la SOCIEDAD DEL SABER." (Druke, 1994)

Debido a esto la información se convierte en un activo de la institución, la misma que debe ser protegida y debe mantener su integridad, operatividad y privacidad.

La información navega a través de las redes de información, las mismas que tienen diferentes formas de seguridad para que los datos fluyan con confiabilidad a través de ella.

Existen distintas maneras de proteger la información, pero no todas se implementan con un 100% de seguridad, y una de las herramientas que se utilizan para la seguridad informática son los honeypots.

"La tecnología Honeypots ayuda a detectar y rechazar las amenazas dirigidas contra una organización. También ofrece valiosa información sobre los gusanos automatizados, auto-routers, motivación y organización del atacante y más, que se puede aplicar para mejorar la prevención, detección y reacción." (Portal, 2006)

Una máquina virtual puede ser definida de la siguiente manera: "Es un equipo dentro de un equipo, implementado en el software. Una máquina virtual emula un sistema de hardware completo, desde el procesador a la tarjeta de red, en un entorno de software independiente y aislado que permite el funcionamiento simultáneo de sistemas operativos que serían incompatibles de otro modo. Cada sistema operativo se ejecuta en su propia partición de software independiente.", (Center, 2011)

1.3 Planteamiento del Problema

Hoy, son más frecuentes los ataques informáticos a través de la red, es así que en noviembre del 2012 se realizaron ataques a las páginas Web de instituciones públicas del gobierno, lo que demuestra que existe debilidad en la seguridad de dichas instituciones.

Así como existen innumerables formas de ataque, las técnicas de seguridad han aumentado, y una de estas herramientas son los Honeypots como una alternativa a este problema.

El Ministerio de Defensa Nacional cuenta con una seguridad informática mínima, vulnerable a cualquier ataque, su seguridad física cuenta con un antivirus del parque informático, software especializado para filtro de contenido, un firewall que permite la conexión hacia la red externa.

Para mejorar la seguridad del Ministerio, se necesita establecer si existen intrusos que estén atacando a la red, para lo cual se implementará un sistema de detección de intrusos por medio de honeypots.

1.4 Formulación del Problema

Hoy, son más frecuentes los ataques informáticos a través de la red, es así que en noviembre del 2012 se realizaron ataques a las páginas Web de instituciones públicas del gobierno, lo que demuestra que existe debilidad en la seguridad de dichas instituciones.

Así como existen innumerables formas de ataque, las técnicas de seguridad han aumentado, y una de estas herramientas son los Honeypots como una alternativa a este problema.

El Ministerio de Defensa Nacional cuenta con una seguridad informática mínima, vulnerable a cualquier ataque, su seguridad física cuenta con un antivirus del parque informático, software especializado para filtro de contenido, un firewall que permite la conexión hacia la red externa.

Para mejorar la seguridad del Ministerio, se necesita establecer si existen intrusos que estén atacando a la red, para lo cual se implementará un sistema de detección de intrusos a través de honeypots.

1.5 Subproblemas o preguntas de investigación

- ¿El sistema de detección de intrusos, permitirá mejorar la seguridad informática en el Ministerio de Defensa Nacional?
- ¿Existen vulnerabilidades en la red de la Institución?

- ¿Qué software de virtualización es el que presenta mejores condiciones para la implementación de los Honeypots?

1.6 Objetivos

1.6.1 Objetivo General:

Implementar una red de honeypots para detección y clasificación de intrusos mediante máquinas virtuales en el Ministerio de Defensa Nacional.

1.6.2 Objetivos Específicos:

- Análisis de la situación actual de la seguridad informática
- Diseñar modelo de implementación de los Honeypots
- Instalar, conFigurar la estructura de los Honeypots en las máquinas virtuales
- Realizar pruebas de rendimiento de los Honeypots en los servidores
- Realizar pruebas de ataques a la red

1.7 Justificación e Importancia

La seguridad informática en la actualidad es indispensable, ya que existen personas que pueden robar información de las empresas, para que no sucedan estos inconvenientes, existen diferentes sistemas de seguridad, pero no todos proporcionan una seguridad total.

Una de estas formas de seguridad se puede hacer a través de implementación de Honeypots.

Los Honeypots son herramientas que permite atraer y analizar a los atacantes que desean ingresar a la red sin autorización, con la finalidad de ver los movimientos de los atacantes y saber que debilidades tiene la red de una institución.

El Ministerio de Defensa cuenta con una aceptable seguridad, pero requiere de la implementación de un sistema de detección de intrusos que ayude a mejorar su seguridad hacia el exterior e interior de la institución, por ello los Honeypots son una herramienta que permite mejorar su seguridad.

Con los honeypots se puede identificar a los atacantes potenciales de la red del Ministerio, saber cuáles serían sus estrategias de ataque, y atraerlos para que se ocupen atacando las máquinas falsas y lejos de los sistemas de la institución.

Se realizará un análisis de la red para establecer en que parte se ubicará el sistema de Honeypots, para no afectar a la red LAN de la institución.

1.8 Hipótesis

Hipótesis direccional: Con la implementación de un sistema de detección de intrusos no autorizados permitirá mejorar la seguridad del Ministerio.

1.9 Actividades a Realizarse y Cronograma

El desarrollo del proyecto se divide en dos fases:

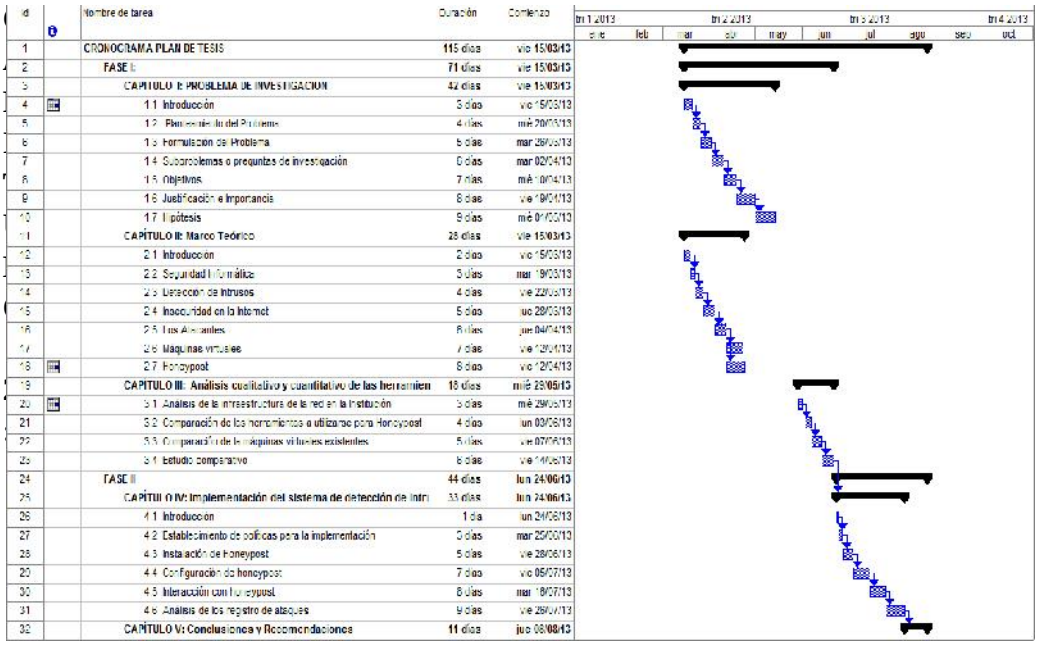
- Fase 1: Análisis de los sistemas de detección de intrusos
  - Abarca los capítulos I, II y III
  - Se refiere a la recopilación de la información sobre Seguridad Informática y sus distintas herramientas
  - Análisis teórico de los Honeypots
  - Estudio comparativo de Honeypots existentes

- Estudio comparativo de máquinas virtuales existentes
- Análisis de la situación actual de la seguridad en la institución

- <u>Fase 2: Aplicación del sistema de identificación de intrusos</u>

  - Abarca los capítulos IV, V
  - Implementación de la aplicación de Honeypots para la detección de intrusos
  - Pruebas de vulnerabilidades de la red
  - Análisis de los resultados obtenidos en base a la implementación del sistema de detección de intrusos
  - Conclusiones y recomendaciones sobre el proyecto realizado.

A continuación se muestra un cronograma de la relación de las dos fases.



Id	Nombre de tarea	Duración	Comienzo
1	CRONOGRAMA PLAN DE TESIS	115 días	vie 15/03/13
2	FASE I	71 días	vie 15/03/13
3	CAPITULO I: PROBLEMA DE INVESTIGACION	42 días	vie 15/03/13
4	1.1 Introducción	3 días	vie 15/03/13
5	1.2 Planteamiento del Problema	4 días	mié 20/03/13
6	1.3 Formulacion de Problema	5 días	mar 26/03/13
7	1.4 Subproblemas o preguntas de investigación	0 días	mar 02/04/13
8	1.5 Objetivos	7 días	mié 03/04/13
9	1.6 Justificación e Importancia	8 días	vie 12/04/13
10	1.7 Hipótesis	9 días	mié 01/05/13
11	CAPITULO II: Marco Teórico	28 días	vie 15/03/13
12	2.1 Introduccion	2 días	vie 15/03/13
13	2.2 Seguridad Informática	5 días	mar 19/03/13
14	2.3 Detección de Intrusos	4 días	vie 22/03/13
15	2.4 Inseguridad en la Internet	5 días	jue 28/03/13
16	2.5 Los Atacantes	6 días	jue 04/04/13
17	2.6 Maquinas virtuales	7 días	vie 12/04/13
18	2.7 Honeypost	8 días	vie 12/04/13
19	CAPITULO III: Análisis cualitativo y cuantitativo de las herramien	18 días	mié 29/05/13
20	3.1 Analisis de la infraestructura de la red en la Institución	5 días	mié 29/05/13
21	3.2 Comparación de los honeynets a utilizarse para Honeypost	4 días	lun 03/06/13
22	3.3 Comparación de las máquinas virtuales existentes	5 días	vie 07/06/13
23	3.4 Estudio comparativo	8 días	vie 14/06/13
24	FASE II	44 días	lun 24/06/13
25	CAPÍTULO IV: Implementación del sistema de detección de intru	33 días	lun 24/06/13
26	4.1 Introduccion	1 día	lun 24/06/13
27	4.2 Establecimiento de políticas para la implementación	3 días	mar 25/06/13
28	4.3 Instalación de Honeypost	5 días	vie 28/06/13
29	4.4 Configuración de honeypost	7 días	vie 05/07/13
30	4.5 Interacción con Honeypost	8 días	mar 16/07/13
31	4.6 Analisis de los registro de ataques	9 días	vie 26/07/13
32	CAPÍTULO V: Conclusiones y Recomendaciones	11 días	jue 08/08/13

1.10 Fuentes de financiamiento de la investigación

La realización del proyecto de tesis conlleva los siguientes costos aproximados:

El financiamiento será por fondos propios del proponente.

Cantidad	Detalle	Valor unitario	Valor total
4	Resmas de papel	4	16,00
3	Empastados	85	255,00
2	Anillados	2	4,00
1	Derechos de grado	400	400,00
1	Tutorías	1400	1.400,00
15	Papeles politécnicos	0,7	10,50
10	Carpetas	0,6	6,00
15	Gastos administrativos	5	75,00
20	Movilización	5	100,00
6	Internet	20	120,00
300	Impresiones	0,08	24,00
2	Cartuchos de impresora	40	80,00
2	Material de apoyo (libros)	30	60,00
TOTAL			**2.550,50**

CAPíTULO 2: MARCO TEÓRICO

2.1 Introducción

En el presente capítulo se detallan los conceptos que permiten un mejor entendimiento de lo que es la seguridad informática, el sistema de detección de intrusos, el uso de las máquinas virtuales y su funcionamiento.

También se analizará los tipos de ataques que se pueden presentar y daños que generan, se definirá que es un Honeypots, sus características e implementación para un mejor funcionamiento del mismo.

2.2 Seguridad Informática

La seguridad es un término amplio que abarca múltiples usos, y dentro de ellos está la seguridad informática, que permite asegurarse que los recursos del sistema tengan protección hacia riesgos.

En la actualidad la información viene a ser un activo de una organización, la misma que requiere de protección y con la aparición de nuevas tecnologías (Internet, red de datos WAN, LAN), la seguridad de la información también fue evolucionando, por lo que se detalla una pequeña reseña histórica de la seguridad informática.

La historia de la información empieza en lo físico, al inicio se realizaba a través de dibujos, escritos en piedra y posteriormente en papel, y cuando aparece el papel las empresas o personas que requieren guardar y cuidar la información, esto se lo realizaba en archivadores, y su protección a través de guardias, alarmas y bajo llave (seguridad física).

Para conseguir que exista seguridad de comunicación de mensajes, anteriormente se realizaba a través de cartas, telegramas o personas, las mismas que podían ser interceptadas y llegar el mensaje al enemigo, un ejemplo se encuentra en el cifrado para ocultar la información que inventó el emperador César. (Eric, 2005)

Muchos otros países también utilizaron antiguamente este tipo de sistema de seguridad en la comunicación de la información, como Alemania en la segunda guerra mundial y la encriptación fue interceptada por la resistencia, esta máquina se llamó enigma.

En el campo militar se utilizan codificaciones para comunicarse, sin que se pueda descifrar la información que se envía hacia otros lugares, es así que para evitar este tipo de problemas de intercepción de información, los Estados Unidos crearon un programa llamado TEMPEST, cuyo objetivo era reducir las emisiones que podría utilizarse para capturar información.

Desde que llegaron los computadores la información de las organizaciones se volvió electrónico, magnético, que se envía a través de la red, con el pasar del tiempo las computadoras fueron más fáciles de usar, los datos se guardaron en sistemas, y muchas personas pudieron acceder a la misma, luego llegó el internet, y la información recorrió a través de él, ante lo cual se vio la necesidad de mejorar la seguridad informática.

Ante este avance tecnológico en la seguridad y riesgos en la información se estudiará a los Honeypots los mismos que pueden ayudar a mejorar la seguridad informática, se revisará algunos conceptos que permitirán orientar la implementación de esta herramienta de seguridad.

2.2.1 Concepto Seguridad Informática

Como se describió anteriormente la seguridad informática surgió en la necesidad de proteger la información tanto física como comunicacional de una institución u organización, ya que existen personas o riesgos que pueden afectar la integridad de la misma.

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización y que la comunicación que se realice de la información sea también segura sin que se pueda interceptar los datos o mensajes. (Rios, 2013)

"Se puede entender como seguridad un estado de cualquier tipo de información (informática o no) o la que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo." (Gallo, y otros, 2012)

El concepto describe una seguridad a todo nivel del área informática, redes, servidores, información, bases de datos, etc., pero esta investigación será direccionada hacia la protección de los datos e información, para evitar el ingreso de intrusos a la red y el robo de la misma.

2.2.2 Retos u objetivos que se obtienen con la seguridad informática

Para tener una adecuada seguridad en la información, la protección de la misma debe entregar confiabilidad, disponibilidad, integridad, confidencialidad y no repudio en la información.

Confiabilidad:

La información será accedida por el personal autorizado, es decir protección de los datos, por esto la seguridad informática debe buscar las herramientas que protejan de invasiones y accesos por parte de personas o programas no autorizados.

Disponibilidad:

Es la necesidad de que un servicio no se detenga y esté disponible cuando el usuario lo requiera y donde sea.

Integridad:

Asegurar que los datos no sufran cambios, que la información llegue integra, completa hacia su destinatario.

Confidencialidad

Asegurar que solo las personas autorizadas puedan ingresar a la información, y que se garantice el secreto de las personas que envían y receptan los mensajes.

No repudio

Establece que el receptor y emisor del mensaje no pueden negar que se transmitió el mensaje. (Introducción Seguridades de la Información, 2009)

2.3 División de Seguridad Informática

Existen dos tipos de seguridad informática:

2.3.1 Seguridad Física

Se refiere a los mecanismos de protección de los desastres naturales que se presentan y pueden afectar a los equipos; a la detección y prevención de posibles incendios, bajos de energía, daños de baterías y averías de los equipos.

Dentro de esta categoría también está la restricción de acceso físico, ya que personas y empleados ajenos a las instalaciones del data center u otras pueden ingresar a los equipos y podrían bajar algún servicio importante para la empresa o robar información importante.

2.3.2 Seguridad Lógica

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y que sólo las personas autorizadas puedan acceder a ellos. (Borghello, 05)

2.4 Medidas para una seguridad informática

Como se indica anteriormente la seguridad informática permite proteger la información, por lo que existen medidas que van a ayudar a que el objetivo de la seguridad se realice y estas se pueden clasificar en:

- Prevención o defensa
- Salvaguardia
- Detección
- Recuperación
- Aprendizaje
- Denuncia

Prevención o defensa:

Evita o impide que se produzca un ataque o daño en nuestra red, establecer normas o políticas que protejan a la información.

Salvaguardia

Mecanismos que permiten reducir riesgos, pueden ser procedimientos, dispositivos, físicos o lógicos que se utilizan para contrarrestar las acciones de perjuicio que se pueden presentar en la organización.

Detección

Consiste en establecer mecanismos que permitan detectar acciones que pueden afectar a la red de información, mientras más rápido sea la detección se podrá tomar las medidas para proteger los datos.

Recuperación

Son procedimientos para recuperar la información o infraestructura en el caso que se produzca un desastre tanto físico como lógico.

Denuncia

Son los procesos para identificar a los causantes y realizar las denuncias a las autoridades competentes. (Torres, y otros, 2012)

2.5 Detección de Intrusos

La seguridad lógica es la protección de la información de una organización almacenada en bases de datos y a la cual solamente pueden acceder las personas autorizadas.

El estudio en la tesis es hacia la protección de datos, y una de las herramientas de seguridad a utilizar es la detección de intrusos, para lo cual se desarrollará algunos conceptos y características de funcionamiento de estos programas.

2.5.1 Concepto de un IDS

Programa que permite detectar accesos no autorizados a la red de una organización para realizar daños en el sistema o robo de información.

Existen hackers o personas que ingresan a la organización a través de la red para modificar o robar información, sin que el administrador de la red pueda detectarlos, y los IDS son sistemas que permitirán informar el momento qué personas ajenas a la institución intentan ingresar.

2.5.2 Características de sistemas de detección de intrusos

- Debe funcionar continuamente en ejecución sin supervisión humana.
- Debe recuperarse automáticamente ante una caída del sistema.
- Debe monitorizarse a sí mismo para asegurarse de que no ha sido modificado.
- Debe utilizar mínimos recursos de la red. Un sistema que relentiza la máquina, simplemente no será utilizado.
- Debe ser conFigurado de acuerdo a las normas de seguridad de la empresa.
- Debe observar desviaciones sobre el comportamiento estándar.
- Debe ser fácilmente adaptable al sistema ya instalado y a los cambios que se pueden presentar.
- Debe ser difícil de "engañar".

2.5.3 Clasificación de los IDS

Se clasifican de acuerdo a:

- Localización o función
- Modelo de detección
- Naturaleza

2.5.3.1 Localización o función

NIDS (Network Intrusion Detection System)

Analiza el tráfico de toda la red completa, examinando paquetes individualmente en búsqueda de opciones no permitidas, o armados maliciosamente y para no ser detectados por el cortafuegos. Al encontrar paquetes maliciosos produce alertas cuando estos intentan explorar algún fallo en un programa de servidor.

HIDS (Host Intrusion Detection System)

Analiza el tráfico en un servidor o PC, busca que está sucediendo en el host y puede detectar intentos fallidos de acceso o modificaciones de archivos críticos.

2.5.3.2 Modelo de detección

Detección de mal uso

Este tipo de detección del mal uso permite saber que sucesos ilegales dentro del tráfico de la red, secuencias ilegales para realizar ataques contra la red.
Ejemplo: los sniffers, exploit, escaneo de puertos.

Detección del uso anómalo

Se refiere al análisis estadístico del tráfico de la red, analizar el comportamiento de los usuarios en la red en determinado tiempo de trabajo, es así que si se presenta tráfico en la red en noche o madrugada esto es una situación anormal dentro de la red.

2.5.3.3 Según su naturaleza

Pasivos

Detectan violaciones a la red e informan del ataque pero no toman medidas que puedan cambiar este ataque.

Activos

A diferencia de los pasivos estos toman medidas que cambian el curso del ataque.

2.5.3.4 Distribuidos y centralizados

Distribuidos

Son los sistemas en donde se van a implementar varios IDS que se comunican entre sí con un servidor central que permite correlacionar todos los datos generados por ellos.

Centralizados

Son los IDS que emplean sensores que transmiten información a un sistema central desde donde se controla todo el proceso de identificación de intrusos.

2.6 Estructura de los Sistemas de Detección de Intrusos (IDS- Intrusion Detection System) (Garcia, 1986)

Al igual que la seguridad y la tecnología han evolucionado con el tiempo, los IDS también evolucionaron, a continuación se presenta la estructura que conforma un IDS.

Se pueden identificar cuatro componentes básicos:

- Generador de eventos (E-boxes)
- Motor de análisis (A-boxes)
- Unidades de almacenaje (D-boxes)
- Unidades de respuesta (R-boxes)

Generadores de eventos (E-boxes)

Los generadores de eventos, sensores o sondas, tienen como objetivo la obtención de datos del exterior del sistema de detección de intrusos, son los “ojos” del IDS. Las entradas de los generadores de eventos serán los datos en bruto del entorno exterior al IDS. A su salida presentar a esos datos procesados en forma de eventos

comprensibles por el resto de los componentes. Los generadores pueden ser diversos, dependiendo del tipo de datos que recogen, aunque su funcionamiento a nivel conceptual suele ser muy similar. Reciben los datos de entrada, los preprocesan para pasarlos a un formato común al resto de los componentes y proporcionan los eventos al resto de componentes prácticamente en tiempo real.

Motor de análisis (A-boxes)

El motor de análisis es el núcleo de los IDS, es el motor de inferencia que, gracias a unos conocimientos, será capaz de discernir la relevancia de los eventos recibidos de las E-boxes y generar nuevos eventos como salidas. Estos motores de análisis pueden ser de muchos tipos, sistemas estadísticos de profiling, reconocedores de patrones, sistemas de correlación de eventos, etc.

Unidades de almacenaje (D-boxes)

Este componente es el encargado de almacenar físicamente las inferencias del motor de análisis. Contendrá todos los eventos generados por las ´ A-boxes y normalmente se organizan en forma de bases de datos. Es por tanto un componente esencial a la hora de aplicar técnicas de datamining y correlación de datos como fuentes de información forense.

Unidades de respuesta (R-boxes)

Las unidades de respuesta son los componentes encargados de realizar acciones en nombre de otros componentes del sistema. Este componente suele emplearse para desplegar unidades que ejecuten contramedidas ante una intrusión. Es decir, permiten al sistema reaccionar de forma activa ante las acciones procesadas por otros componentes.

Estas acciones pueden ser muy variadas, aunque en la gran mayoría de los casos están orientadas a prevenir ataques de fuentes maliciosas previamente detectadas o a cortar un ataque en curso. Cuando el sistema cumple lo anterior se dice que además de ser un sistema de detección de intrusos (lo cual implica pasividad), se le concede la denominación de sistema de prevención de intrusos o IPS. En general, un IPS suele auto contener la noción de IDS, no obstante algunos puristas prefieren denominar a dichos sistemas como I(D\P)S.

2.7 Inseguridad en la Internet

Internet ha crecido desde su aparecimiento, siendo una red mundial, todos se conectan y comunican a través de ella, y las aplicaciones actualmente están orientadas hacia el Internet. Es una herramienta que permite la comunicación a distancia, muy útil para la educación, medicina, compras electrónicas, negocios electrónicos y banca electrónica.

Los usuarios frecuentes se conectan a diario y están conectados todo el día. Los dispositivos móviles son uno de los disparadores del crecimiento en los accesos y los usuarios ingresan a través en forma móvil. Las redes sociales crecen sostenidamente e Internet crece como canal de comunicación y de entretenimiento.

Pero debido a que muchas personas pueden navegar y conectarse a través de él, se han realizado fraudes informáticos como el robo de información, robos de cuentas bancarias, etc.

Se han creado protocolos de comunicación que permite proteger la navegación en el internet, estos son:

- SSH (Secure Shell): Usado exclusivamente en reemplazo de telnet
- SSL (Secure Sockets Layer): Usado principalmente en comunicaciones de hipertexto pero con posibilidad de uso en otros protocolos
- TSL (Transport Layer Security): Evolución del protocolo SSL

- HTTPS (Hypertext Transfer Protocol Secure): Usado exclusivamente para comunicaciones de hipertexto

Adicional al tipo de protocolo que se use, se debe tener en cuenta algunas consideraciones para la navegación por medio del internet.

- Realizar copias de seguridad.
- No guardar nada confidencial en directorios compartidos de programas.
- Instalar un antivirus.
- Apagar el ordenador siempre que no se esté utilizando.
- Extremar el cuidado en sistemas con IP fijas (ADSL).
- Instalar el software de firewall personal, preferentemente con sistema de detección de intrusos. (Para usuarios expertos)
- No instalar software de fuentes no conocidas.

2.8 Los Atacantes

Para poder combatir a la inseguridad y establecer políticas de seguridad en una institución u organización es necesario establecer que son los ataques, su clasificación y forma de realizar el ataque.

2.8.1 Concepto de ataque

Es la ejecución deliberada y organizada en el que una o varias personas desean hacer daño a la red o sistema informático, comprometiendo a la seguridad de información que posee una persona u organización.

Históricamente el primer ataque informático que se presentó fue en el año 1989, cuando una empresa regalo un Cd que contenía un virus que afecto a empresas e instituciones.

Actualmente los ataques se realizan vía internet, aunque también se puede realizar a través de telefonía, redes, wifi y en las redes de área local.

2.8.2 Tipos de ataques

Existen varios tipos de ataques que pueden afectar a nuestra red, a la información, etc., estos tipos de ataques se dividen en dos grandes grupos:

Ataque pasivo: El intruso monitorea la red para capturar contraseñas o información pero no realiza ninguna modificación contenida en los sistemas.

Ataque activo: El intruso interfiere en el proceso de la comunicación de la red, y realiza modificaciones en la información contenida en el sistema.

A continuación se menciona algunos ataques que se ejecutan para dañar la información de la institución.

De negación de servicio

Estos ataques niegan el uso de recursos a los usuarios o quitan de operación algún servicio. Un ejemplo: un computador puede procesar gran cantidad de información, impidiendo que el usuario pueda utilizarlo.

Dentro de este tipo de ataques tenemos a los de denegación de servicios distribuidos, que son aquellos un conjunto de sistemas previamente configurados que

realizan un ataque distribuido sincronizado a un objetivo, con lo cual afectan el ancho de banda y satura procesos de gran importancia para la empresa.

De refutación

Es un ataque que entrega información falsa en una transacción o evento ocurrido.

Sniffers

Programa que rastrea paquetes de información que recorren en la red para monitorear la actividad de un ordenador. Su objetivo principal obtener cualquier tipo de información como claves, cuentas, ip, etc.

Spoofing (engaño)

Programas que tratan de dar información falsa sobre la identidad del atacante con el fin de mantener su anonimato, un ejemplo puede ser los ip soofing, que enmascaran la IP para llegar a su objetivo.

Spyware

Recopila información de un ordenador en el cual se graban las actividades realizadas por el usuario y transmite a otro lugar la información obtenida. Entre los programas como spyware están los cokies, adware y monitores de sistema.

Exploits

Es un programa que explora alguna vulnerabilidad del sistema, y causa daños en los equipos, igualmente puede violar medidas de seguridad para acceder sin autorización y permitir el ataque de terceros.

Caballos de troya

Son Programas que permanecen ocultos en el computador y posteriormente atacan realizando fuertes daños, a diferencia de los gusanos estos no pueden propagarse solos, estos vienen juntos a correos electrónicos, mensajes.

Virus, Gusanos

Son programas que fueron diseñados con el fin de realizar daños en los equipos informáticos, los virus alteran el servicio del computador sin el permiso o el conocimiento del usuario.

Los gusanos son programas que se propagan automáticamente en el computador sin la intervención del humano.

Ingeniería Social

Este tipo de ataque no va hacia el sistema, sino contra una persona para obtener cierta información reservada, y con la información recabada se puede iniciar un ataque.

Vishing

Este tipo de ataque se realiza a través de la voip y la ingeniería social para estafar a las personas.

Ataques a aplicaciones

Son ataques que afecta a las aplicaciones Web que aparentemente están protegidas, pero existen vulnerabilidades a través de las cuales los atacantes pueden ingresar a la red. Se menciona a continuación algunos ataques a aplicaciones.

Fuerza Bruta

Un ataque de fuerza bruta es un proceso automatizado de prueba y error utilizado para adivinar un nombre de usuario, contraseña, número de tarjeta de crédito o clave criptográfica.

SQL Inyection

La inyección de código SQL es una técnica de ataque usada para explotar sitios Web que construyen sentencias SQL a partir de entradas facilitadas por el usuario. (Consortium, 2004)

Cross-site Scripting

Cross-site Scripting (XSS) es una técnica de ataque que fuerza a un sitio Web a repetir código ejecutable facilitado por el atacante, y que se cargará en el navegador del usuario.

Inyección LDAP

La inyección LDAP es una técnica de ataque usada para explotar sitios Web que construyen sentencias LDAP a partir de datos de entrada suministrados por el usuario.

En el Ecuador, según un estudio de GMS y Kaspersky, los delitos informáticos en el Ecuador se incrementaron en 360%, entre 2009 y 2010, dejando una pérdida aproximada de un millón de dólares a los usuarios de la banca electrónica.

Cualquier persona que sea usuario de sistemas de mensajería instantánea, redes sociales o ingrese a su banco de manera electrónica, puede ser víctima de los llamados

phishing, spyware y backdoors, encargados de realizar operaciones informáticas que permitan obtener las claves virtuales. (Almeida, 2011)

En el país, el 61% de ataques cibernéticos se localizan en Pichincha y las provincias que reflejan menor grado de violaciones de seguridad informática son el Guayas y el Azuay, con el 20% y 7%, respectivamente.

En noviembre del 2012 se realizaron ataques por parte de la organización anymus a páginas del gobierno central y de municipalidades, como se puede ver estas organizaciones no estuvieron preparadas para este ataque, ya que muchas veces la gente piensa que nunca van a ser atacados y que la institución donde laboran está bien protegida de robo de información.

Entre las páginas que fueron afectadas son:
http://www.chone.gob.ec
http://www.ame.gov.ec
http://www.municipiobanos.gob.ec
http://www.rocafuerte.gob.ec
http://www.quininde.gob.ec
http://www.24demayo.gob.ec
http://www.gobiernodezapotillo.gob.ec
http://www.latacunga.gob.ec
http://www.sanvicente.gob.ec
http://quitohonesto.gob.ec
http://www.manta.gob.ec
http://www.canar.gob.ec
http://www.ibarra.gob.ec/cultura
http://goberguayas.gob.ec (Comercio, 2012)

Se han mencionado algunos ataques que se ejecutan para obtener información privada de organizaciones o personas, ante estos tipos de ataques se debe establecer los mecanismos de seguridad para contrarrestarlos y una de las herramientas que ayudan a mejorar la seguridad son los Honeypots, la misma que será analizada e implementada en el Ministerio de Defensa para detectar este tipo de ataques, que un firewall o un bloqueador de contenidos no puede identificarlos con facilidad.

2.9 Máquinas virtuales

Antes de conocer que son máquinas virtuales es necesario definir que es virtualización.

2.9.1 Virtualización

Definición: La virtualización es un proceso que permite ejecutar varios sistemas operativos independientes dentro de un mismo computador.

En la virtualización se comparten la unidad de procesamiento central (CPU, Central Processing Unit), memoria, dispositivos de entrada y salida, etc., en un entorno virtual se pueden ejecutar programas como los de ofimática en un sistema operativo que pueden instalarse en Windows XP, muy independiente y sin interrumpir el trabajo de otros programas que se ejecutan en un sistema operativo diferente como el Linux, en resumen se pueden ejecutar sistemas operativos como el Windows XP, Linux, Sun o el que se desea en un solo computador, y estos funcionarán independientemente compartiendo el hardware sin problema, como se describe en la Figura No. 1.

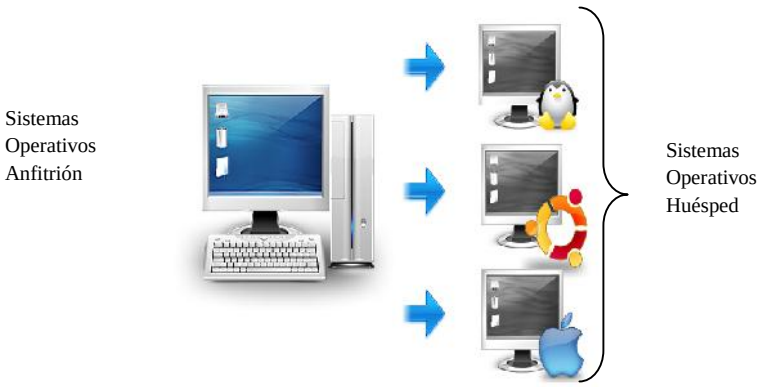


Figura 1: Virtualización

Pero como, surgió la virtualización, este término virtual vino funcionando desde hace tiempo, no es un término que recientemente apareció, es así que se usa en los años setenta con la finalidad de dividir o mejorar la utilización de los mainframes, que se encontraban subutilizados.

2.9.2 Historia de la virtualización

La virtualización hoy en día está en auge, pero realmente se comenzó hablar de virtualización en el año 1960, la empresa IBM (International Business Machines) fue la que empezó a particionar mainframe o supercomputadoras a fin de mejorar su utilización (particiones lógicas), ya existía subutilización de los equipos, en el año 1970 IMB desarrollo varios sistemas de soporte de virtualización: IBM system/360, IBM VM/370.

En el año 80 aparecieron las microcomputadoras lo que ocasionó que el tema de virtualización desaparezca, debido a que las microcomputadoras eran más económicas y las personas empezaron a utilizarlas y las supercomputadoras desaparecieron, a finales de los 90 se vuelve a retomar la virtualización, ya que aparece el mismo problema que en los años 60, es decir un alto nivel en hardware y su subutilización en hardware, espacio, energía y dinero, por lo que se necesitaba virtualizar o particionar estos equipos para mejorar su utilización.

Hoy en día la virtualización ha ayudado a muchas empresas a mejorar su situación informática, donde se puede implementar varios sistemas operativos en un solo equipo, modificando sus instalaciones tecnológicas y consolidando sus recursos de hardware, software y disminución de costos. Existen algunas empresas que se han

dedicado a realizar software de virtualización, por lo que posteriormente se hablará de cuáles son estas y cual conviene en la implementación del proyecto. (WMware.com)

2.9.3 Máquina virtual

Es un software que crea una máquina diferente a la máquina original, esta máquina virtual puede utilizar un sistema operativo diferente al del original, las máquinas virtuales se comportan igual que la original, contienen su propio disco duro, RAM (Random Access Memory - Memoria de Acceso Aleatorio), tarjetas de interfaz de red, CPU todos estos basados en software y no de hardware.

Se pueden implementar varias máquinas virtuales en un computador de acuerdo a las necesidades.

2.9.4 Hypervisor o virtual machine monitor (VMM)

Hypervisor es el software que permite la virtualización, se le conoce también con el nombre de Virtual Machine Manager (VMM), este software realiza la abstracción de los recursos físicos de la máquina original para las máquinas virtuales que se ejecuten, además permite el nivel de aislamiento de las máquinas virtuales y proporciona la interfaz gráfica para el hardware.

2.9.4.1 Tipos de hypervisores

Tipo 1.- Se conoce con el nombre de nativo, unhosted o bare metal (sobre el metal desnudo), este software se ejecuta directamente sobre el hardware, para ofrecer una mejor funcionalidad. Su estructura se detalla en la Figura 2.

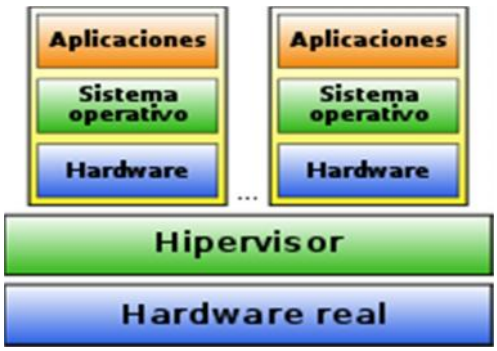


Figura 2 : Hypervisor tipo 1

Tipo 2.- En este caso el hypervisor se ejecuta sobre el sistema operativo, este se carga antes que el sistema operativo, y las máquinas virtuales se cargan sobre el hypervisor. Se le llama también hypervisor hosted. La Figura 4 presenta la ilustración del hypervisor.

Figura 3 : Hypervisor tipo 2

Tipo 3.- Se le denomina hypervisor híbrido ya que tanto el sistema operativo como el hypervisor interactúan directamente con el hardware físico. Las máquinas virtuales se ejecutan sobre el hypervisor es decir en un tercer nivel, pero también pueden

interactuar con el sistema operativo. A este tipo de hypervisor algunos autores lo encasillan como de tipo2. (Datakeeper, 2011), la estructura del hypervisor se detalla en la fígura 4.

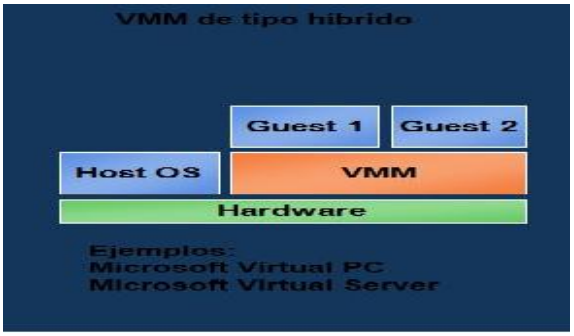


Figura 4: Hypervisor tipo 3

2.9.5 Tipos de virtualización

Las soluciones de virtualización se dividen en software de plataforma y de recursos.

2.9.5.1 Virtualización de recursos:

Es la que permite la simulación y combinación de múltiples recursos, como volúmenes de almacenamiento, recursos de red.

A cotinuación mencionados algunos ejemplos:

- VPN (virtual prívate network),
- Discos RAID,
- VLAN (Red de área local virtual),
- Virtualización de almacenamiento,
- Clusters, grid computing,

2.9.5.2 Virtualización de plataforma:

Este tipo de virtualización permite la creación de una máquina virtual con todos sus componentes utilizando el hardware y software, es decir sus procesadores, componentes e interconexiones de la plataforma. (Villar, y otros)

Este tipo de virtualización se realiza utilizando un software de virtualización, que permite la creación de un software invitado en un software original.

De esta manera esta virtualización permite que varias máquinas virtuales con distintos tipos de sistemas operativos, funcionen independientemente una de la otra, compartiendo la misma máquina física.

En la virtualización de plataforma se menciona los siguientes:

Emulación o simulación

Consiste en imitar o suplantar una máquina virtual en un hardware completo, (procesador, memoria, conjunto de instrucciones, comunicaciones…), la emulación puede hacer creer al programa que se está ejecutando en una plataforma diferente a la que fueron escritos.
Ejemplos: BOCHS, PearPC, QEMU, MAME (emulador de hardware de máquinas recreativas)

Completa

Simula un hardware en el que se puede ejecutar un sistema operativo huésped sin ser modificado, es decir ejecutar el sistema operativo huésped sobre el mismo CPU de la máquina original, lo que permite un alto rendimiento de la máquina virtual.

Ejemplos: Parelles wokstation, VirtualBox VMware Workstation, VMware Server, Microsoft virtual server, Xenserver, OracleVM, Etc.

Paravirtualización

Utiliza el hypervisor de tipo 1, como capa de virtualización y así compartir y administrar el acceso al hardware y a diferencia de la virtualización completa, permite la modificación del sistema operativo y comunicación directa con el sistema operativo anfitrión a través del hypervisor, lo que no ocurre en la completa, el virtualizador más conocido es el XEN Server. (Pillateum)

A nivel de sistema operativo

El sistema operativo anfitrión virtualiza el hardware a nivel de SO, es decir a nivel del Kernel del anfitrión, no existe un hypervisor, en este caso el uso de dispositivos se realizan a nivel del kernel que permite que esto sea más rápido.
Ejemplos: FreeBSD jails, Solaris containers, OpenVZ

2.9.6 Plataformas de virtualización

Existen varias plataformas que se utilizan para realizar virtualización, y a continuación se mencionarán las más relevantes

2.9.6.1 Virtual Pc:

Desarrollado por Connectix y comprado por Microsoft para crear ordenadores virtuales. Su función es emular un hardware sobre el que funcionen varios sistemas operativos.

Con esto se puede conseguir ejecutar varios sistemas operativos en la misma máquina a la vez y hacer que se comuniquen entre ellos.

Windows Virtual PC admite los siguientes sistemas operativos host y cliente:

- Host: Windows 7 Home Basic, Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate y Windows 7 Enterprise.
- Cliente: Windows XP Service Pack 3 (SP3) Professional, Windows Vista Enterprise Service Pack 1 (SP1), Windows Vista Ultimate Service Pack 1 (SP1), Windows Vista Business Service Pack 1 (SP1), Windows 7 Professional, Windows 7 Ultimate y Windows 7 Enterprise.

2.9.6.2 VMware Inc.:

Es un sistema de virtualización por software, filial de EMC Corporation que proporciona la mayor parte del software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player. El software de VMware puede funcionar en Windows, Linux, y en la plataforma Mac OS X que corre en procesadores INTEL, bajo el nombre de VMware Fusion. (Emprendedores, 2011).

VMWARE WORKSTATION, la interfaz gráfica es bastante clara, y no se tiene muchos problemas a la hora de encontrar funciones críticas.

VMware Workstation tiene las capacidades de copiar, pegar, arrastrar y soltar ficheros entre anfitrión y huéspedes. No importa que sistema operativo se use, VMware Workstation es también permite el soporte para USB 2.0.

VMware Workstation es una, sin duda, potente utilidad que permite varios sistemas operativos instalados sin necesidad de particiones, consiguiendo además que cambiar de uno a otro sea sencillísimo, casi tanto como cargar un programa más.

Otra de sus ventajas es que una vez instalados los sistemas operativos adicionales a través de VMware se podrá utilizarlos de forma individual y trasladarlos a otros PC tranquilamente.

El programa anfitrión sólo puede ser ejecutado bajo Windows NT, 2000, XP o Vista (también existe versión para Linux) pero una vez instalado existen las posibilidades de instalar nuevos sistemas operativos se ejecuten.

Otra de las ventajas es que las instalaciones de sistemas operativos “adicionales” son independientes, de forma que se pueden trasladar a otro equipo que también posea VMware y ahí tendrás ése sistema operativo entero y listo para funcionar. (Workstation)

2.9.6.3 KVM (Kernel-based Virtual Machine)

Está formada por un módulo del núcleo (con el nombre kvm.ko) y herramientas en el espacio de usuario, siendo en su totalidad software libre. El componente KVM para el núcleo está incluido en Linux desde la versión 2.6.20.

Permite ejecutar máquinas virtuales utilizando imágenes de disco que contienen sistemas operativos sin modificar. Cada máquina virtual tiene su propio hardware virtualizado: una tarjeta de red, discos duros, tarjeta gráfica, etc.

2.9.6.4 VirtualBox:

Software de virtualización para arquitecturas x86 de 32 y 64 bits, que fue desarrollado originalmente por la empresa alemana Innotek GmbH, pero que fue adquirida por la empresa Sun Microsystems en febrero de 2008 y actualmente desarrollado por Oracle Corporation.

Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como “sistemas invitados”, dentro de otro sistema operativo “anfitrión”.

Posee una interfaz gráfica llamada virtual box manager, que permite crear máquinas virtuales, definiendo sus características virtuales de memoria, disco, teclado, mouse, cdrom y la red. Permite el manejo de la máquina en forma remota.

2.10 Honeypots

Como se dijo anteriormente, Honeypots es una herramienta de seguridad de la información, que nos permitirá básicamente conocer los intrusos que ingresan a nuestra red y poder establecer que tipo de ataque están realizando en nuestra red y vulnerabilidades de la misma y así poder mejorar nuestra seguridad.

2.10.1 Concepto

Es una herramienta de seguridad informática, cuyo objetivo es almacenar información falsa en servidores de datos y ubicados estratégicamente en la red, con la

finalidad de atraer atacantes o hackers y registrar sus pasos o movimientos de manera detallada en la red.

2.10.2 Funciones principales de los Honeypots

- Desviar la atención del atacante de la red real del sistema, de manera que no se comprometan los recursos principales de información.
- Formar perfiles de atacantes y sus métodos de ataque preferidos, de manera similar a la usada por una corporación policiaca para construir el archivo de un criminal basado en su modus operandi.
- Conocer nuevas vulnerabilidades y riesgos de los distintos sistemas operativos, entornos y programas las cuales aún no se encuentren debidamente documentadas.
- Capturar nuevos virus o gusanos para su posterior estudio (Hernández, y otros).

2.10.3 Clasificación de los Honeypots

Se clasifican de acuerdo al ambiente de producción y de la interacción

De acuerdo al ambiente de producción

Para producción: son aquellos que se utilizan para proteger la información en ambientes reales, se instalan en las empresas con servicios vulnerables, puertos abiertos, datos falsos para desviar la atención de máquinas mucho mas importantes, trabajan las 24 horas del día.

Para investigación: Este tipo de Honeypots no se instala para proteger redes, sino que es puramente educativo o de investigación, no contiene datos importantes y su objetivo principal es estudiar patrones de ataque y amenazas.

De acuerdo a la interacción: permite definir el rango de posibilidades de ataque que puede permitir un honeypots al atacante.

Interacción baja:

Estos Honeypots emulan servicios y sistemas operativos, se destacan por su simplicidad, ya que son fáciles de utilizar, pero su desventaja es que la recopilación de la información es poca y limitada. Se utiliza para realizar pruebas de escaneo y analizar tráfico malicioso. Ejemplo emulación de FTP, specter, honyed y KFsensor. Este tipo de honeypots se describe en la Figura 5.

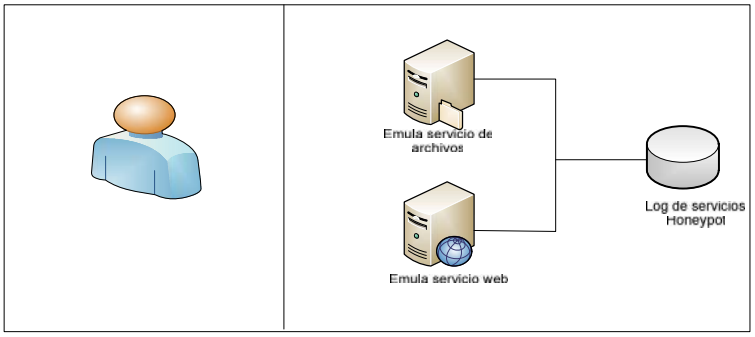


Figura 5: Honeypots Interacción baja

Interacción alta:

A diferencia de la interacción baja esta es mucho más compleja en su implementación, ya que permite una interacción real con el atacante, no se emulan servicios, sino que se ejecutan servicios, aplicaciones y sistemas operativos reales, dentro de máquinas reales o virtuales, la ventaja de este Honeypots es que permite almacenar grandes cantidades de información para analizar y ver las vulnerabilidades de la red, pero también es riesgosa ya que el atacante puede darse cuenta que es un Honeypots y a través de este atacar a la red real que no forma parte del Honeypots, para

lo cual se requiere de una tecnología adicional que prevenga al atacante dañar la red real. Se detalla su funcionamiento en la Figura 6.

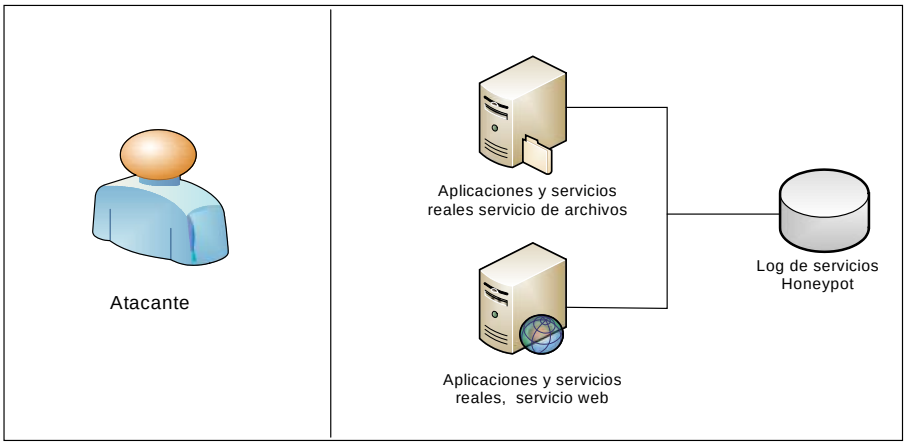


Figura 6: Honeypots Interacción alta

2.10.4 Ventajas y Desventajas

Ventajas

- Captura de información, recopilación de datos de manera detallada a diferencia de otros programas de análisis de seguridad, siendo esto una información muy valiosa.
- Recursos mínimos, significa que se puede utilizar recursos mínimos de hardware e implementar una plataforma lo suficiente potente para operar a gran escala, se puede utilizar hardware reciclado.
- Simplicidad, debido a su arquitectura son conceptualmente simples, y fáciles de implementarlos.
- Flexibilidad de uso, el trabajo para el que fue instalado el Honeypots es flexible, ya que no está atado a resolver un problema específico.
- Retorno de inversión: a diferencia de otras herramientas de seguridad como los firewalls los Honeypots permiten un retorno de inversión, precisamente cuando

funcionan bien, es muy sencillo demostrar que muchas instituciones o personas están expuestas constantemente a ataques y es necesario dedicar recursos a la seguridad.

- Protocolo IPv6, es un sistema que a diferencia de otros permite trabajar en protocolos versión IPv6, detectara ataques igualmente que si estuviera trabajando sobre IPv4.

Desventajas

Vistas limitadas: solo permite extraer información sobre lo que interactúa con ellos, lo que está a su alcance, no se puede tener información de sistemas vecinos.

Riesgo: Este es la mayor desventaja, debido a que como los Honeypots atraen a los atacantes y se interactúa directamente con ellos, los atacantes pueden usar los recursos del Honeypots para comprometer los sistemas reales.

Huella digital o perspectiva limitada: si el atacante perciben al honeypots antes de ingresar a ella, y no se realizan ataques, el Honeypots no sirve para nada y por tanto se anula su funcionalidad y efectividad; y, pueden atacar a otra parte de la red.

2.11 Metodología para realizar las pruebas de vulnerabilidades y su evaluación

La metodología que se utilizará para realizar las pruebas de vulnerabilidades es "The Open Web Aplication Security Project - OWASP", esta metodología es libre y permite la aplicación de sus técnicas para medir las vulnerabilidades de aplicaciones Web.

En la Guía para Construir Aplicaciones y Servicios Web Seguros (2010), menciona que OWASP "es un nuevo tipo de entidad en el mercado de la seguridad. Nuestra libertad de las presiones comerciales nos permite brindar información imparcial, práctica, y rentable sobre seguridad de aplicaciones..." (FOUNDATION)

OWASP presenta dos tipos de proyectos de documentación y de desarrollo, dentro de la segunda están algunas técnicas y metodologías para realizar protección en las aplicaciones Web, y dentro de los documentales se tiene la Guía de Testeo -guía centrada en pruebas de la seguridad de aplicaciones Web.

Metodología de pruebas OWASP

Las pruebas de intrusión nunca serán una ciencia exacta mediante la cual se pueda definir una lista completa de todas las incidencias posibles que deberían ser comprobadas. De hecho, las pruebas de intrusión son solo una técnica apropiada para comprobar la seguridad de aplicaciones Web bajo ciertas circunstancias.

El modelo de pruebas consta de:

- Auditor: La persona que realiza las actividades de comprobación
- Herramientas y metodología: El núcleo de este proyecto de guía de pruebas
- Aplicación: La caja negra sobre la cual realizar las pruebas

Las pruebas se dividen en 2 fases:

Modo pasivo: la persona a cargo de la realización de las pruebas intenta comprender la lógica de la aplicación, juega con la aplicación; puede usarse una utilidad

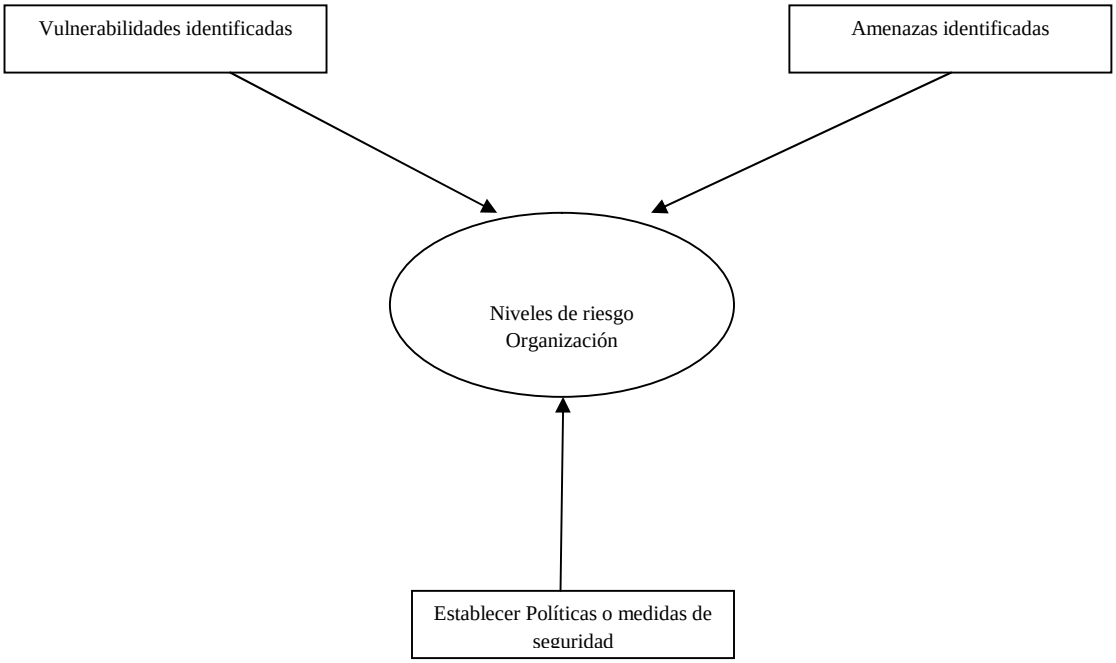
para la recopilación de información, como un proxy HTTP, para observar todas las peticiones y respuestas HTTP. Al final de esta fase se debería comprender cuales son todos los puntos de acceso (puertas) de la aplicación.

Modo activo: en esta fase la persona a cargo de la comprobación empieza a realizar las pruebas. (OWASP, 2008)

Se ha dividido en un conjunto de 9 subcategorías:

- Pruebas de gestión de la conFiguración
- Pruebas de la lógica de negocio
- Pruebas de Autenticación
- Pruebas de Autorización
- Pruebas de gestión de sesiones
- Pruebas de validación de datos
- Pruebas de denegación de Servicio
- Pruebas de Servicios Web
- Pruebas de AJAX

Después de realizar las pruebas se debe evaluar e identificar las vulnerabilidades de los sistemas, verificar los puntos de acceso de los sistemas, y tomar las medidas necesarias para poder contrarrestar estos riesgos, como se muestra en la Figura 7.



gura 7: Componentes de evaluación de riegos organizacional

CAPÍTULO 3: ANÁLISIS DE LA ESTRUCTURA DE RED DEL MINISTERIO Y HONEYNET A IMPLEMENTAR

3.1 Introducción

En este capítulo se realizará un estudio de la situación actual de la infraestructura del Ministerio, como se encuentra estructurada, si tiene implementada seguridades en su red, se realizará comparación entre las distintas formas de realizar virtualización, que software de virtualización es el que conviene utilizar en la institución e igualmente un análisis de que herramienta Honeypots se empleará para realizar la detección de intrusos.

3.2 Análisis de la infraestructura de la red de la Institución

La red de datos del Ministerio se encuentra estructurado a través de VLAN que se dividen por áreas de trabajo y separado por DMZ para un mejor control del manejo de la red de datos.

El Firewall Perimetral de hardware dedicado, filtra el acceso a puertos de los servidores que permite publicar las redes públicas, maneja nateo de estos servicios, divide en zonas de seguridad a nuestros servidores controlando así los accesos a los mismos, y es un concentrador VPN, al momento no utilizado debido a que no se cuenta con sucursales remotas.

Equipo de filtro de intrusos y ataques de capa 7, filtra ataques a los aplicativos de los servidores, bases de datos, usuarios internos, previniendo así ataques de malware, denegación de servicios, barrido de puertos, inyecciones sql, etc.

Switch controlador de Access Points, permite concentrar la administración de todos los Access Points en una sola consola, adicionalmente levanta túneles encriptados con los mismos a fin de mantener la confidencialidad e integridad en este tipo de redes, maneja políticas de acceso centralizadas junto con el switch de autenticación ACS.

Consola de Antivirus Symantec: Consola de Administración de los clientes de antivirus, maneja reportes de incidentes de virus, maneja un repositorio de actualizaciones que son repartidas localmente a los clientes, envía políticas a nivel de firewall nativo en cada máquina y de desinfección en caso de virus, malware, etc. Como seguridad de ingreso de usuario a los computadores se utiliza el active directory

A continuación se detalla en la Figura No. 8 la distribución de la red:

1. Cisco/router 2901: router balanceador de carga que mediante rotue-maps y las balancea el tráfico saliente a internet.
2. Cisco/firewall ASA 5520: Firewall perimetral de hardware dedicado, filtra el acceso a puertos de los servidores que publicamos a redes públicas, maneja nateo de estos servicios, divide en zonas de seguridad a nuestros servidores controlando así los accesos a los mismos.
3. Cisco/IPS SSM-40 tarjeta adicional en Cisco ASA: equipo filtro de intrusos y ataques de capa 7.
4. Checkpoint/Gateway de seguridad GAIA R75.60: equipo que filtra las conexiones salientes a internet por parte de los usuarios del Ministerio.
5. Checkpoint/Gateway de administración GAIA R75.60: ConFigura las políticas en el Gateway de administración GAIA R75.60.
6. Cisco/Switch Core 4506E: Comutador de gran escala que interconecta todos los switches de acceso a la red.
7. Cisco/ACS 5.2 Servidor AAA: Servidor AAA de autenticación tanto por red cableada como por red inalámbrica.

8. Cisco/WLC 5508 switch controlador inalámbrico: Switch controlador de Access points.
9. Cisco switch: Switch de acceso a los usuarios de los diferentes departamentos del Ministerio.
10. Consola de antivirus Symantec: Consola de administración de los clientes de antivirus.

.

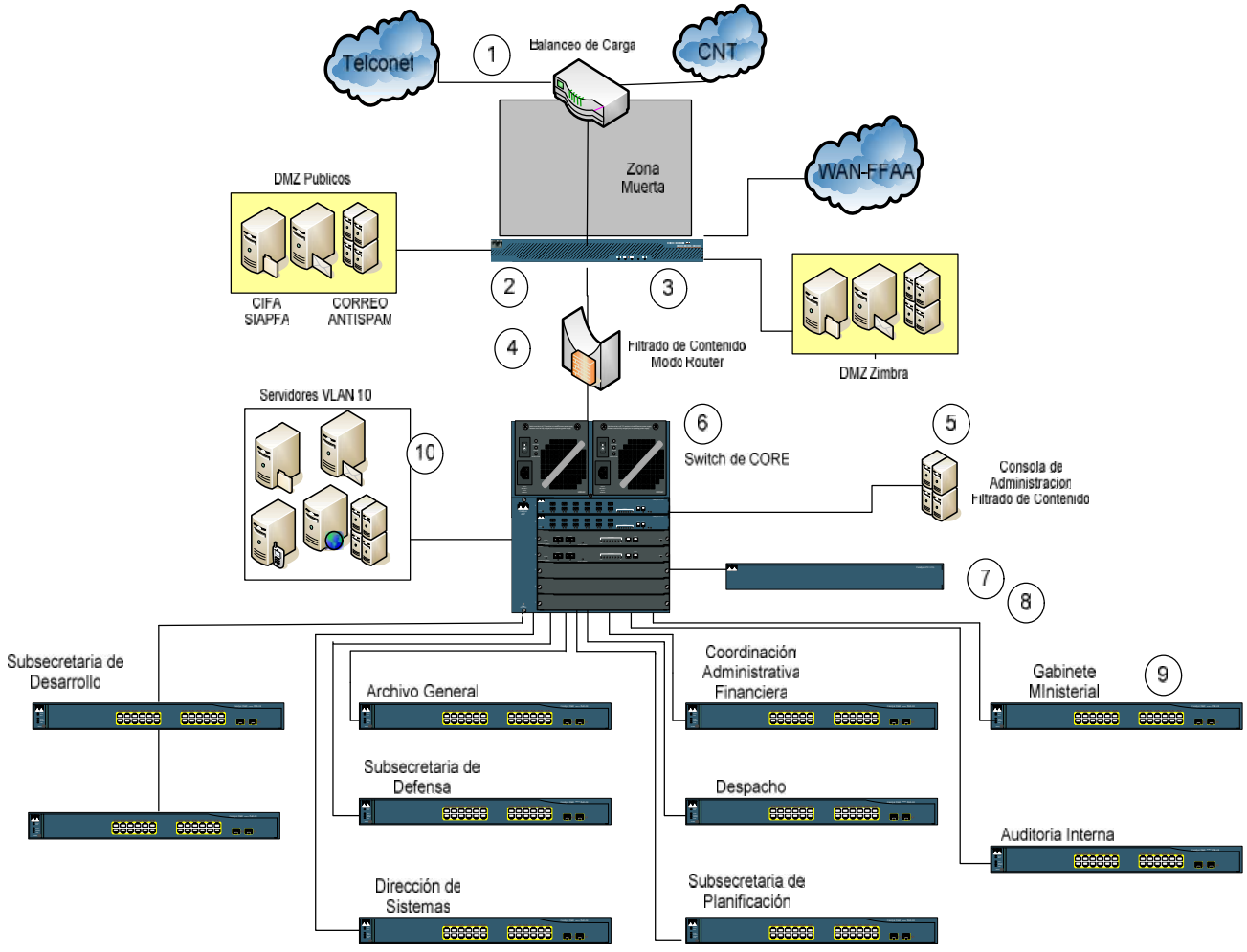


Figura 8: Estructura de la red

3.3 Comparación de las herramientas a utilizarse para Honeypots

Como se estableció en el marco teórico los Honeypots permiten realizar detección de intrusos en la red.

En Honeypots existen dos tipos de producción e investigación, por lo que en este estudio se utilizará para producción ya que se requiere proteger la información en ambientes reales, igualmente se utilizará Honeypots de interacción alta para poder analizar la información de ataques o vulnerabilidades que existe en la red.

Como una herramienta para la implementación de un Honeypots de alta interactividad es honeynets.

3.3.1 Honeynets: Son un tipo de Honeypots, que actúa sobre una red entera, en este caso se usan equipos, sistemas operativos reales y por ende aplicaciones reales.

Se utiliza para comprobar los ataques, su forma en que atacan y las nuevas técnicas de ataque a la red.

Normalmente está compuesto por un solo sistema en el que emula otros sistemas, emula servicios conocidos o vulnerabilidades, o crea entornos cerrados.

Con los honeynets se atendería dos aspectos importantes:

El Control de datos: define el grado de vulnerabilidad de los sistemas expuestos y sea apetecible al atacante.

Captura de datos: Permite establecer que herramientas y métodos se utilizan para el monitoreo de las actividades realizadas en el honeynet, donde se almacenarán las actividades de la red y establecer los perfiles de los atacantes. (Vinueza, 2012)

3.4 Arquitecturas de los honeynets

3.4.1 Primera Generación: Este tipo de honeynets se destaca por la sencillez de su estructura, está formada por:

- Un firewall o cortafuegos: responsable del control de datos,
- Un router: Para el encaminamiento de la información.
- Un servidor centralizado de logs: permite el almacenaje de los datos
- El IDS: para la detección de los intrusos
- Conjunto de máquinas para señuelos

La tarea de control de intruso se realiza entre el router y el cortafuegos, el cortafuegos mantiene una traza de cuantas conexiones se realizan desde un honeypots saliendo al internet, en el momento que este número de conexiones aumente, este se cerrará, impidiendo cualquier intento más. Para establecer el umbral depende de lo que se quiere analizar dentro del honeynet. La estructura de Honeynet de primera generación se detalla en la Figura 9.

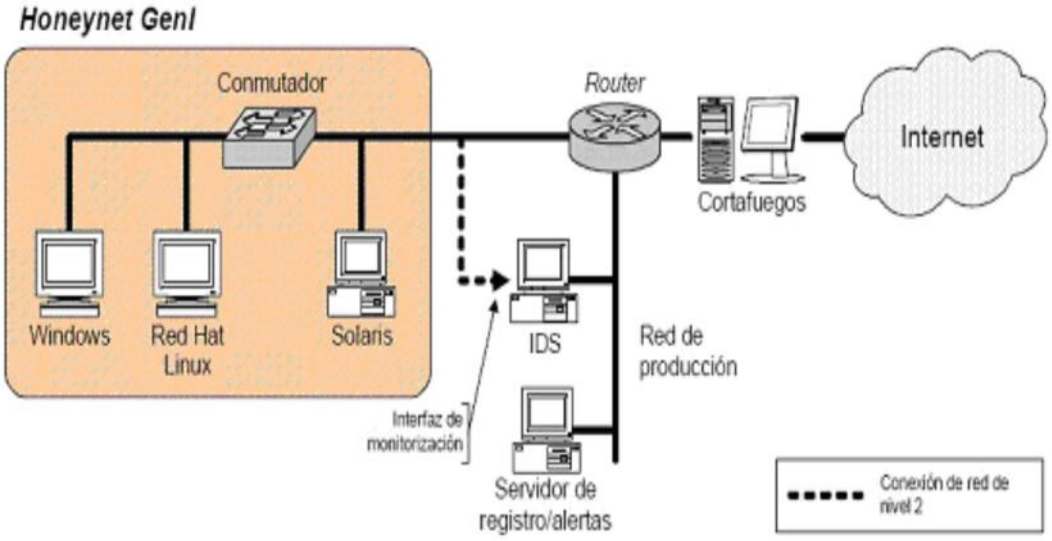


Figura 9: Honeynet primera generación, Sistemas de detección de intrusos (2003). recuperado de http://www.dgonzalez.net/papers/ids/html/

3.4.2 Segunda Generación: La diferencia con la primera generación es que se cuenta con la posibilidad de monitorear a los atacantes durante mucho mayor tiempo, y mejores posibilidades de interactuar con los sistemas comprometidos, sin que estos se den cuenta de la presencia de los honeypots.

El control de datos, captura y recolección se realiza en un mismo recurso, lo que hace más fácil el control y mantenimiento del honeynet. Con el honeynet de segunda generación se establecerá las actividades del agresor y no solo que conexiones realiza.

En esta generación se tiene al honeywall, sistema que contiene las herramientas necesarias para el control de datos, captura y la recolección, es decir todo centralizado.

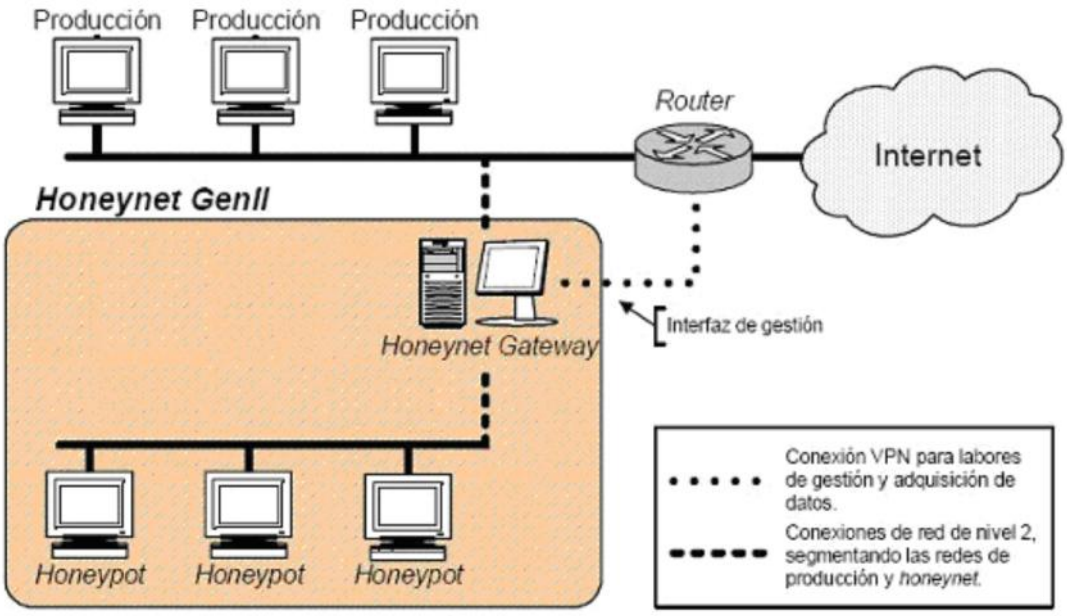


Figura 10 : Honeynet segunda generación. Sistemas de detección de intrusos (2003). recuperado de http://www.dgonzalez.net/papers/ids/html/

3.4.3 Virtuales: Este tipo de honeynet es nuevo, consiste en combinar todos los elementos físicos de la honeynet en un solo equipo, utilizando para ello software de virtualización.

Con los honeynets virtuales existe menor gasto de recursos en infraestructura todo se ubica en un solo hardware, pero la dificultad es que como esta en una sola máquina el atacante puede darse cuenta que es una honeynet y dañar toda su red implementada o a través de esta atacar a toda la red real.

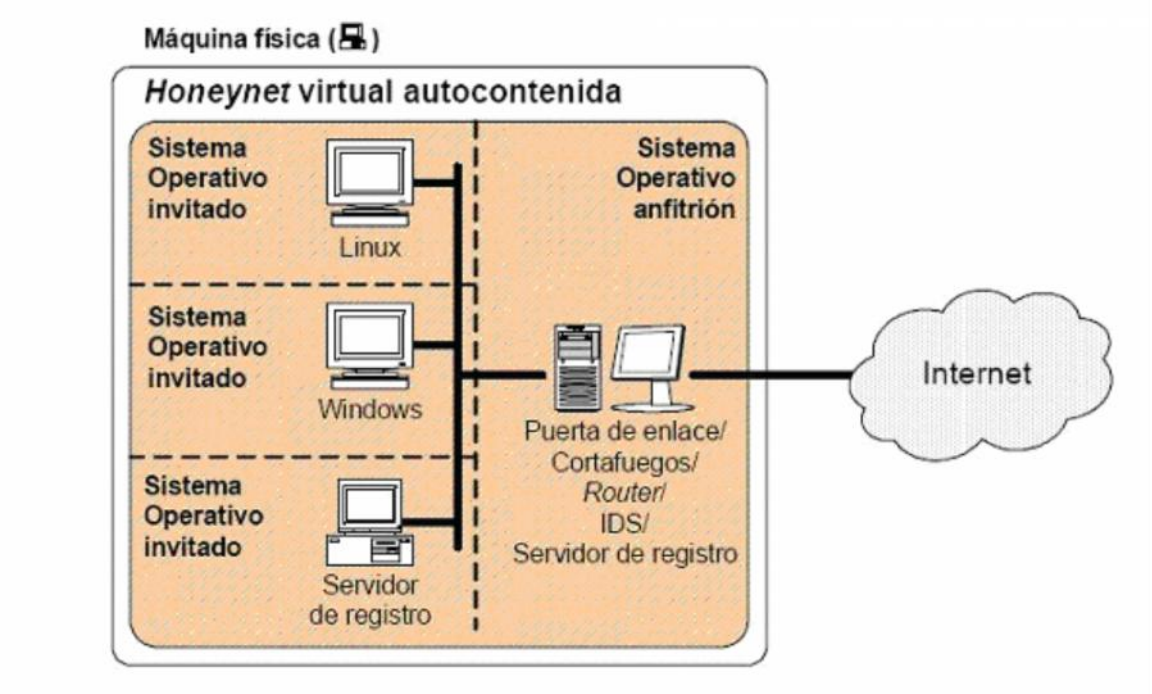


Figura 11 : Honeynet virtual. Sistemas de detección de intrusos (2003). recuperado de http://www.dgonzalez.net/papers/ids/html/

CONCLUSIONES: Para realizar el trabajo de Honeypots se utilizará la herramienta honeywall virtualización, ya que permitirá una revisión de los intrusos mucho más profunda, la información se centralizará y permitirá la simplificación de los procesos de desarrollo y administración de la honeynet.

3.4 Comparación de máquinas virtuales

De acuerdo al marco teórico estudiado en el capítulo anterior, la paravirtualización y virtualización completa son las que tiene un mejor rendimiento en la implementación de virtualización.

Paravirtualización: La virtualización permite que los resultados de rendimientos sean mejores que otras técnicas. En esta plataforma se tiene XEN server y WMWARE ESXI, con estas herramientas analizaremos sus características, funcionamiento y facilidades de uso para el usuario, soporte de servicio y costos.

3.4.1 XEN Server: Es un sistema que utiliza la paravirtualización, es software libre, de código abierto desarrollado por la universidad de Cambridge y que fue comprado por la empresa Citrix.

XEN Server funciona en arquitecturas x86 de 32 y 64 bits.

Funcionamiento:

El software XEN funciona por debajo del sistema operativo, y actúa como un supervisor que se encuentra en la capa cero.

XEN divide en dominios, el sistema operativo de un equipo se ubica en el dominio 1 y el hypervisor de XEN se ubica en el dominio 0, comunicándose directamente con el hardware (CPU), lo que proporciona un mejor rendimiento, es decir que al momento de encender un computador iniciará el hypervisor, que viene a ser un administrador de las máquinas virtuales, como se describe en la Figura 12.

Figura 12: Estructura XEN, recuperado de: http://recursostic.educación.es/observatorio/Web/es/software/servidores/1080-introducción-a-la-virtualización-con-xen

En XEN pueden funcionar sistemas operativos de software libre, con los propietarios es diferente por lo que se requiere modificar el núcleo, pero con las nuevas tecnologías de Intel y AMD han permitido que el sistema operativo se ejecute en nivel 0 sin realizar modificaciones.

Características de XEN Server

Se enumera sus principales características:

- Código fuente reducido y buena velocidad y gestión de los recursos (E/S, red, CPU y memoria).
- Buen rendimiento.
- Con soporte de hasta 32 procesadores en paralelo (SMP).
- Soporta PAE (Physical Address Extension) para servidores de 32 bits con más de 4GB de memoria RAM.
- Permite 'mover en caliente' máquinas virtuales.

- Instalar XEN solo necesita un kernel con el parche de XEN y las herramientas de usuario para poder crear, destruir y modificar los valores de las máquinas virtuales en caliente. (Mifsud-k, 2012)

Costos: Existe versiones que no tienen costo, pero si existe una caída del servicio a quien se acudiría?, ya que no existe empresas que den un soporte de funcionamiento del mismo, y como no se tiene los conocimientos suficientes para atender esta situación, esto puede acarrear problemas si el sistema es importante, para solucionar esta situación adquirir el XEN con costo con el se tiene soporte y mejores ventajas que el gratuito.

Soporte: El soporte es limitado, solo CITRIX que es la empresa de XEN, es la encargada de entregar este soporte, no existe diferentes partnert que apoyen en este tema.

Xen server tiene un mayor nivel de trabajo a nivel de cloud, y la diferencia con VMware es que este tiene mayor estabilidad y conocimiento en el mercado que Xen server y VMware es mas a nivel empresarial.

3.4.2 VMWARE ESXI:

Es una versión especial de la empresa VMware, al igual que XEN utiliza paravirtualización, la diferencia que es un software propietario y tiene costo.

VMware ESXI utiliza hypervisores que se instalan directamente en el hardware del servidor. Proporcionan el mayor rendimiento y escalabilidad. Es decir no requiere de un sistema operativo host como Windows o Linux, su estructura se detalla en la Figura 13.

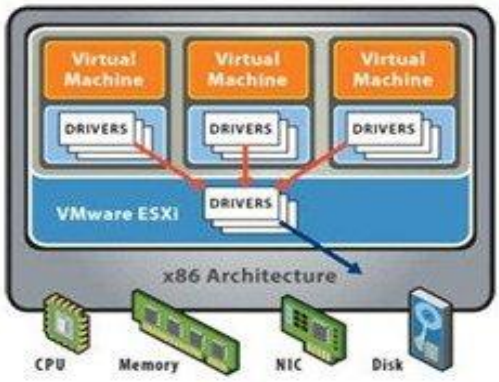


Figura 13: VMware ESXI. Adaptado de VMware vSphere 5.1 Hypervisor (Free – ESXI 5.1) Limitations (2012), recuperado de http://techhead.co/VMware-vsphere-5-1-hypervisor-free-ESXI-5-1-limitations/.

CARACTERISTICAS VMWARE

- Soporte para máquinas físicas con hasta 64 CPUs (físicas), 256 CPUs virtuales y 1 TB de RAM. Cada máquina virtual puede disponer de hasta un máximo de 255 GB RAM.
- Optimización para aplicaciones críticas de negocio: bases de datos Oracle o Microsoft SQL Server, Microsoft Exchange, etc.
- Mejoras de rendimiento para el almacenamiento iSCSI.
- Soporte para multiprocesamiento simétrico (SMP, Symmetric Multi-Processing): una máquina virtual podrá utilizar múltiples procesadores físicos simultáneamente (hasta un máximo de ocho).
- VMware VMsafe: tecnología de seguridad que ayuda a proteger las cargas de trabajo virtualizadas, proporcionando para ello un conjunto de APIs de seguridad.
- VMDirectPath: mejora la eficiencia de la CPU permitiendo la posibilidad de acceder directamente al hardware para aquellos accesos frecuentes a dispositivos de I/O.
- Sistema de archivos clusterizado VMFS (Virtual Machine File System): permite el acceso concurrente de múltiples máquinas virtuales a un mismo espacio de almacenamiento.
- Redes virtuales (Virtual networking): VMware permite la creación de redes complejas entre las distintas máquinas virtuales, empleando para ellos dispositivos virtuales tales como tarjetas y switches.
- Balanceo automático de recursos en función de las necesidades de las máquinas virtuales. (Esxi, 2009)

Costo: A diferencia de XEN el VMWARE ESXI tiene costo, pero con la ventaja de un soporte de la empresa, en el caso que existan problemas de caída, es un software mucho más robusto.

3.4.3 Diferencias entre VMWARE y XEN

Los dos virtualizadores se manejan con paravirtualización, una de las mejoras de XEN es que es un software libre, pero existe una versión mejorada que se requiere de pago al igual que VMware ESXI.

En VMWARE ESXI tiene costo, es comercial, pero te da mejores opciones de manejo y funcionamiento, si se cae o daña el disco duro existen herramientas para su recuperación, a diferencia de XEN, VMWARE es mucho más maduro.

XEN no tiene un soporte oficial para su manejo e implementación, VMWARE si lo tiene.

VMWARE, permite el manejo de la virtualización a través de una interface gráfica que en el caso de XEN no lo tiene.

CONCLUSIONES:

VMware es de fácil uso, su instalación y su forma de manejarlo a través de VMware vSphere Client, el mismo que se conecta en un equipo físico y a través de este programa se puede conectar a diferentes servidores virtuales, es decir una administración centralizada.

VMware ESXI tiene su costo al igual que Xen server con sus versiones actuales, y en el Ministerio de Defensa se adquirieron en el 2011 licencias de VMware ESXI.

Por lo que en esta investigación de Honeypots, se utilizará VMware ESXI, que es más estable, más consolidado y la institución posee las licencias de dicho software de virtualización.

CAPíTULO 4: IMPLEMENTACIÓN Y PRUEBAS HONEYNET

4.1 Introducción

En este capítulo se analizará la situación actual de la red, que servicios los que se utilizan con frecuencia, se implementarán el honeynet y se realizarán las pruebas de ataque al honeynet.

4.2 Medición del tráfico de la red

Se realiza un diagnóstico inicial del estado de la red interna a través de una medición del tráfico que permite determinar su comportamiento en tiempo real y obtener información relevante acerca del tipo, volumen, protocolos y puertos más utilizados, de manera que se establezca un patrón característico acerca del uso de los recursos de la red.

Para realizar este objetivo, se emplea la aplicación gratuita de código abierto NTOP, que según la información en la página oficial del software, es una sonda de tráfico de red diseñada para ejecutarse tanto en plataformas UNIX como en Windows.

Se basa en la librería de captura de paquetes libpcap. Esta herramienta de monitoreo y medición soporta varias actividades de gestión que incluyen la optimización, planeamiento y detección de violaciones en la seguridad de la red.

Se realiza un diagnóstico inicial del estado de la red interna, a través de la medición del tráfico para determinar su comportamiento en tiempo real y obtener información relevante acerca del tipo, volumen, protocolos y puertos más utilizados, de manera que se establezca un patrón característico acerca del uso de los recursos de la red.

Se detallan a continuación los datos obtenidos con Ntop.

4.2.1 Distribución de datos globales por protocolo

Las estadísticas generadas señalan que el 88% del total de datos capturados por NTOP corresponden al protocolo de Internet IP, de los cuales 89% coinciden con el protocolo TCP, el 11.2% a UDP y el 0.0% restante se distribuye entre los protocolos ICMP, ICMPv6, IGMP (Véase Figura 14).

Protocol	Data	Percentage			
IP	163.6 MBytes	87.9%	**TCP**	145.2 MBytes	88.7%
			UDP	18.3 MBytes	11.2%
			ICMP	6.0 KBytes	0%
			IGMP	190.4 KBytes	0%
(R)ARP	1.2 MBytes	0%			

Figura 14: Distribución global de la distribución del tráfico de red

4.2.2 Distribución del tráfico por aplicación

Se describen los protocolos/aplicaciones empleados con mayor recurrencia dentro de la red.

En el gráfico 15, se observa que el protocolo que más se utiliza es el http, servicio de internet, a través del protocolo 80.

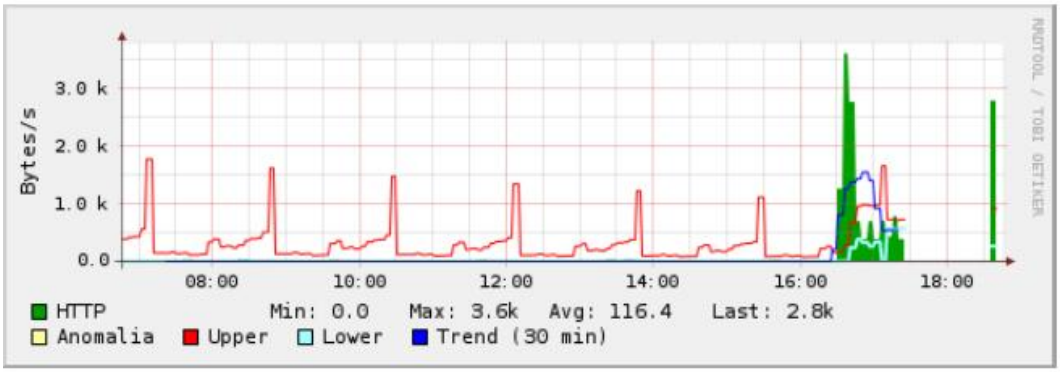


Figura 15: Vista histórica del protocolo HTTP en la red.

El siguiente protocolo que utiliza es el Netbios (Network Basic Input/Output System), que permite ver la entrada y salida sobre tcp/ip, (ver Figura 16).

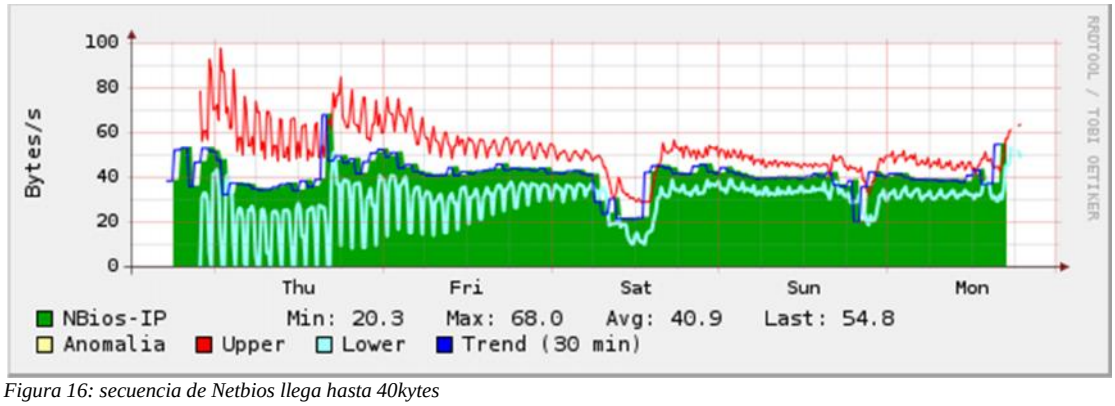


Figura 16: secuencia de Netbios llega hasta 40kytes

4.2.3 Análisis de puertos abiertos en la red

Se realizó un prueba para ver los puertos que se tienen abiertos en la red, se utilizó la herramienta de nmap para Windows gratuita, que permite tener facilidad en su uso a través de pantallas, como se puede observar en la Figura No.17, donde los puertos abiertos son el 21 para FTP, 22 SSH, en el equipo principal.

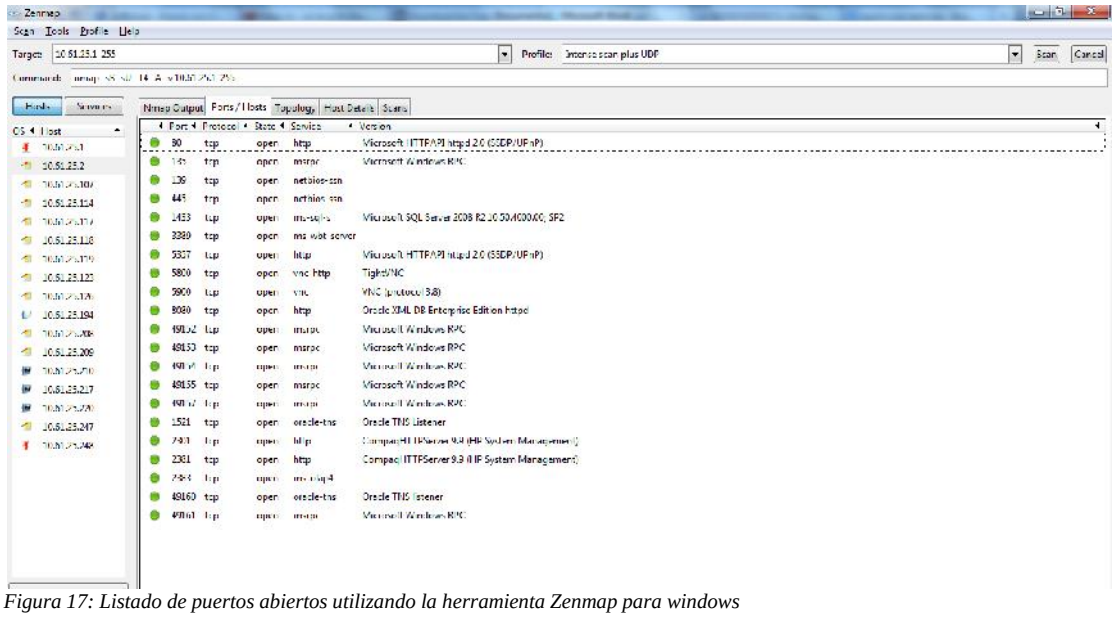


Figura 17: Listado de puertos abiertos utilizando la herramienta Zenmap para windows

Zenmap permite saber qué tipo de sistema operativo se está utilizando en los equipos de la organización, como se puede observar en la Figura 18.

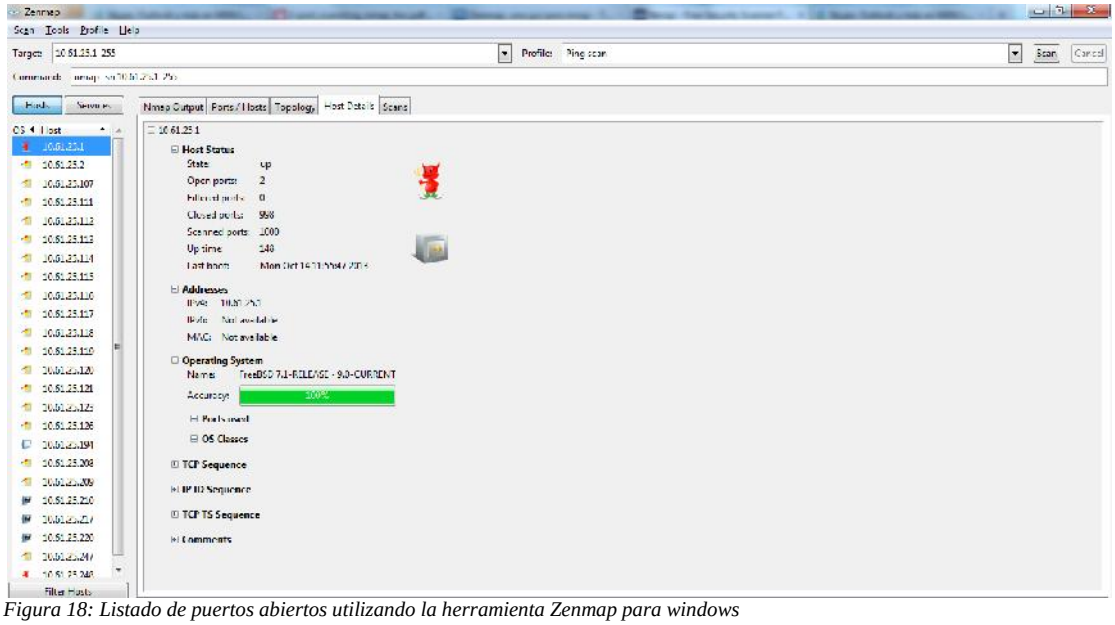


Figura 18: Listado de puertos abiertos utilizando la herramienta Zenmap para windows

4.2.4 Ataque fuerza Bruta

La herramienta Brutus se utilizó, para realizar un ataque de fuerza bruta, el mismo que permite saber claves de equipos, como se puede ver en la Figura No. 19, en donde se ubica la ip a la que se quiere revisar y empieza a realizar una comparación con un listado de datos que se encuentran almacenados en el programa, y proporcionará una idea de que clave puede ser.

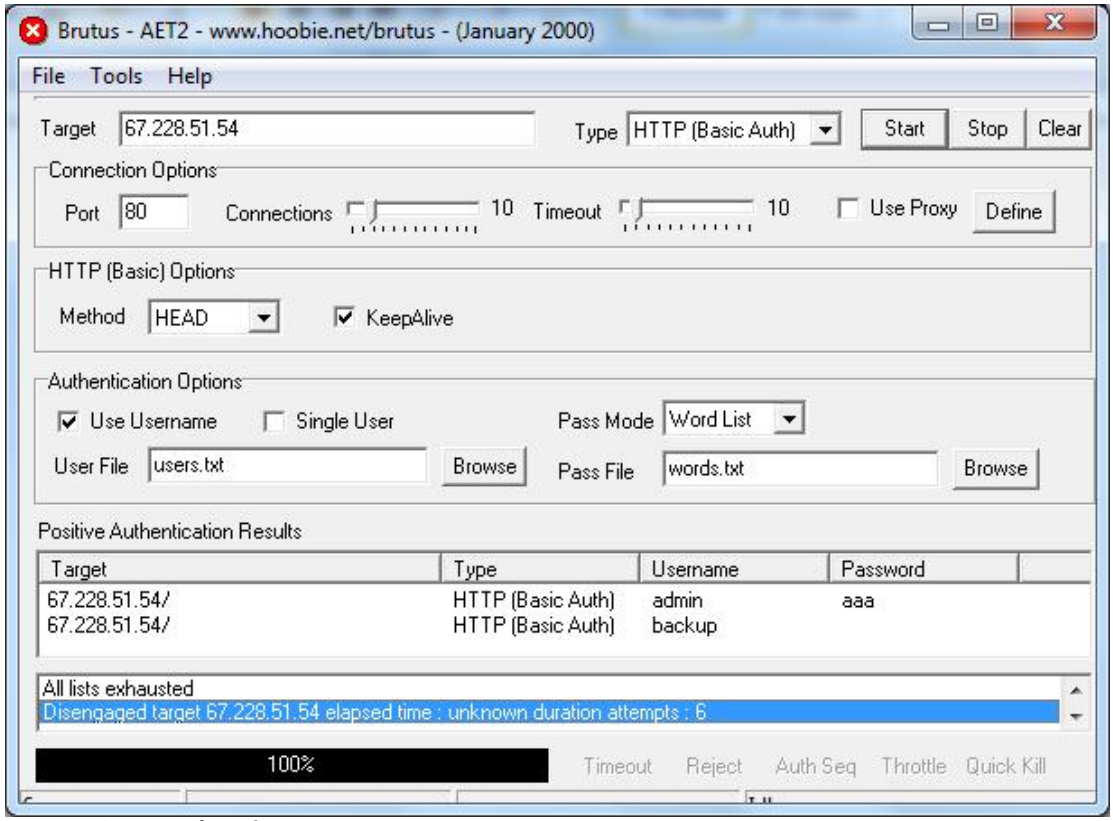


Figura 19: Ataque por fuerza bruta

4.3 Funcionamiento de la Honeynet

Como se explicó en el capítulo III, existen tres arquitecturas de la honeynet, y la que se implementará será de virtualización, que permite el control de datos, captura de datos, análisis de datos y recolección de datos.

Así mismo con el objetivo de minimizar costos se decidió utilizar la virtualización, en el host se instalará el VMware ESXI, que utiliza paravirtualización, lo que permitirá la instalación de las máquinas virtuales del honeynet.

4.4 Ubicación de la Honeypots en la red

Como se vio en el capítulo II, existen diferentes ubicaciones de la honeynet, puede ser en la DMZ pero esta es muy compleja y requiere de un análisis más minucioso.

Otra forma es la ubicación en la red interna, la misma que solo proporcionaría datos interno y no ataques desde fuera de la red.

Pero como uno de nuestros objetivos es detectar los ataques, analizarlos y determinar las vulnerabilidades y mejoras en la red para disminuir el ingreso de intrusos se decide ubicar la honeynet fuera del firewall, ya que se obtendrían los ataques externos que se están realizando en la red.

4.5 Modo de operación de la honeynet

Para el funcionamiento de la honeynet se va a requerir un equipo en el cual se instalará el software de virtualización VMware ESXI que utiliza la paravirtualización.

El honeywall es el principal componente de la honeynets, ya que este actúa como un puente transparente y permite la ejecución de las tareas de control, captura y análisis de datos.

El honeywall utiliza el CENTOS como sistema de control, para lo cual se descarga de: https://projects.honeynet.org/honeywall/, el mismo que gratuito del proyecto “The Honeynet Project”.

Con el honeywall se instalan algunos programas como, el SEBEK, el mismo que permite la captura de extensa colección datos, permite incluso recopilar pulsaciones de teclado en el sistema e incluso en entornos cifrados.

El sebek se ubica en el kernel del sistema operativo, y está comprendido de dos elementos uno como servidor que se ubica en el honeywall y el cliente en uno de los Honeypots, el cual envía los datos hacia el servidor.

Otra de las herramientas que utiliza el honeywall es el sistema de detección de intrusos Snort, que se utiliza para detectar y alertar actividades sospechosas y ataques a los Honeypots, además de esta función permite del tráfico redundante de la red interna.

El honeywall utiliza iptables en la conFiguración del cortafuegos, el mismo que permite las conexiones entrantes y limita las salientes.

El análisis de los datos recolectados se la realiza a través de las interfaces denominada GUIR Web Walleye para examinar las actividades realizadas en los Honeypots, también permite monitorear las alertas de la red interna. Este acceso se lo realiza desde cualquier host perteneciente a la red del Ministerio.

Adicionalmente se dispone de dos Honeypots virtuales, en los cuales se conFigura los servicios de SSH, FTP, WEB, DNS, Base de datos y aplicaciones.

El sistema operativo que se utilizará es el Bad store y Windows xp

.

4.6 Hardware y software necesario

4.6.1 Equipo anfitrión

Servidor HP Proliant ML370 G5
Memoria RAM de 2 GB
Disco Duro de 200 GB
Tarjeta de red de 10/100/1000 Mbps
Software VMware ESXI 5, para la instalación de las máquinas virtuales y el honeywall

4.6.2 Honeywall requiere del siguiente software

MySql Server: servidor de base de datos utilizado para almacenar y relacionar el contenido capturado.

Sebek Server: Es una herramienta diseñada para capturar al atacante sobre las actividades en el Honeypots.

Snort: sistema de detección de intrusos basado en reglas capaz de realizar análisis de tráfico de la red.

Snort inline: Toma decisiones sobre el tráfico saliente siempre y cuando tenga ataques conocidos.

Swatch: Es una herramienta que comunica al administrador incidentes a través de correo electrónico.

Menú: Una interfaz gráfica utilizada para la conFiguración y mantenimiento del honeywall.

Pcap: Interfaz de captura de datos del kernel de Linux.

Walleye: proporciona al administrador herramientas de análisis de datos de manera remota.

4.6.4 Configuración de los Honeypots

Honeypots 1,

Se requiere del siguiente software instalado:

- El sistema BadStore, de 11MB, que arranca un sistema Linux en modo live, este software permite realizar explotación de vulnerabilidades Web.

- En este sistema se encuentra instalado una página Web, la misma que permitirá realizar ataques y ver sus vulnerabilidades.

- Se encuentra instalado servidor Web Apache que es open source para el levantamiento de páginas Web.

- Programa PHP, para desarrollar páginas Web,

- MySql donde se almacena los datos de la página Web que tiene el Badstore

- Se encuentra habilitado SSH para conexiones remotas.

Honeypots 2

Se instala Windows xp sin service pack, en este sistema operativo se aloja el programa sebek cliente para recolectar los datos y tendrá las vulnerabilidades propias del Windows xp.

Honeypots3

En este honeypots se instaló el sistema operativo CENTOS, conjuntamente con SSH y FTP.

Instalado el servidor Apache para ejecución de página Web

4.7 Instalación de la red honeynet

El honeywall se instalará fuera del firewall, la máquina anfitrión tiene una Ip pública y cada honeypot se le configura una ip privada, esto se realiza para que se puedan conectarse desde fuera a los equipos y realizar los ataques, como se muestra en la Figura 20.

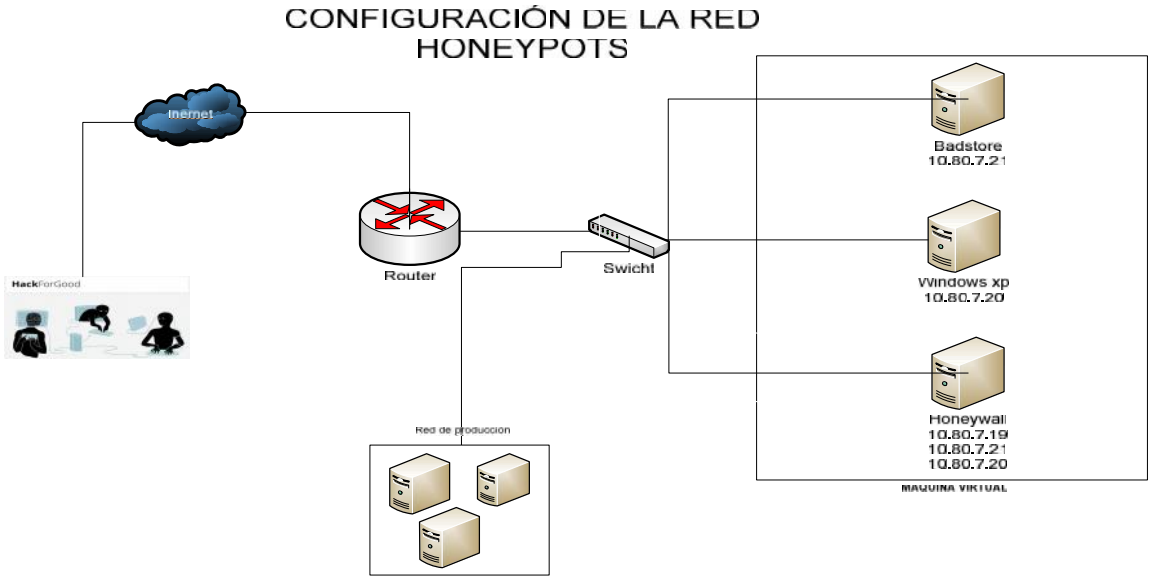


Figura 20 : Honeynet virtual en la red

Qué se consigue con esta conFiguración:

- Acceso directo de los atacantes, y obtener información del comportamiento de los mismos, se obtiene datos reales del ataque.
- Evitar que otros sistemas de seguridad intervengan en el ataque
- Evitar la detección de atacantes internos, ya que se tiene controlado internamente el funcionamiento de los equipos por usuarios del Ministerio.
- Que la red en producción no sufra algún daño.

ConFiguración de la red:

Como se puede observar en la Figura 14, se está realizando las conexiones, de la honeynet con los equipos físicos y virtuales necesarios para un buen funcionamiento.

En una sola máquina física se conecta directamente con la red de producción, con el software de virtualización VMware ESXI, utilizado para levantar las tres máquinas virtuales usadas dentro de la honeywall.

Honeywall utiliza tres interfaces virtuales de red: una en modo brigde y dos en modo host-only, y los Honeypots utilizan la interface virtual host-only. Este método host-only permite la conexión entre máquinas virtuales entre sí, mientras que en modo bridge se asocia a la red externa o en producción, hacia el equipo anfitrión.

4.8 Instalación y conFiguración WMWARE ESXI

El software de virtualización se va a utilizar para la creación de las máquinas virtuales es VMware ESXI, el mismo que debe ser instalado correctamente para el levantamiento de las máquinas virtuales, Anexo a.

Como primer paso se va a instalar la máquina virtual honeywall, para lo cual se utilizará la versión 1.4, se instalarán tres tarjetas de red, de tal manera que eth0 eta en modo bridge y eth1 y eth2 en modo host-only.

4.9 Instalación y conFiguración del Honeywall

Se levanta la máquina virtual y booteamos la imagen del disco CD-ROOM, con esto se inicia el proceso de instalación automático, después de la instalación se reiniciará el sistema desde el CD-ROM.

EL honeywall viene con dos cuentas roo y root, las mismas que comparte las misma clave, por defecto es honey, que dará paso a la instalación del programa, para mayor detalles de la conFiguración en el Anexo b.

4.10 Instalación de los Honeypots

Se van a instalar tres máquinas virtuales correspondientes a los Honeypots, usando badstore y Windows xp sin servipack la misma que presenta vulnerabilidades y una máquina con Centos.

Cada máquina virtual tendrá una tarjeta de red en modo host-only, en la cual se instalarán los sistemas operativos.

4.11 Pruebas

Se requiere realizar pruebas de conexión de los Honeypots, con el honeywall, para saber si existen conexiones entre las máquinas.

4.11.1 Prueba No. 1:

- Los Honeypots deben poder establecer conexiones entrantes y salientes a la red interna usando el protocolo IP.
- Realizar Ping a cada Honeypots desde la máquina de pruebas,
- Ejecutando ping <IP>.
- Verificar que se obtiene respuesta de conexión entre los Honeypots

- Se verificó, mediante respuestas echo replies al comando ***Ping***, desde el honeypots 1 al honeypots2, como se puede ver en la Figura No. 21, existe conectividad entre el honeypots 2 al honeypots 3, como se ve en la Figura No. 22

.

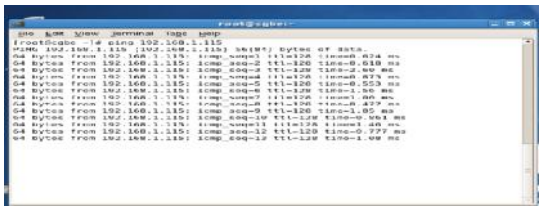


Figura No. 21, Ping de conexión honeypots 1

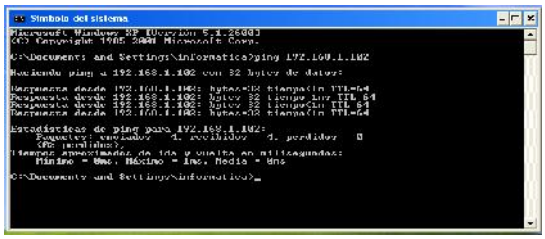


Figura No. 22, Ping de conexión honeypots

4.11.2 Prueba No. 2:

Otra de las pruebas de funcionamiento del honeywall, es la observación de la captura de información a través de Inboud, que registra los ping que se realizó, a través del protocolo ICMP. Como se puede observar en la Figura No. 23

- El Honeywall está registrando el tráfico.
- Ingresar al Honeywall como root.
- Seleccionar Menu->Status->Inbount Connectios/Onbout
- Connections

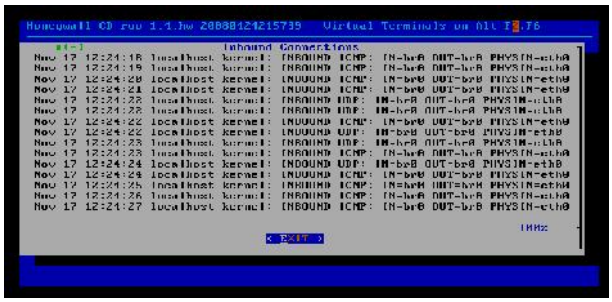


Figura No. 23, registró de tráfico al honeywall

4.11.3 Prueba No. 4

Verificar si están enviando alertas por e-mail, se prueba al entrega de correos a través del puerto 25 SMTP del honeywall, como se puede observar en la Figura No. 24

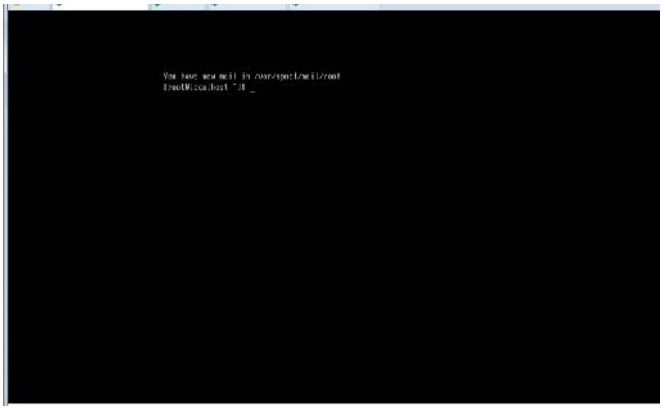


Figura No. 24, Funcionamiento de correo del honeywall

4.11.5 Prueba No. 5

Verificar si Sebek realmente está recolectando la actividad de los sistemas, como se puede verificar en la Figura No. 25, está marcada con la palabra sebek, que indica que si está funcionando.

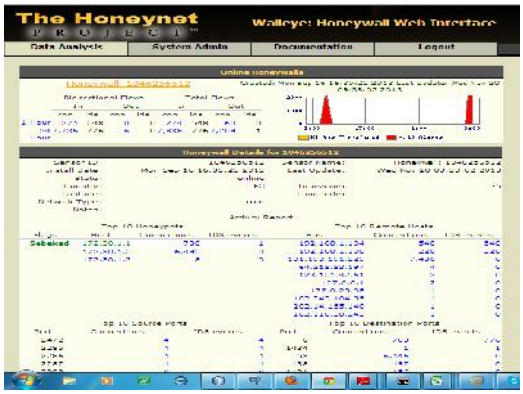


Figura No. 25, Funcionamiento de la herramienta sebek

4.11.6 Prueba 6

Otra prueba es ver el funcionamiento de la página de administración del honeywall – walleye, como se ve en la Figura No. 26.

- Walleye está activado y permite ingresar con el usuario.
- Conectar la máquina de pruebas a la interface de administración, conFigurar la IP correspondiente e ingresar a “https://IPADMISTRACIÓN/walleye.pl:443’.
- Ingresar el usuario y contraseña.
- Verificar que el acceso este correcto.

Figura No. 26, Funcionamiento de la página de administración de honeywall

4.12 Recolección de datos

Una vez que se ha conFigurado e implementado la red honeynet con los honeypots en la herramienta de virtualización (VMware), y realizada las pruebas de conexión, el siguiente paso a seguir es el Control, la Captura y el Análisis de Datos.

4.12.1 Simulación de ataques informáticos

Para empezar a realizar una simulación de ataques se sigue los siguientes pasos que realiza un profesional en ethical hacking:

- Reconocimiento del objetivo o a quien se va a realizar el ataque
- Búsqueda de vulnerabilidades
- Realizar el ataque
- Obtención de resultados

De acuerdo a la revisión de los procesos que realizan los hackers existen dos procesos que son Mantener acceso que consiste en retener los privilegios como atacante a lo que se descubrió para que otros no puedan ingresar, otro punto es borrado de huellas cuyo objetivo es borrar las huellas de ingreso, cuyos puntos no se realizará ya que no se tiene el pleno conocimiento para realizar estos pasos.

- **Reconocimiento del objetivo o a quien se va a realizar el ataque**

Consiste en analizar la institución, empresa a la que se va a realizar el estudio, cual es su funcionamiento, a que se dedica la institución.

- **Búsqueda de vulnerabilidades o escaneo**

El escaneo es la fase de pre-ataque, donde se escanea la red con la información anterior, con el fin de establecer vulnerabilidades y puntos de entrada para realizar el ataque.

- **Realizar el ataque**

Consiste ya en la penetración hacia las vulnerabilidades presentadas en la fase anterior, es decir realizar el ataque mismo.

- **Obtención de resultados**

Después de realizar los ataques, se analizará que tipo de información generó el honeynet, también se realizan simulación de ataques para ver el funcionamiento del honeynet y establecer su respuesta.

Para facilitar se ha utilizado la herramienta de Open Source de seguridad de Linux “Backtrack 5R1”, la misma que permite realizar ataques hacia una red ya que esta se desarrollo específicamente para los profesionales de seguridad informática los cuales utilizan, para realizar ingreso a las redes, esta herramienta se implementó como una máquina virtual.
Se utilizó la herramienta de apoyo en la simulación, el Wireshark, que es un analizador de paquetes de red software de código abierto, el mismo que permitirá examinar con detalle el contenido del paquete de red, los ataques se realizaron de acuerdo a las fases establecidas anteriormente.

4.12.2 Fase búsqueda de vulnerabilidades

Escaneo de puertos TCP/SYN

Esta técnica es la llamada escaneo "half-open" (o mitad-abierta), lo que hace es enviar un paquete SYN como si fuera a entablar una conexión TCP completa y se espera por una respuesta. Se puede recibir un SYN|ACK si el puerto está escuchando o un RST si el puerto está cerrado. Si se recibe SYN|ACK en respuesta, inmediatamente se envía un RST (Acosta)

La simulación del ataque se efectúa empleando NMAP, una herramienta gratuita que facilita la exploración de redes. Para lo cual digitamos el comando en Backtrack, el mismo que permitirá conocer los puertos que permanecen abiertos en el Honeypot 2

(172.30.1.5) como se puede observar en la Figura No. 27, la respuesta a este ataque se registra en el honeyneto, como se puede ver en la Figura No. 28.

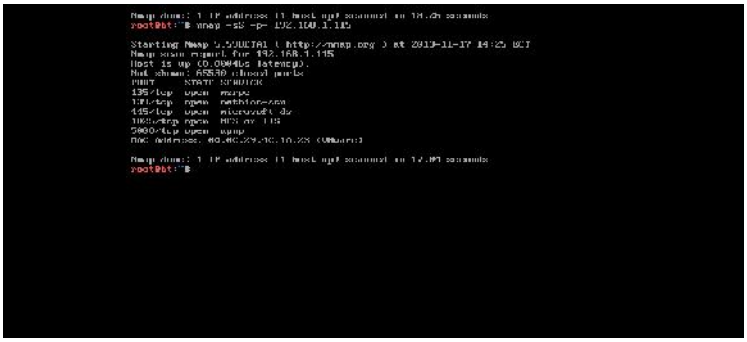


Figura No. 27, muestra de escaneo de puertos

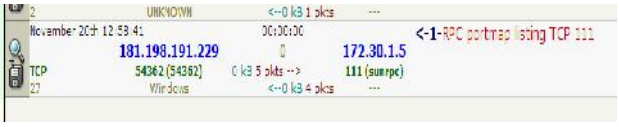


Figura No. 28, registró del escaneo de puertos en el honeywall

El honeynet, indica que ser realizó desde la ip 181.198.191.229, un scaneo de puertos a las 12:58, al honeypots 172.30.1.5.

Una vez que se ha realizado un análisis de vulnerabilidades, se puede ver que los puertos 22 y 21 se encuentran abiertos, por lo que se realiza un ataque al puerto 22.

4.12.3 Fase de ataque

Ataque de fuerza bruta

Se realizó un ataque de fuerza bruta a MySql del honeypot 2, con el siguiente comando: **medusa –h 172.30.1.3 –u root –P /pentest/passwords/John/password.lst –M MySql –f –b,** realiza un escaneo de acuerdo a la Figura No. 29 , indica que no tiene

clave MySql, con el usuario root, y el honeynet detecta el ingreso a la red como se puede ver en la Figura No. 30.

Figura No. 29, registró del ataque para saber la clave del servicio SSH

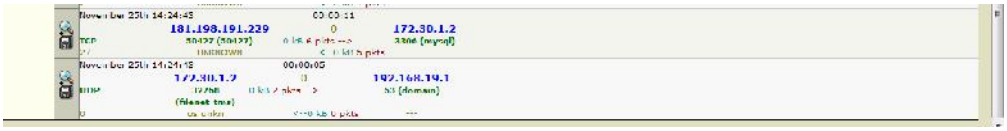


Figura No. 30, registró del ingreso al MySql instalado en el honeypots 172.30.1.2

Se realizó un ingreso a MySql, al saber que no tiene clave, con el siguiente comando: MySql –u root –h 172.30.1.5, el cual permite ingresar a la base de datos, se puede observar en la Figura No. 32.

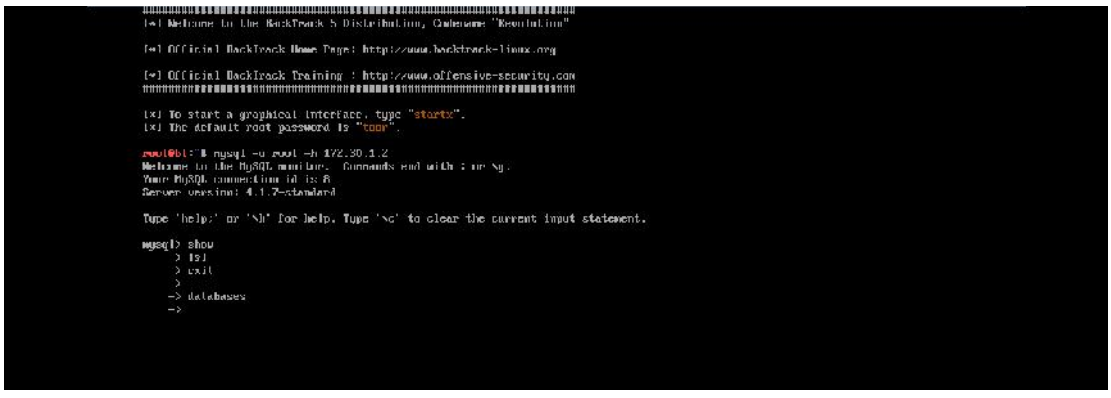


Figura No. 32, Ingreso a la base de datos MySql del honeypot 2.

Ataque de denegación de servicios usando inundación Tcp/syn (flooding)

Este tipo de ataque, consiste en enviar un número elevado de paquetes, con lo cual la red se inunda y comienza la denegación de servicios del equipo al que se está realizando el ataque. Esta técnica permite atacar el ancho de banda.

Se realiza un ataque en contra el honeypot 2, con el comando hpin3, que es una herramienta que permite crear y analizar paquetes tcp/ip, pero también permite realizar un syn flodd attack.

Comando: hping3 –i eth0 172.30.1.2

El honeywall registra el ataque y muestra el siguiente mensaje, como se puede observar en la Figura No. 31

Figura No. 31, Registró del ataque de denegación de servicio

Un ataque de denegación de servicio, se puede observar que se realizó el 29 de noviembre a las 8h30 de la mañana, como se puede observar en la Figura No. 32

Figura No. 32, Registró del ataque de denegación de servicio

En este caso el atacante está realizando un tráfico al puerto 80, esto ocasionó que al querer ingresar a la página de administración del honeynet no se pueda desde otra red y el honeynet no capturo más peticiones.

Se pudo ver con la herramienta de análisis wireshark que el puerto0, rechazo la conexión ya que este se encontraba cerrado, enviando una respuesta RST, como se puede ver en la Figura No. 33.

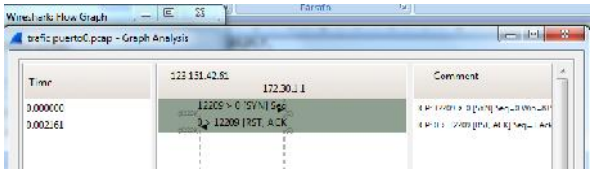


Figura No. 33, Registró del ataque de denegación de servicio

4.12.4 Herramientas de apoyo para el análisis de la información capturada

Con la ayuda del software networkminer, se puede establecer el ip del equipo que ingreso a nuestra red, ayuda a ver qué sistema operativo utiliza, como se puede ver en la Figura No. 34.

Figura No. 34, revisión con el networkminer de los equipos que ingresaron a la red

De esta información se deduce que la ip 221.50.89.83 de Japón, ingreso a nuestro honeypots 172.30.1.2, puerto 80, tal vez su ingreso fue a la página Web que está funcionando en el badstore.

En la Figura No. 35, a través del networkminer, se puede ver también los ataques de spoofing a la red, este software lo reconoce como anomalías.

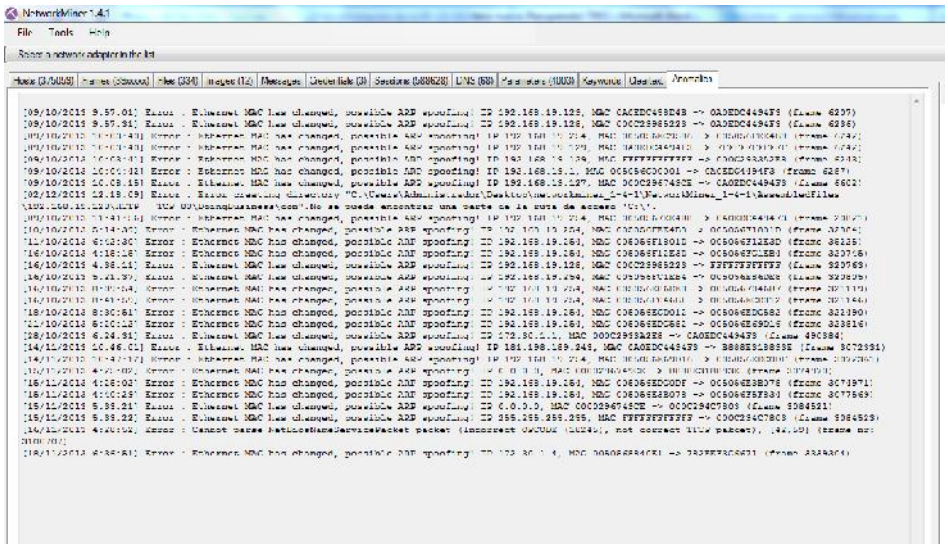


Figura No. 36, alerta sobre el ingreso de spoofing

CAPITULO 5: EVALUACION DE RESULTADOS Y DISCUSION

5.1 Actividades recolectadas de los honeypots

Después de haber implementado la Honeynet, se comprobó su correcta actividad conjuntamente con sus instrumentos, por lo que se procede a realizar un análisis e interpretación de los datos, para establecer conclusiones de este proyecto, esta recolección de datos se realizó durante un mes.

Se utilizó herramientas que ayuden a interpretar los datos obtenidos, como el Excel, para realizar los análisis establecidos.

- **Resumen total de conexiones**

De la revisión a los datos obtenidos se puede observar que se realizaron algunas conexiones a los honeypots, se analizó el tráfico dirigido a los honeypots, es necesario indicar que todo el tráfico realizado en el sistema de honeypost es considerado como malicioso, esto se debe a que los honeypots no tienen información importante para los usuarios de la red.

Se registraron un total de 250.000 conexiones, de los cuales el mayor número se registra en el protocolo TCP con un total de conexiones de 245.683 que corresponde al 91,62%, el protocolo UDP que corresponde a 22.260 que representa el 8,30% y en ICMP corresponde a 225 conexiones que representa el 0,08%. (Véase Figura No. 37)

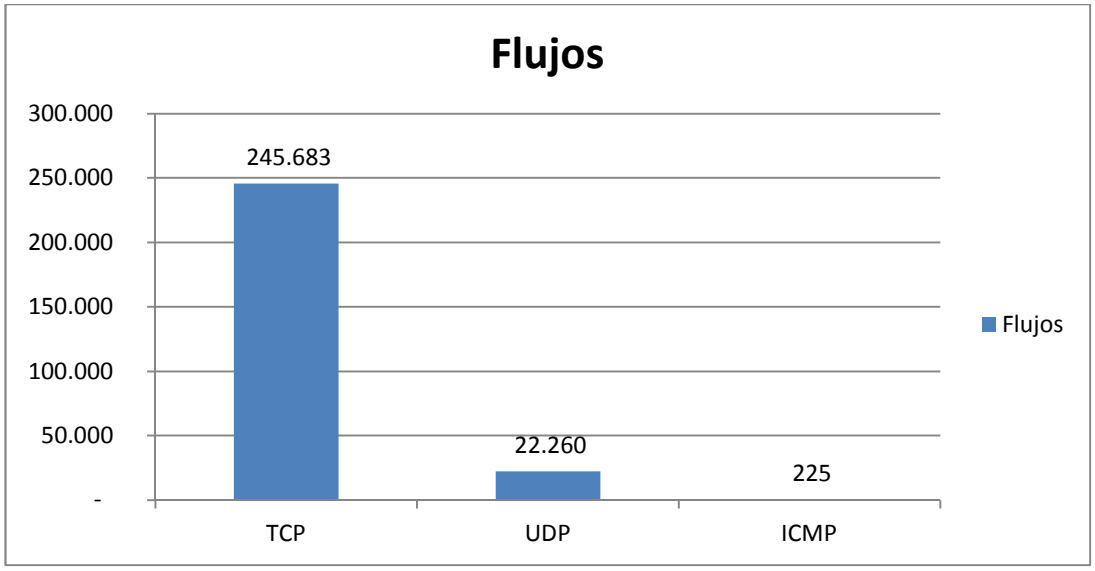


Figura No. 37, conexiones realizadas

- **Puertos de destino más frecuentes**

Se detalla los puertos a los que se realizaron conexiones más frecuentes, registradas en los honeypots. Se visualiza en el cuadro No. 1 y Figura No. 38

Se puede observar que la mayor conexión que existe es en el puerto 80, http, que ocupa el 96% de ingreso, así mismo hubo un ataque de denegación de servicio hacia el puerto 80, realizando que se ejecuten conexiones múltiples, y estos se registren en la red.

El 1,16 representa a conexiones del puerto 443, que corresponde a las conexiones de salepes que es la interfaz gráfica del honeynet, para revisar y realizar análisis del ingreso a la red.

El 0,95% hace mención al puerto 53, correspondiente al servicio DNS, que es un servicio de nombres de dominio.

El 0,91% hace mención al puerto 1101 que corresponde a la conexión del honeynet con el sebek cliente que se encuentran ubicado en el sistema operativo Windows.

El puerto 25 SMTP que tiene un porcentaje del 0,27%, corresponde a los envíos de correos desde el honeynet, para informar como está funcionando el servicio del honeynet.

El 0,19% representa al puerto 22, que maneja SSH, que es un protocolo que facilita conexiones remotas seguras entre dos sistemas a través de cliente/servidor, para poder ingresar a un equipo a través de este puerto, es necesario establecer claves seguras.

Los puertos 137, 135 , 445 y 21 representan menos del 0,01% de tráfico, por lo que no representan mucho movimiento de estos puertos, pero, el puerto 21 que corresponde a FTP- Protocolo de transferencia de archivos entre sistemas cliente servidor, de lo que se puede ver se intentó ingresar a este protocolo, con 31 conexiones.

Cuadro No. 1, Puertos de destino más frecuentes

DESCRIPCIÒN	CONEXIONES	%
FTP - 21	31	0,02
Microsoft-Ds - 445	59	0,04
Portmapper de Windows - 135	82	0,06
NetBios Name Service -137	257	0,18
SSH - 22	277	0,19
SMTP -25	380	0,27
PT2-DISCOVER 1101	1.305	0,91
DNS - 53	1.349	0,95
HTTPS-443	1.654	1,16
HTTP - 80	37.329	96,22
TOTAL	**142.723**	**100,00**

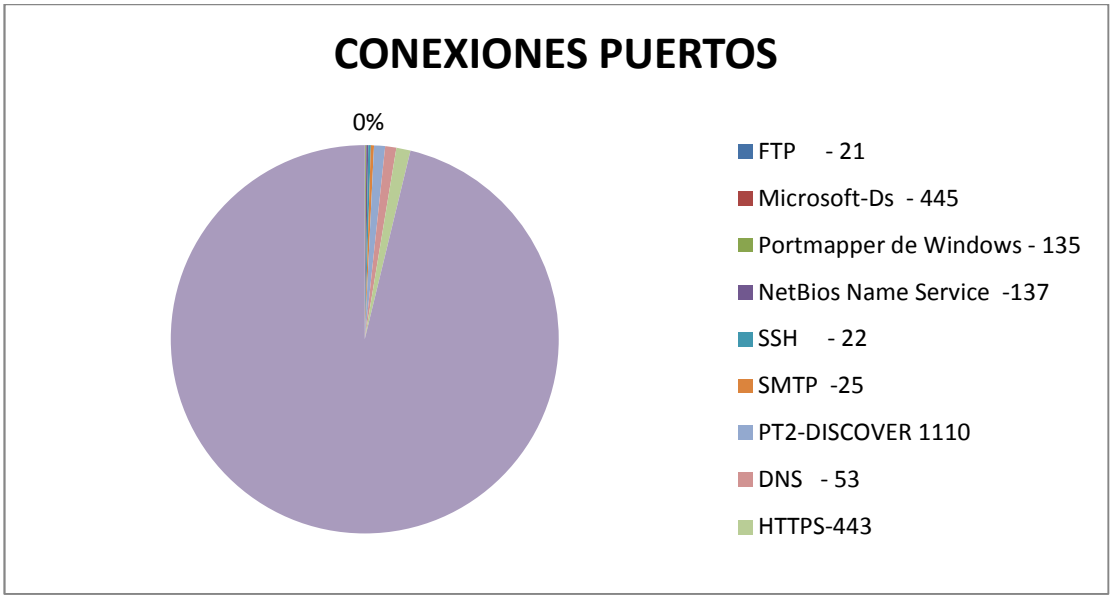


Figura No. 38, comparación de los puertos más accedidos registrados en el honeywall

A continuación se detalla las direcciones ip que ingresaron a la red de acuerdo a los diferentes tipos de servicios ofrecidos por los honeypots. El cuadro No. 2 reporta el ingreso al puerto 443, que ejecuta el servicio http.

Cuadro No. 2, ip que ingresaron al puerto 443.

DIRECCIONES	CONEXIONES
198.143.173.183	1
192.168.1.118	1
181.198.191.229	1,221
181.198.189.243	30
172.30.1.20	4
172.30.1.1	1,977
141.212.121.46	1
141.212.121.30	5
141.212.121.10	4
134.170.24.123	1
59.159.25.12	1
54.254.203.3	1
37.247.36.97	1

Del cuadro No. 2, se puede ver que la conexión que se realiza es de la ip 172.30.1.1, pero este equipo corresponde al honeypots 1, esta se debe a que se utiliza la conexión para ingresar al wallepey, que es la página de administración del honeywall.

Otra de los puertos que se analizó es el 3306, por donde se ejecuta la base de datos MySql, en el cuadro No. 3, se detalla las ip de origen hacia la base de datos.

Cuadro No. 3, ip que ingresaron al puerto 3306.

DIRECCIONES IP	CONEXIONES
216.99.158.72	1
181.198.191.229	46
181.198.189.243	1
169.77.152.168	1
162.212.181.89	1
88.80.223.152	5
58.92.126.182	1

Del análisis se puede observar que la ip 182.198.191.229 realizó el mayor tiempo de conexiones hacia la base de datos MySql del honeypots 1 y en segundo lugar es la ip 88.80.223.152.

Se realizó un análisis del puerto 22, conexión a SSH, en el cuadro No. 4 se detalla las ip que trataron de acceder al servicio.

Cuadro No. 4, ip que ingresaron al puerto 22.

DIRECCIONES IP	CONEXIONES
222.189.239.124	1
222.189.239.83	2
222.189.239.72	1
222.189.239.70	1
222.189.239.42	1
222.175.114.136	1
222.175.114.132	1
222.73.236.219	1
222.43.96.226	1
221.12.12.3	1

DIRECCIONES IP	CONEXIONES
220.181.82.213	1
218.26.89.179	1
207.178.204.85	1
195.145.53.226	1
192.168.1.103	2
192.168.1.102	1
192.168.1.100	4
192.96.206.158	1
192.96.206.139	2
190.145.7.78	1
188.190.98.6	1
183.129.249.98	1
181.198.191.229	472
181.198.189.243	7
180.211.214.206	1
123.150.106.145	2
113.12.83.88	1
93.120.27.62	1
89.45.14.87	1

Se puede ver que el número de conexiones ip que trataron de ingresar a este servicio son mayores que las ip que ingresaron en los servicios anteriores, aunque realizan una sola conexión.

Se detalla en el cuadro No. 4, las ips que se conectaron en el puerto 80, aunque la mayoría de todos realizan una sola conexión, se escogió una pequeña muestra, ya que existían distintas ip, alrededor de 4.000.

Cuadro No. 5, ip que ingresaron al puerto 80

DIRECCIONES	CONEXIONES
223.167.226.213	1
223.168.156.170	1
223.168.160.123	1
223.172.138.198	1
223.172.172.243	1
223.172.182.168	1

DIRECCIONES	CONEXIONES
223.172.226.182	1
223.173.219.198	1
223.174.211.108	1
223.176.138.122	1
223.176.197.167	1
223.177.193.171	1
223.179.186.235	1
223.179.236.250	1
223.181.134.219	1
223.181.158.179	1
223.182.123.183	1
223.182.136.186	1
223.182.198.219	1
223.183.132.148	1
223.185.152.110	1
223.185.221.164	1
223.186.102.118	1
223.186.113.131	1
223.186.250.121	1
223.193.100.120	1
223.193.123.109	1
223.193.173.242	1
223.193.176.102	1
0.0.0.0	2
1.93.48.94	1
2.0.119.179	1
2.0.219.189	1
2.10.120.223	1
2.10.134.109	1
2.11.107.164	1
2.11.120.198	1

5.2 Ubicación de las ip que registró el honeynet

Revisando aleatoriamente las ubicaciones de las direcciones ip, se puede ver que los ataque son de China, Korea, Francia, Estados Unidos, como se puede ver en las

siguientes Figuras, se utilizó la herramienta del Geo ip Tol, que permite ver a que país pertenece las ips, como se pueden ver en las Figuras No. 39,40 y 41.

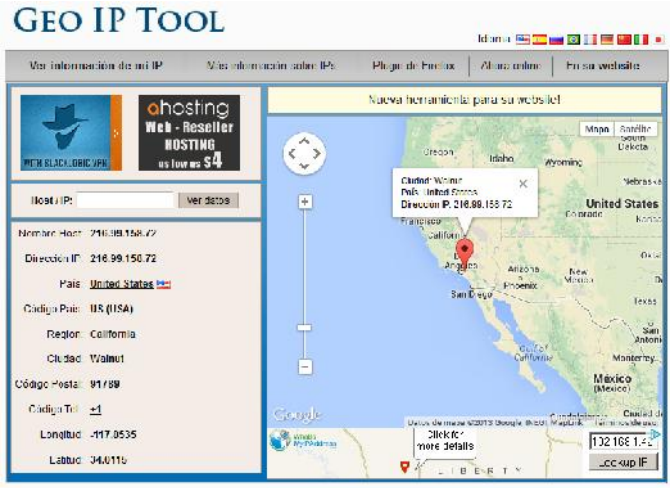


Figura No. 39, ip 216.99.158.72, se ubica en Estados Unidos

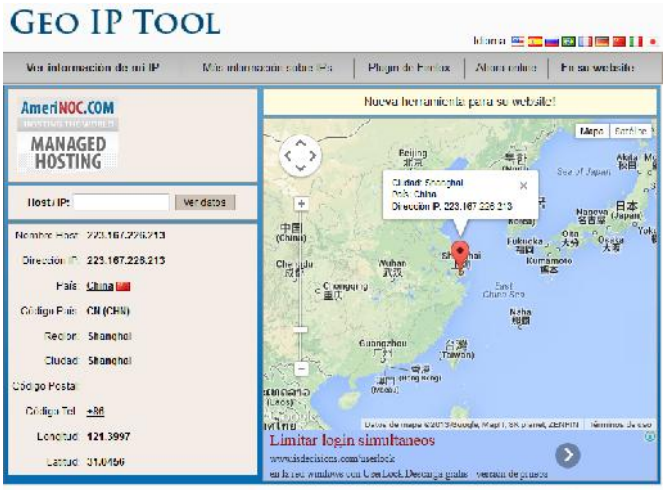


Figura No. 40, ip 223.167.226.213, se ubica en China

Figura No. 41, ip 223.167.226.213, se ubica en China

5.3 Comparación entre el tráfico inicial sin el honeynet y con el honeynet

Del análisis de tráfico que se realizó en la institución sin el honeynet, se puede observar que tienen el mismo comportamiento, el protocolo más usado en ambos ambientes es el TCP, como se puede ver en las Figuras No. 42 y 43.

	Data	Percentage				
	163.6 MBytes	87.9%	TCP	145.2 MBytes	88.7%	
			UDP	18.3 MBytes	11.2%	
			ICMP	6.0 KBytes	0%	
			IGMP	190.4 KBytes	0%	
	1.2 MBytes	0%				

Figura No. 42, Tráfico sin honeynet

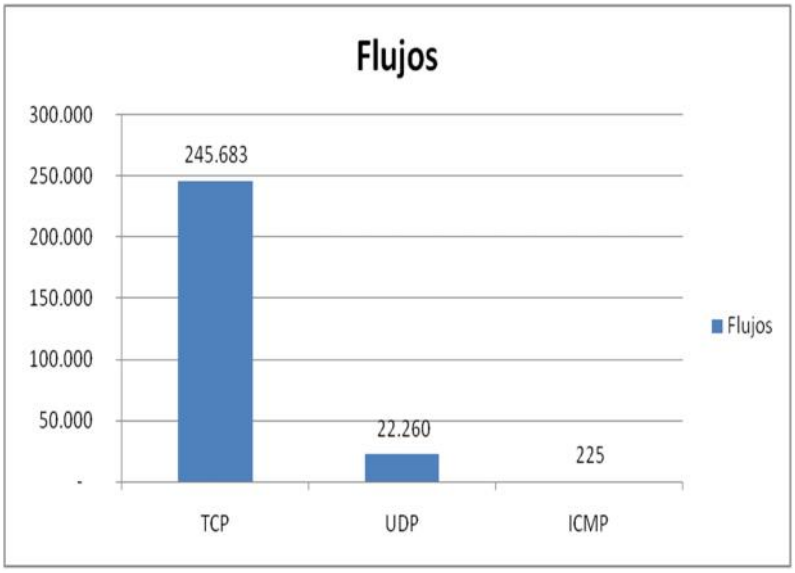


Figura No. 43, Tráfico con honeynet

Lo que se puede ver es que con el honeynet, existen más conexiones de red que en la red de producción, por lo que se deduce que hubo gran cantidad de movimientos en la red.

En relación a los puertos más utilizados con el honeynet y en la red de producción, en el análisis el puerto 80 es el que presenta mayor cantidad de movimiento, como se puede ver en las Figuras No. 44 y 45.

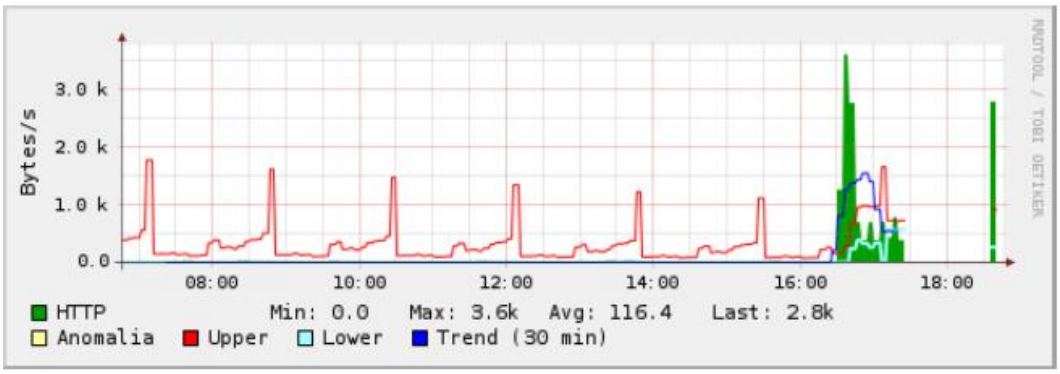


Figura No. 44, Puerto 80 más utilizado red de producción

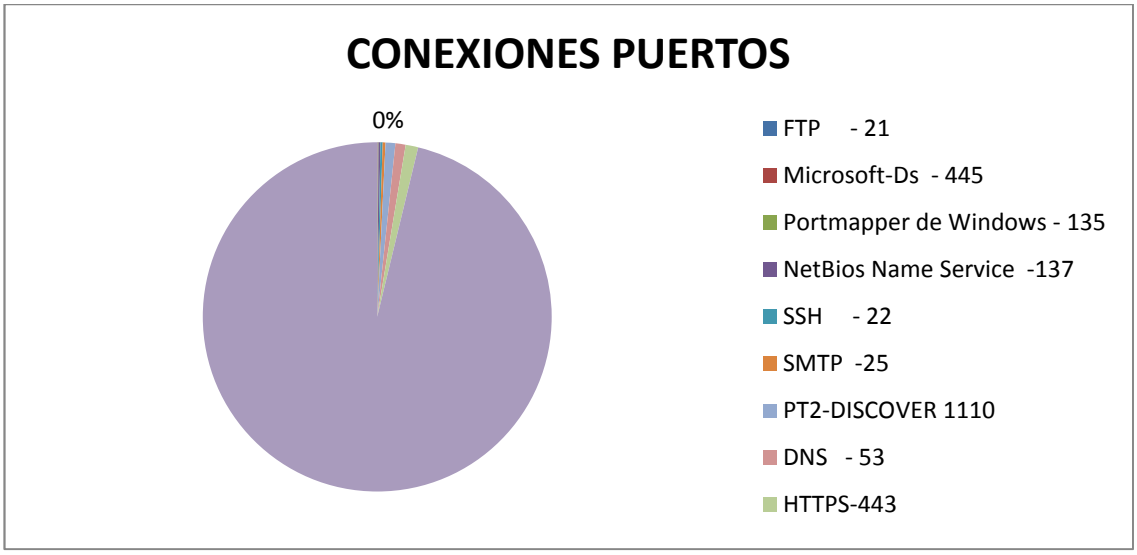


Figura No. 45, Puerto 80 más utilizado en honeynet

En la red de producción se debe un uso más en el puerto 80 ya que la mayoría de personas navegan y todos los sistemas gubernamentales son por el Internet, en el caso del honeynet, se debe a que hubo un ataque dos la puerto 80, lo que registró estas actividades el honeynet.

Igualmente se hicieron ataques de scaneo de puertos en la red de producción, los mismos que no se registraron ya que no existe un IDS para poder establecer estas conexiones, igualmente se realizó un ataque de fuerza bruta la misma que no se registró o detectó, la diferencia con el honeynet es que en este si se registró los tipos de ataque y que está realizando el atacante hacia la red.

5.4 Discusión

En base al trabajo elaborado en este proyecto, se ha tenido resultados en el desarrollo de las tecnologías honeynet y este ha sido muy importante en el desarrollo intelectual y académico en temas de seguridad de redes y telecomunicaciones.

El honeynet es una herramienta de seguridad de la información de una organización, la cual permite ver como los atacantes ingresan a la red y que es lo que pueden realizar, y generar conocimiento de los riesgos a los que están expuestos la información en las instituciones.

Para el desarrollo de este tema, se vio la necesidad de trabajar en herramientas de seguridad, temas de virtualización, trabajar con plataformas Linux y Windows, análisis de tráfico, herramientas de red, estudio de vulnerabilidades, los cuales aportaron para la culminación de este proyecto.

Durante la implementación del proyecto hubieron inconvenientes, como es la instalación de la herramienta, no existe asistencia que ayude a establecer porque se presentan los problemas que se presenta como la conFiguración del honeywall, ya que al estar virtualizado se necesita conFigurar los equipos para que puedan verse fuera de la red y se vio la necesidad de solicitar la ayuda de la empresa proveedora del servicio para que facilite la ayuda y el administrador de la red de la institución.

Los resultados obtenidos en la implementación de este herramienta de seguridad, es un aporte de investigación y seguridad en la institución en la que se implementó, donde se concluye que se ha realizado un ataque de denegación de servicio, lo que impide que se ejecute algunos servicios en la red, otro de los ataques que se realizaron es al puerto 22 y el escaneo de puertos que son los ataques que se ejecutaron durante la implementación del honeynet.

Otro aporte del proyecto es que los ataques vienen de Asia, cuya pregunta es que están buscando estas personas, que requieren o quiénes son estos atacantes del otro continente.

Gracias a esta información se puede tener una idea del nivel de exposición al que están los servicios de la institución y tener mucho más cuidado en la seguridad.

El tiempo de recolección fue corto, pero a pesar de esto se puede evidenciar que existen atacantes en busca de información, pero para realizar un análisis más profundo de los datos capturados se requiere de mayor tiempo de recolección y del conocimiento de herramientas para que ayuden a interpretar los datos del honeynet.

5.6 Recomendaciones generales de seguridad

Por la información detectada por el honeynet virtual implementada, la misma que advierte sobre los ataques que intentan ingresar a la red, se detalla a continuación algunos detalles que ayudarán a disminuir estos intentos de ataques o establecer políticas de seguridad en la red.

- Se debe programar análisis periódico, una vez a la semana revisión de los sistemas y actualización de firmas ante nuevas amenazas y vulnerabilidades.
- Actualizar el sistema operativo y el software de los equipos, ya que los ataques que se presentan son programas que se ingresan al equipo y este se propaga tomando las vulnerabilidades presentes.
- Se debería restringir el acceso a páginas a los usuarios de la institución.
- Informar a los usuarios sobre las tendencias de ataques que se están presentando en la actualidad.

5.7 Medidas de Respuesta

Se detalla algunas medidas de prevención a los ataques sucedidos en la investigación.

- **Escaneo de Puertos**

Se ejecutó el ataque de escaneo de puertos, con el objetivo de iniciar como está la red, si existen vulnerabilidades a las que se puede atacar.

Medidas

1. Abrir los puertos necesarios y cerrar los que no se usa
2. Un atacante buscará escanear probablemente con un robot y por fuerza bruta, por lo que se debe abrir los puertos que realmente se van a usar, ya que muchas veces los administradores olvidan cerrar los puertos que no se usan.
3. Utiliza puertos que no sean un estándar
4. Cuando un atacante recoge información de un sistema, intentará seguramente hacerlo por puertos estándar es decir: el 1521 para Oracle, o el 22 que es SSH. Por lo que sería utilizar puertos no estándares para dificultar al atacante.
5. roteger el acceso a aquello que deba ser restringido y a sus conexiones.
6. Si se necesita ofrecer un servicio a algún usuario o empresa, pero es un servicio susceptible de ser atacado, debe ser protegido con sistemas de autentificación adecuados, o utilizar conexiones seguras como el https.
7. Usar métodos preventivos: Cortafuegos e IDS
8. Cuando se tiene un servicio público, se debe utilizar tener sistemas preventivos que reaccionen de forma inteligente a los ataques. Es en este punto donde los IDS y los firewalls actúan. El uso del firewall es necesario que se lo puede hacer con hardware o software. (García, 2010)

- **Ataques de Fuerza Bruta**

Se pudo realizar ataques de fuerza bruta, buscando claves en el servicio SSH y en la base de datos MySql, por lo que se detalla medidas de prevención.

Medidas

1. No permitir el login remoto del usuario root
2. Esta medida evitará que en caso de una agresión con resultado favorable para el atacante, puedan acceder al servidor con permisos absolutos es decir, como súper usuario.
3. Limitar la cantidad de intentos de logueo fallidos, en este caso, se indica que el máximo número de veces que se pueden equivocar al intentar loguearnos, es de tres. Esta directiva cerrará la conexión.
4. Limitar la cantidad de conexiones simultáneas, indica que no puede haber más de dos conexiones simultáneas desde una misma IP.
5. Limitar la cantidad máxima de tiempo durante la cual se mostrará la pantalla de logueo
6. Limitar el acceso SSH a un usuario determinado

7. Si solo se habilita el acceso por SSH a un usuario, los intentos del agresor por ingresar al servidor, serán prácticamente imposibles, siempre y cuando éste, desconozca por completo el nombre del usuario que cuenta con dicho permiso.
8. Cambiar el puerto por defecto
9. Una medida menos efectiva pero algo astuta, es modificar el puerto por el cual se accede mediante el protocolo SSH. Por defecto, este puerto es el 22, aunque cambiar este puerto no garantiza absolutamente nada, simplemente retrasará unos pocos minutos el ataque.
10. La alternativa más segura: no permitir el acceso mediante contraseña, existe una alternativa para iniciar sesión por SSH, mediante la cual, en vez de utilizar una contraseña, el servidor verifica tu identidad de la misma forma que tu verificas la suya: a través de una huella digital única.

    Esta técnica, consiste en generar una clave RSA en el ordenador desde el cual se le permitirá el acceso a un determinado usuario y luego, enviar una copia de la clave pública generada al servidor.

11. Bloquear las IP tras varios intentos fallidos
12. Se puede instalar una herramienta que se encargue de detectar los intentos de acceso fallidos (verificando los logs de autenticación) y automáticamente, cree reglas que bloqueen la ip. (Bahit)

- **Ataques de denegación de servicios**

Al igual que los ataques anteriores se describe algunas medidas que se deben tomar en cuenta para disminuir estos ataques:

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). (Caitoira, 2012)

CAPITULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

En el desarrollo de este proyecto se mencionan algunas conclusiones que se detalla

1. Durante este proceso se desarrollo una honeynet virtual, que se implementaron de acuerdo a los recursos que se presentaron en la institución, los mismos que fueron mínimos para el desarrollo del proyecto.

2. Durante la implementación de este honeynet virtual, se ejecutó sobre plataforma de virtualización, lo que ayudó a tener un mayor conocimiento de cómo funcionan las máquinas virtuales, su conFiguración y memoria que se requiere.

3. Es necesario tener ejecutando este sistema por un periodo aproximado de 8 horas, a fin de estudiar más a fondo los ataques a una red, sin embargo se debe tener especial cuidado en su sistema en producción, ya que este sistema podría volverse en contra de la institución.

4. Se puede crear una red pequeña a través de máquinas virtuales, facilitando que se utilicen pocos equipos (hardware) y conexiones en uno solo computador.

5. En la recolección y análisis de datos existía gran cantidad de tráfico, y para poder entender estos datos se aprendió el uso de herramientas como wireshark y networkMiner.

6. A través de este proyecto se pudo ver como el honeynet tiene la capacidad de capturar intrusos a la red y demostrar que es lo que están realizando.

7. La conFiguración del honeynet es complicada si no se tiene claro como está la estructura de la red, y depende de cómo se ubique en la red, en este caso al red se ubico fuera de la red de producción, solicitando una ip pública.

8. La honeynet virtual es fácil de trasladarla, de un lugar a otro ya que se ubica en una sola máquina, solo se requiere tener ip pública para su funcionamiento en otra área de la institución.

9. Es necesario monitorear y medir el tráfico de red para así establecer un patrón característico del uso de los recursos y así establecer la información que se necesita para poder garantizar el correcto funcionamiento del honeynet.

10. Se registraron ataques de denegación de servicios al puerto 80, esto ocasionó que el honeynet deje de funcionar ya que este tiene un límite de conexión lo que prohibió que sigan realizando conexiones, pero al querer ingresar desde otro equipo a la página de administración no se pudo.

11. El honeynet como un medio de investigación en la forma en que se realizan los ataques es una herramienta que se puede implementar para realizar dicho estudio.

12. Existe poca información sobre el funcionamiento del honeynet lo que dificultó la instalación del mismo.

13. A pesar que en la institución se tiene implementado un firewall y restricciones de acceso a páginas Web, existen amenazas que están tratando de ingresar a la red, por lo que se requiere mejorar su seguridad.

14. Con la implementación de este sistema de honeynet, se puede determinar que de acuerdo a la hipótesis establecida, si mejora la seguridad en la institución ya que permite detectar quien está atacando, que está realizando en la red honeynet y que medidas se puede tomar para contrarrestar estos ataques y atraer a los hackers a manipular información falsa ubicada en los honeyposts, desviándolos de la red en producción.

6.2 RECOMENDACIONES

- Se deben establecer políticas de seguridad a nivel de toda la institución en las que se definan las normas y responsabilidades de los usuarios, y conFiguración de equipos de seguridad, de manera que la información de la institución está protegida de ataques.

- A pesar de tener implementado un firewall se requiere la integración de un equipo de detección de intrusos, que permita juntar estas dos herramientas para una mejor protección del sistema de información.

- Se deben colocar un honeynet en cada una de las organizaciones que forman parte de la institución militar, ya que esta se implemento solo en la parte central del Ministerio.

- Es necesario que los administradores mejoren las seguridades en cuando al manejo de claves en la institución.

- Realizar un seguimiento continuo del tráfico de la red, y que se mejore en el análisis de los datos recolectados para poder tomar las medidas necesarias frente a los ataques que se presentan, por lo que se requiere que se conozca las herramientas que ayudan a interpretar la información.

- Se debe documentar la información que se obtiene del honeynet, para realizar un análisis de cómo se comporta el atacante.

- Como se diseñó una honeynet autocontenida virtual, se debe obtener copias de los maquinas virtuales implementadas en el caso de que se colapsen o sufran algún desperfecto, y poder recuperarlas.

- Debido a que el proyecto es virtual, se requiere como hardware un equipo con mayor memoria y capacidad de disco, para que no se colapse o se ponga lento el sistema de honeynet.

Bibliografía

Acosta, Pablo. Pablin. [En línea] [Citado el: 17 de 11 de 2013.] http://www.pablin.com.a.

Almeida, Xavier. 2011. El Hoy. [En línea] 01 de 01 de 2011. [Citado el: 16 de 05 de 2013.] http://www.hoy.com.ec.

Bahit, Eugenia. eugeniabahit. [En línea] [Citado el: 29 de 11 de 2013 .] http://library.originalhacker.org/.

Borghello, Cristian. 05. Seguridad de la Información. [En línea] 2013 de 05 de 05. [Citado el: 05 de 05 de 2013.] http://www.segu-info.com.ar.

Caitoira, Fernando. 2012. Welivesecurity. [En línea] 28 de 03 de 2012. [Citado el: 29 de 11 de 2013.] http://www.welivesecurity.com/.

Center, Microsoft System. 2011. System Center. [En línea] 01 de 04 de 2011. [Citado el: 25 de 05 de 2013.] http://technet.microsoft.com.

Comercio. 2012. El Comercio. [En línea] 10 de 08 de 2012. [Citado el: 05 de 05 de 2013.] http://www.elcomercio.com.ec.

Consortium, Web Application Security. 2004. Web Application Security Consortium . [En línea] 01 de 01 de 2004. [Citado el: 21 de 09 de 2013.] www.webappsec.org.

Datakeeper. 2011. Datakeeper. [En línea] 23 de 12 de 2011. [Citado el: 15 de 05 de 2013.] http://www.datakeeper.es/?p=716.

Druke, Pete. 1994. *Sociedad Postcapitalista.* s.l. : Harpecollins, 1994.

Emprendedores, Centro de Apoyo Tecnológico a. 2011. Gestores de máquinas virtuales. [En línea] 01 de 01 de 2011. [Citado el: 23 de 09 de 2013.] http://www.bilib.es.

Eric, Maiwald. 2005. *Fundamentos de Seguridad de Redes.* México : McGraw-Hill, 2005.

Esxi, VMware. 2009. Redes Privadas. [En línea] 01 de 01 de 2009. [Citado el: 29 de 09 de 2013.] http://redes-privadas-virtuales.blogspot.com.

FOUNDATION, OWAS. OWASP. [En línea] [Citado el: 21 de 09 de 2013.] https://www.owasp.org.

Gallo, Mayra y Liveya, Zoraya. 2012. *Proyecto previo a la obtención del título de Ingeniero en sistemas e informática.* Quito : s.n., 01 de 09 de 2012.

Garcia, Alejandro. 1986. ECURED. [En línea] 05 de 05 de 1986. [Citado el: 05 de 05 de 2013.] http://www.ecured.cu/.

García, Alejandro. 05García Alejandro. Presente y futuro de los IDS. Universidad Politécnica de Madrid. ECURED. [En línea] 2013 de 05 de 05García Alejandro. Presente y futuro de los IDS. Universidad Politécnica de Madrid. [Citado el: 2013 de 05 de 05.] http://www.ecured.cu/.

García, David. 2010. Redes Zone. [En línea] 24 de 10 de 2010. [Citado el: 29 de 11 de 2013.] http://www.redeszone.net.

Hernández, Miguel y Lema, Carlos. [En línea] [Citado el: 23 de 09 de 2013.] http://intranet.uat.edu.mx.

Introducción Seguridades de la Información. **Fuertes, Walter. 2009.** 2009, Escuela Politécnica del Ejército, págs. 40-42.

Mifsud-k, Elvira. 2012. [En línea] 01 de 01 de 2012. [Citado el: 25 de 09 de 2013.] http://recursostic.educacion.es.

OWASP. 2008. OWASP FOUNDATION. [En línea] 01 de 01 de 2008. [Citado el: 21 de 09 de 2013.] https://www.owasp.org.

Pillateum. Plataformas virtuales. [En línea] [Citado el: 25 de 05 de 2013.] http://www.pillateunlinux.com.

Portal, Security. 2006. SEINIT. [En línea] 01 de 01 de 2006. [Citado el: 21 de 05 de 2013.] http://www.isoc.org.

Rios, Julio. 2013. Seguridad Informática. [En línea] 05 de 05 de 2013. [Citado el: 05 de 05 de 2013.] //www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml.

Torres, Diego y Zambrano, Paúl. 2012. Escuela Politécnica del Chimborazo. *Escuela Politécnica del Chimborazo.* [En línea] 01 de 01 de 2012. [Citado el: 05 de 05 de 2013.] http://dspace.espoch.edu.ec/handle/123456789/1495.

Villar, Eugernio y Gómez, Julio. Adminso. [En línea] [Citado el: 23 de 09 de 2013.] http://www.adminso.es/images/a/a2/Eugenio_cap2.pdf..

Vinueza, Tatiana. 2012. Escuela Politécnica Nacional. [En línea] 01 de 01 de 2012. [Citado el: 23 de 09 de 2013.] http://repositorio.utn.edu.ec.

WMware.com. Historia de la virtualización. [En línea] [Citado el: 23 de 09 de 2013.] http://www.VMware.com/mx/virtualization/virtualization-basics/history.htm.

Workstation, VMware. VMware Workstation. [En línea] [Citado el: 25 de 05 de 2013.] http://www.intercambiosvirtuales.org.