UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

IMPLEMENTACIÓN DE HONEYPOT PARA LA CORRECCIÓN DE VULNERABILIDADES EN LA RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE HUAMBOS

PARA OPTAR EL TITULO PROFESIONAL DE

INGENIERO DE SISTEMAS

Autor:

Bach. ADRIAN NARCISO HARLYN MAYANGA

BELLODAS

Línea de Investigación:

Tecnología de la Información

Pimentel – Perú
2018

IMPLEMENTACIÓN DE HONEYPOT PARA LA CORRECCIÓN DE VULNERABILIDADES EN LA RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE HUAMBOS

APROBACIÓN DE LA TESIS

_____

Bach. ADRIAN NARCISO HARLYN MAYANGA BELLODAS

Autor

_____

Mg. Ing. Juan Villegas Cubas

Presidente de Jurado

_____

Ing. Mejia Cabrera Heber Ivan

Secretario(a) de Jurado

_____

Mg. Ing. Bances Saavedra David Enrique

Vocal/Asesor de Jurado

DEDICATORIA

Esta tesis se la dedico a mi Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mi familia quienes por ellos soy lo que soy. Para mis padres Orestes y Anita por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

A mis hermanas Kattya, Leidy e Isabel por estar siempre presentes, acompañándome para poderme realizar. A mis sobrinos Andy Fabián, Anita Soledad, Jesús Mateo y Ariana Stephany quien ha sido y es una mi motivación, inspiración y felicidad.

AGRADECIMIENTO

El presente trabajo de tesis primeramente me gustaría agradecerte a Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño anhelado.

A la Universidad Señor de Sipan por darme la oportunidad de estudiar y ser un profesional.

De igual manera agradecer a mi profesor de Investigación y de Tesis de Grado al Ing. Heber Ivan Mejilla Cabrera, por su visión crítica de muchos aspectos cotidianos de la vida, por su rectitud en su profesión como docente, por sus consejos, que ayudan a formarte como persona e investigador.

ÍNDICE

CAPÍTULO I PROBLEMA DE INVESTIGACIÓN 13

1.1. Situación Problemática 14
1.2. Formulación del Problema 16
1.3. Delimitación de la Investigación 16
1.4. Justificación e Importancia de la Investigación 16
1.5. Limitaciones de la Investigación 17
1.6. Objetivos de la Investigación 17
Objetivo general 17
Objetivos específicos 18

CAPÍTULO II MARCO TEORICO 19

2.1. Antecedentes de Estudios: 20
2.2. Estado del arte 26
2.3. Base teórica científicas 28
2.2.2.1. Técnicas Orientadas a la Seguridad Informática 28
2.2.2.2. Sistema de detección de intrusos (IDS) 30
2.2.2.3. Mecanismo de un IDS 30
2.2.2.4. Honeypot 31
2.2.2.5. Honeypot en la red 32
2.2.2.6. Honeynet 33
2.2.2.7. Riegos e inseguridades informáticas más comunes 35
2.2.2.8. Tipos de Honeypot 36
2.2.2.8.1. Specter 38
2.2.2.8.2. Honeyd 39
2.2.2.8.3. KFSensor 39
2.2.2.8.4. PatrioBox 39
2.2.2.8.5. HoneyNet 41
2.2.2.8.6. ManTrap 42
2.2.2.8.7. HoneyWall 42
2.2.2.8.8. Procedimiento de captura y análisis 43
2.2.2.8.9. Información recolectada 43

2.4. FASES EN LA PENETRACIÓN DE UN SISTEMA 44
2.4.1. FOOTPRINTING 44
2.4.2. SCANNING 45
2.5. IDENTIFICACIÓN DE VULNERABILIDADES 45
2.6. PENETRACIÓN AL SISTEMA 46
2.7. BORRADO DE HUELLAS 47
2.8. Definición de la terminología 47
CAPÍTULO III: MARCO METODOLÓGICO 51
3.1. Tipo y Diseño de Investigación 52
3.2. Población y Muestra 52
3.3. Hipótesis 53
3.4. Operacionalización: 53
3.5. Métodos, técnicas e instrumentos de recolección de datos 54
3.5.1. Método de la medición: 55
3.6. Procedimiento para la recolección de datos 56
3.7. Análisis Estadístico e Interpretación de los datos 57
3.8. Criterios éticos 58
3.8.1. Principio de Beneficencia 58
3.8.2. Principio de respeto a la Dignidad Humana 58
3.8.3. Principio de Justicia 58
3.9. Criterios de rigor científico 59
CAPÍTULO IV: SELECCIÓN DE ATAQUES TÍPICOS EN UNA RED DE DATOS DE UNA MUNICIPALIDAD 60
4.4.2 ATAQUES ACTIVOS 64
4.7 Diagnóstico de la Situación Actual 70
4.7.1 FOOTPRINTING 70
4.7.2 SCANNING 73
4.8 IDENTIFICACIÓN DE VULNERABILIDADES 80
4.9 PENETRACIÓN AL SISTEMA 85
4.9.1 BORRADO DE HUELLAS 91
4.10 Resultados en tablas y gráficos 91
CAPÍTULO V: PROPUESTA DE INVESTIGACION 95

5.1 Requerimientos de la solución 96
5.2 Estudio de las arquitecturas y selección de la más apropiada 97
5.3 Análisis de las herramientas 100
5.3.1. Herramientas de Captura de la Honeynet 101
5.3.2 Sebek 102
5.4 IMPLEMENTACIÓN DE LAS HONEYNETS EN LAS REDES DE DATOS DE LA MUNICIPALIDAD DE HUAMBOS 104
5.4.1. Implementación de la Honeynet –MUNIHUAMBOS....104
5.5 Configuración de la red 105
5.6 Instalación y configuración del Honeywall 110
5.7 Instalación y configuración del CD-ROM Honeywall en la máquina virtual 111
5.7.2 Walleye....126
CAPÍTULO VI 128

EVALUACIÓN DE RESULTADOS 128

6.1 PRUEBAS A TRAVÉS DE ATAQUES INFORMÁTICOS SIMULADOS 129
6.2 VERIFICACIÓN DEL DISEÑO....134
6.3 TRAFICO GENERADO EN EL HONEYWALL 143
CAPÍTULO VII GUÍA METODOLÓGICA 148

7.1 DESCRIPCIÓN DE LA GUÍA....149
7.2 ANÁLISIS DE LA INFRAESTRUCTURA EXISTENTE 149
7.3 DISEÑO DE LA HONEYNET 150
7.3.1 Honeynet de Primera Generación: 150
7.3.2 Honeynet de Segunda Generación 151
7.4 IMPLEMENTACIÓN DE LA HONEYNET....152
7.5 VERIFICACIÓN DEL DISEÑO....156
VIII. CONCLUSIONES Y RECOMENDACIONES 161

8.1 CONCLUSIONES 162
8.2 RECOMENDACIONES 164
REFERENCIAS....166
ANEXO A1....169
Anexo A2 178
Anexo A3 186

ANEXO A4.....194
GUIA DE CORRECCIONES DE LAS VULNERABILIDADES 194

ÍNDICE FIGURAS

Figura 1: *Fuente: CÓCARO, Fernando y GARCÍA, Mauricio y ROUILLER, María José. Estado del Arte. [DVD]. 2.0. Montevideo. 21 de Enero de 2008.... 27*

Figura 2: *Honeypot diagrama general..... 32*

Figura 3: *Honeypot como equipo físico en la red..... 33*

Figura 4: *Diagrama Honeynet..... 34*

Figura 5: *Modelo evaluación de riesgos Fuente: https://seguridadinformaticaufps.wikispaces.com/file/view/8.JPG/329075810/531x342/8.JPG..... 36*

Figura 6: *Honeypot de Baja Interacción..... 38*

Figura 7: *Honeypot de Alta Interacción..... 41*

Figura 8: *Estructura de Honeywall..... 42*

Figura 9: *Análisis del atacante en la red (Kali Linux)..... 43*

Figura 10: *Población..... 53*

Figura 11: *Modelo de ataque pasivo..... 63*

Figura 12: *Ataque activo de modificación..... 65*

Figura 13: *Cambio de mac adrress..... 70*

Figura 14: *Verificación de los servidores DNS..... 71*

Figura 15: Prueba *de Traceroute..... 71*

Figura 16: *Prueba de ICMP a los host de la MDH..... 72*

Figura 17: *Búsquedas en el DNS..... 72*

Figura 18: *Hosts en la red de la MDH..... 73*

Figura 19: *Login en Nessus..... 80*

Figura 20: *Selección de Hosts y Plugins en Nessus..... 81*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 21: *Iniciar el escaneo en Nessus* 81

Figura 22: *Análisis de vulnerabilidades en curso* 82

Figura 23: *Análisis de vulnerabilidades completo* 82

Figura 24: *Análisis de vulnerabilidades en la red de la MDH* 83

Figura 25: *Informe ejecutivo de vulnerabilidades* 84

Figura 26: *Configuración del exploit ms08_067_netapi* 85

Figura 27: *Explotando la vulnerabilidad ms08_067_netapi* 86

Figura 28: *Listado de procesos e información del host comprometido* 87

Figura 29: *Inyectando el script screenshot* 88

Figura 30: *Pantalla capturada remotamente* 88

Figura 31: *Inyectando el script run VNC* 89

Figura 32: *Acceso VNC a la victima* 89

Figura 33: *Inyectando el script run multicommand –cl "msg * ERROR DEL SISTEMA"* 90

Figura 34: *Envío de mensaje vía consola* 90

Figura 35: *Escaneo de Vulnerabilidades* 92

Figura 36: *Ataques realizados a un computador* 92

Figura 37: *Veces de ingreso* 93

Figura 38: *Veces de ingreso* 94

Figura 39: *Honeynet Virtual auto-contenida* 100

Figura 40: *Honeynet virtual auto-contenida en la red MUNIHUAMBOS* 104

Figura 41: *Diagrama lógico de Honeynet virtual auto-contenida* 106

Figura 42: *adaptador eth0* 107

Figura 43: *Adaptador eth1* 108

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 44: *adaptador eth2* 108

Figura 45: *Diagrama lógico de Honeynet virtual auto - contenida* 110

Figura 46: *Menú del Honeywall* 124

Figura 47: *Opciones de Estatus* 124

Figura 48: *Opciones de Administrador del Honeywall* 125

Figura 49: *Opciones de Configuración del Honeywall* 125

Figura 50: *Ingreso del Honeywall web* 126

Figura 51: *Cambio de contraseña del Honeywall* 127

Figura 52: *Interface admin del Honeywall* 127

Figura 53: *Escaneo de la Red* 129

Figura 54: *Verificación de puertos y servicios* 130

Figura 55: *Verificación de conexiones* 131

Figura 56: *Patrón de NMAP identificado* 131

Figura 57: *Ejecución del exploit ms08_067_netapi* 132

Figura 58: *Seguimiento del paquete con Honeywall* 132

Figura 59: *Visor detallado del paquete con Honeywall* 133

Figura 60: *Captura del paquete con código malicioso* 133

Figura 61: *Regla de Snort para la vulnerabilidad ms08_067_netapi* 134

Figura 62: *Fecha en el Honeywall* 135

Figura 63: *Fecha en el Honeypot* 135

Figura 64: *Ping hacia los Honeypots* 136

Figura 65: *Ping desde los Honeypots* 137

Figura 66: *Verificación del DNS* 138

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 67: *Prueba de registro de tráfico* *139*

Figura 68: *Dirección IP de interfaz de administración* *140*

Figura 69: *Ingreso a la Administración web* *140*

Figura 70: *Tráfico capturado por Honeywall* *141*

Figura 71: *Recepción de datos a través de Sebek* *142*

Figura 72: *Tráfico Generado*..... *143*

Figura 73: *Mejora de la Red con la implementación del Honeypot*..... *145*

Figura 74: *Total de ataques registrados* *146*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE FIGURAS ANEXO A1

Figura A1 1: *Creación de máquina virtual 170*

Figura A1 2: *Inicio de la instalación del Honeywall 170*

Figura A1 3: *Fase de instalación del Honeywall 171*

Figura A1 4: *Inicio de sesión del Honeywall 171*

Figura A1 5: *Selección del tipo de configuración 172*

Figura A1 6: *Ingreso de la dirección IP del Honeypot 172*

Figura A1 7: *Iniciar la configuración de SSH 173*

Figura A1 8: *Ingreso de los puertos TCP que permiten la salida 173*

Figura A1 9: *Ingreso de los puertos UDP que permitan la salida..... 174*

Figura A1 10: *Activar el snor-inline para evitar el tráfico malicioso a la red. .. 174*

Figura A1 11: *Nombre del archivo que contiene la ubicación de las direcciones IPs que generan SPAM (Blacklist). 175*

Figura A1 12: *Nombre del archivo que contiene la ubicación las direcciones IPs que nunca generan SPAM (WhiteList) 175*

Figura A1 13: *Configuración de las variables del Sebek 176*

Figura A1 14: *Ingreso de la dirección IP del Sebek..... 176*

Figura A1 15: *Ingreso del puerto del Sebek..... 177*

Figura A1 16: *Finalizamos y aceptamos para su reinicio del Honeywall 177*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE TABLAS

Tabla 1: *Componentes del sistema informático a analizar. 52*

Tabla 2: *Operacionalización 54*

Tabla 3: *Procedimiento para la recolección de datos..... 56*

Tabla 4: *Selección de ataques tipos a la MDH 69*

Tabla 5: *Descripción de los ataques realizados a un computador 93*

Tabla 6: *componentes del Honeywall. 102*

Tabla 7: *Sistemas operativos 105*

Tabla 8: *Configuración de Honeypot 109*

Tabla 9: *Configuración de Honeypot 109*

Tabla 10: *Trafico SSH 144*

Tabla 11: *Trafico ICMP.....144*

Tabla 12: *Trafico HTTP 144*

Tabla 13: *Trafico DNS 144*

Tabla 14: *Trafico NETBIOS 145*

Tabla 15: *Registro de incidencias.....147*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE TABLAS ANEXOS A2

Tabla A2 - 1: *Computador 01..... 178*

Tabla A2 - 2: *Computador 02..... 178*

Tabla A2 - 3: *Computador 03..... 179*

Tabla A2 - 4: *Computador 04..... 179*

Tabla A2 - 5: *Computador 05..... 180*

Tabla A2 - 6: *Computador 06..... 180*

Tabla A2 - 7: *Computador 07..... 181*

Tabla A2 - 8: *Computador 08..... 181*

Tabla A2 - 9: *Computador 09..... 182*

Tabla A2 - 10: *Computador 10..... 182*

Tabla A2 - 11: *Computador 11..... 183*

Tabla A2 - 12: *Computador 12..... 183*

Tabla A2 - 13: *Computador 13..... 184*

Tabla A2 - 14: *Computador 14..... 184*

Tabla A2 - 15: *Computador 15..... 185*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE TABLAS ANEXOS A3

Tabla A3 - 1: *Computador 01..... 186*

Tabla A3 - 2: *Computador 02..... 186*

Tabla A3 - 3: *Computador 03..... 187*

Tabla A3 - 4: *Computador 04..... 187*

Tabla A3 - 5: *Computador 05..... 188*

Tabla A3 - 6: *Computador 06..... 188*

Tabla A3 - 7: *Computador 07..... 189*

Tabla A3 - 8: *Computador 08..... 189*

Tabla A3 - 9: *Computador 09..... 190*

Tabla A3 - 10: *Computador 10..... 190*

Tabla A3 - 11: *Computador 11..... 191*

Tabla A3 - 12: *Computador 12..... 191*

Tabla A3 - 13: *Computador 13..... 192*

Tabla A3 - 14: *Computador 14..... 192*

Tabla A3 - 15: *Computador 15..... 193*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Resumen

En la presente investigación identificaremos las posibles vulnerabilidades e inseguridades existentes en las redes de datos y sistemas informáticos en la Municipalidad Distrital de Huambos, Oficina del SIAF. Que al usar la tecnología Honeypot, herramienta que simula servicios y aplicaciones vulnerables en una red trampa llamada Honeynet, a este tipo de tecnologías se les llama como Sistemas de Detección de Intrusos (IDS), utilizados para monitorear los eventos que sucede en un sistema que analiza intentos de intrusión en la red local; todo el tráfico en la red analizado nos permitirá evaluar e incrementar reglas de seguridad informática entre los usuarios internos y externos de la red. Además, en este trabajo se observó la comparativa de los resultados de la situación actual y la situación con la implementación del sistema Honeypot como actividades de un hacker o atacante accediendo a la red, a partir de estas alarmas el administrador del sistema puede tomar medidas preventivas.

Palabras Clave: Honeypot, honeynet, vulnerabilidades, MDH, SIAF, ciberataques, seguridad informática.

Abstract

The present investigation, identify the possible vulnerabilities and present insecurities existing in the data networks and information systems of the Municipality District of Huambos, of the office SIAF. By using Honeypot, a tool that simulates services and vulnerable applications in a network trap called Honeynet, this type of technologies they are known as Intrusion Detection System (IDS) used to monitor the events occurring in a system for intrusion attempts in the network data; all traffic on the analyzed network, allows us to evaluate security rules between internal and external users of the data network. In addition, in this paper we observed the comparison of the results of Honeypot system as activities of a hacker or attacker accessing the network from these alarms the system administrator can take preventive measures.

Key Words: Honeynet, Honeypot, Computer Security, Vulnerabilities, MDH, SIAF, cyberattacks.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Introducción

Actualmente vivimos prácticamente conectados a una red de internet la mayoría del día, los ataques informáticos y las intromisiones han aumentado considerablemente. Este suceso viene de la mano de una clara evolución de las herramientas que utilizan los delincuentes informáticos. Los usuarios avanzados vienen desarrollando aplicaciones diariamente con el propósito de vulnerar alguna red o probar la deficiencia de un sistema, y usan estas deficiencias para poder introducirse en otros sistemas.

Un Honeypot nace de varios estudios en el área de Seguridad Informática, para poder analizarlo se simula un ambiente de red de datos controlados con la finalidad de distraer al intruso del sistema anfitrión real y al mismo tiempo obtener información del mismo analizando las técnicas y métodos utilizados para acceder a un recurso o servicio de la red de datos.

La información que existe en una red de datos puede ser alterada por expertos en el área de redes, pero al mismo tiempo existen atacantes que utilizan dicha información para su conveniencia, un usuario en una computadora dentro de una red de datos puede ingresar a un sistema a través de Internet o localmente, el intruso puede usar un software que permita capturar tramas de la red y así robar información importante. La seguridad informática, eje fundamental en la protección de información, examina las vulnerabilidades que puedan existir en su red de datos o estaciones de trabajo.

El informe final del presente trabajo de investigación se orienta a la seguridad informática de la Municipalidad Distrital de HUAMBOS, dividido en capítulos, que proporcionan una mejor comprensión del contenido del mismo. Toda la

investigación se basa en una fuente bibliográfica de la cual se ha recolectado la información necesaria, como también los anexos de las configuraciones adicionales y resultados obtenidos en el proyecto de investigación.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO I
PROBLEMA DE INVESTIGACIÓN

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

1.1. Situación Problemática

La Municipalidad Distrital de Huambos cuenta con una red de datos de comunicación que tiene diferentes servicios al ciudadano en general. Todo esto incluido en el uso de la red inalámbrica o física, tomando en cuenta los dispositivos de conexión a la red local e Internet, el implementar una política de seguridad condicional en el uso de la red puede ser un problema.

Hoy en día, existe una mayor facilidad para el acceso a la red, lo que ha contribuido a la evolución de técnicas de ataques existentes y ha generado cambios en los escenarios típicos que causan amenazas para cualquier sistema que brinde servicios a través de Internet, por ejemplo, la Municipalidad de Huambos, cuenta con seguridad informática de cuatro sistemas como; Oficinas de Contabilidad, Tesorería, Rentas y Registro Civil, las cuales están vulnerados directamente usando equipos del mismo departamento, sin saber que la portátil de un de un usuario puede ser el causante de un delito informático.

Contar con información detallada de los movimientos de los intrusos que ingresan a sus redes es crucial, ya que ayuda a poder tomar medidas preventivas sobre los ataques, además se pueden actualizar las políticas de seguridad para poder evitar ataques similares. También proporcionaría información detallada sobre las vulnerabilidades del sistema que no han sido afectadas. Se busca algo simple y que funcione en diversas plataformas, si el sistema es

dañado es un servicio significativo y no debe ser deshabilitado, por ejemplo, un Servidor de Base de Datos

El objetivo de las Honeynet es, al igual que el Honeypot, analizar el uso de las técnicas y herramientas que usan los atacantes en Internet. Se diferencia de un Honeypot ya que no supone una sola máquina, sino varios sistemas y aplicaciones que emulan otras, copian vulnerabilidades o servicios o crean entornos “jaula” desde donde se puede observar y analizar los ataques. Los requerimientos básicos e indispensables para elaborar una Honeynet son: Data Control (control de datos) y Data Capture (captura de datos).

A nivel Institucional: Actualmente la Municipalidad Distrital de Huambos, no cuenta con un sistema de seguridad informático que proteja su información, por lo que está expuesto a continuos ataques sin que el administrador pueda informarse de estos delitos informáticos.

Los Delitos Informáticos más comunes que existen son:

Falsificación de información.

Por ejemplo, un usuario ajeno al sistema puede violar un sistema y lograr acceder al **SIAF** (SISTEMA INTEGRADO DE ADMINISTRACIÓN FINANCIERA DEL ESTADO), que al guardar data se puede restaurar en otro computador y se puede; modificar presupuesto, y conseguir aumentar los pagos, anular pagos, alterar datos mediante Visual Fox Pro y otros.

Ataques de denegación del servicio (DDoS).

Ataques a Servidores por conexiones ajenas, con el fin de evitar que se pueda investigar el origen de los ataques.

1.2. Formulación del Problema

¿Con la implementación de honeypot se detectarán las vulnerabilidades en la red de datos de la Municipalidad Distrital de Huambos?

1.3. Delimitación de la Investigación

La presente investigación se realizará en un periodo de tres meses, desde la fecha de aprobación de Universidad Señor de Sipan.

La presente investigación se realizará en la Municipalidad Distrital de Huambos (Tesorería, Presupuesto, Abastecimiento e Informática).

1.4. Justificación e Importancia de la Investigación

El tema por investigarse tiene gran importancia, debido a que con ello se podrá tener un mejor control sobre la seguridad informática de la Municipalidad, siendo esta la razón de mayor prioridad, ya que pretende facilitar y agilizar la administración de los sistemas informáticos y de las redes de datos. Además, se obtendrán recomendaciones de cómo evitar futuros delitos informáticos y así poder resguardar la Seguridad Informática de la Municipalidad.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Actualmente la Municipalidad Distrital de Huambos, se ha puesto como meta identificar las inseguridades que existen en las redes de datos y sistemas informáticos, teniendo como limitación principal las barreras de seguridades de nivel administrativo, pero no a nivel general, de acuerdo con las necesidades que tienen las oficinas, siento una vía de control crítico para la misma. La aplicación de Honeypots como una herramienta de investigación implica el diseño de una red Honeynet para ser comprometida por intrusos, además estudia las técnicas utilizadas por los atacantes que han conseguido acceder, consiguiendo así implementar alguna solución que permita neutralizar los problemas de seguridad informática en la Municipalidad Distrital de Huambos.

1.5. Limitaciones de la Investigación

Se tuvo limitaciones al momento de realizar pruebas en las áreas del SIAF, ya que en esas oficinas tienen mucho movimiento por motivos de pagos a los proveedores mediante el SIAF.

1.6. Objetivos de la Investigación

Objetivo general

Implementar Honeypot para la detección y corregir vulnerabilidades en la red de datos de la Municipalidad Distrital de Huambos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Objetivos específicos

a) Selección de ataques típicos en una red de datos de una Municipalidad.
b) Implementar un honeypot que permita mejorar la seguridad informática en la Municipalidad Distrital de Huambos.
c) Evaluar los resultados del honeypot en la red de datos de la Municipalidad Distrital de Huambos.
d) Realizar una guía de prevención para mejorar la seguridad de las vulnerabilidades encontradas en la red de datos de la Municipalidad Distrital de Huambos, a través de la tecnología Honeypot.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO II
MARCO TEORICO

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.1. Antecedentes de Estudios:

A nivel mundial Alfonso Antonio Berenguela Castro, Juan Pablo Cortes Collado, "Metodología de Medición de Vulnerabilidades en Redes de Datos de Organizaciones", 2006 "Segu.Info: Seguridad de la Informática", Disponible en: www.segu-info.com.ar/tesis/medicion-vulnerabilidades.zip

La presente tesis se concentra en crear una metodología mediante el diseño de guías, para poder medir la seguridad de redes de datos que ayuden al administrador a conocer la red y le brinde información necesaria para la creación de políticas de seguridad, analizando el costo/beneficios de la misma.

Esta investigación ayuda a nuestro trabajo, debido a que muestra diversas herramientas utilizadas al momento de medir las vulnerabilidades y los riesgos de las redes en las organizaciones, haciendo hincapié en los beneficios de su configuración al inicio, y la utilización de metodologías que permitan hacer retroalimentaciones.

A.S.S Borghello, Cristian Fabian, "Seguridad Informática: Sus Implicancias e Implementación", 2001, "Según Info: Seguridad de la Informática", Disponible en: www.segu-info.com.ar/tesis/tesis-borghello-full.zip

El principal objetivo de esta tesis es disminuir el número de ataques externos que logran evadir los mecanismos de seguridad y atentan los servicios que brindan mediante el control y el aislamiento del equipo comprometido.

La importancia del siguiente trabajo para nuestro proyecto es que ofrece mecanismos de seguridad como herramientas en software o hardware que buscan brindar un servicio de seguridad.

Cada uno posee una función determinada, la cual está en base al servicio de seguridad que desee brindar, por ejemplo, los servidores proxy, los cortafuegos, encriptación, sistemas de monitoreo, antivirus, Honeypots tiene como objetivo limitar los accesos al sistema o de este al exterior.

Luis Alberto Orellana Benavides, Rafael Cristóbal Hernández Vásquez, "Seguridad en Redes de Datos", 2003, Disponible en: http://rd.udb.edu.sv:8080/jspui/bitstream/123456789/265/1/033380_tesis.pdf

Esta tesis tiene como principal objetivo demostrar que la disponibilidad de la información y el crecimiento de las redes ha generada una debilitación y disminución de privacidad y seguridad de los datos, asimismo, se encuentra expuesta a transmitir información viral, creando inestabilidad, reducción del ancho de banda, hasta imposibilidad de transmisión de datos.

Es importante para nuestra investigación ya que describe diversos enfoques sobre seguridad a lo largo del tiempo, asimismo, brinda un esquema estándar para estas situaciones, los tipos de ataques más frecuentes y como configurarlas y algunos métodos de protección.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Eduardo Gallego, Jorge López de Vergara. Honeynets: Aprendiendo del atacante. [En línea]. [Fecha de consulta: 22 de Agosto 2013]. Disponible en: http://web.dit.upm.es/~jlopez/publicaciones/mundointernet04.pdf

En principal objetivo de esta tesis es elaborar una plataforma informática de experimentación, en ambiente Linux, que permita simular ataques a redes IP mediante la utilización de tecnologías de Virtualización con el propósito de efectuar mecanismos de seguridad para contrarrestarlo.

Este trabajo brinda, principalmente, un modelo de diseño para una topología de prueba con el objetivo de emular ataques reales a redes en ambiente Linux, usando escenarios de redes virtuales, además de herramientas para analizar la vulnerabilidad de una red, brindando un entorno más amigable desde la creación, instalación, configuración y administración de las máquinas virtuales.

Lance Spitzner, consultor y analista informático, experto en seguridad, a comienzos del año 2000 elaboró en su casa una red de seis ordenadores. Esta red fue diseñada par analizar el comportamiento y las formas de actuación de los atacantes. Spitzner fue uno de los primeros en adoptar esta idea y hoy en día es uno de los mayores expertos en honeypots y es precursor de proyecto Honeynet (www.honeynet.org) , que inició en 1999, además de escribir el libro "Honeypots: Tracking Hackers".

Este sistema estuvo de prueba por aproximadamente un año (abril 2000 – febrero 2001), almacenando toda la información que se generaba. En los resultados se pudo observar que en los momentos de mayor intensidad de ataques era a través del escaneo de los equipos de su casa desde el exterior, hasta 14 veces al día, y se utilizaban herramientas de ataque automatizadas.

Desde ese momento, se ha instaurado una comunidad de desarrolladores agrupados alrededor de honeynet.org, quienes ofrecen diferentes herramientas y consejos para poder utilizar las herramientas.

A nivel Nacional en la UNIVERSIDAD CESAR VALLEJO DE PIURA con el tema titulado "SERVIDOR SEÑUELO INFORMÁTICO HONEYNET HÍBRIDO Y SU INFLUENCIA EN LA SEGURIDAD INFORMÁTICA ACTIVA LÓGICA DEL CENTRO DE DIÁLISIS PIURA" se llegó a la conclusión de que en el área de tecnologías informáticas de la Diálisis Piura existen diversos mecanismos para proteger la información, el riesgo principal es la falta de conocimiento sobre estos, esto se debe a que diariamente aparecen nuevas herramientas que monitorean la red así como diversas amenazas.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

La principal característica de Honeypot es que es un sistema flexible, capaz de identificar los movimientos que tienen los atacantes y dos o tres comportamientos de la captura de las últimas vulnerabilidades que se propagan en línea a las redes de quipos para analizar. Los Honeypots se han estado utilizando por el Gobierno, las grandes empresas, organizaciones sin fines de lucro y escuelas. Estas entidades utilizan la tecnología honeypot para protegerse de los ataques para invadir el sistema seguro.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.2. Estado del arte

Las computadoras han tenido una expansión masiva en todos los ámbitos de la sociedad, además de la rápida evolución de las tecnologías de las comunicaciones, han sido las bases para el crecimiento de las redes de computadoras. Un ejemplo de ello es la red de computadores más grande: Internet.

Hoy en día, millones de personas alrededor del mundo usan Internet como parte de su trabajo o de ocio. La importancia que tiene la red de redes permite que exista conectividad global permanente entre actores en el mundo, de forma rápida y económica. Esto ha empujado a las empresas a aumentar la participación en este mundo y poder lograr un mayor alcance de estas en la sociedad.

Sin embargo, mientras se interconectan más equipos los incidentes de seguridad han ido aumentando, y ello pone en peligro la integridad de los sistemas y seguridad de la información. En la imagen 2.1 se puede observar un gráfico donde se puede ver que cada año los ataques se vuelven más sofisticados y debido a la accesibilidad de herramientas, los atacantes no precisamente deben contar con conocimientos avanzados para poder llevarlo a cabo.

A partir de los primeros incidentes reportados, las tecnologías de seguridad pretended boquear posibles ataques (firewalls) o detectarlos con anticipación para que no se infiltren e infecten la red (IDS's). Ambas tecnologías son críticas, pero presentan restricciones. Lo que sucede es que las herramientas que se usan generan mucha información, tienen tasas altas de falsos negativos y por

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ello no brindan los datos a tiempo para poder proteger los sistemas vulnerables y aminorar los efectos de las intrusiones.

¿Por qué no emplear una técnica milenaria, usada en las guerras?

“El arte de la guerra se basa en el engaño”, Sun Tzu. .

El uso adecuado del engaño puede brindar tiempo adicional, consiguiendo información para elaborar una buena defensa y prever el ataque. La idea principal es hacer funcionar una de las estrategias utilizadas con mayor frecuencia al largo de la historia, para defender las redes y los sistemas. Es decir, aprender de los ataques a diferentes sistemas en una organización para poder detectar las vulnerabilidades y los posibles problemas con la seguridad y poder aprender las técnicas utilizadas por los atacantes. Este objetivo se halla detrás de la tecnología de honeypots.

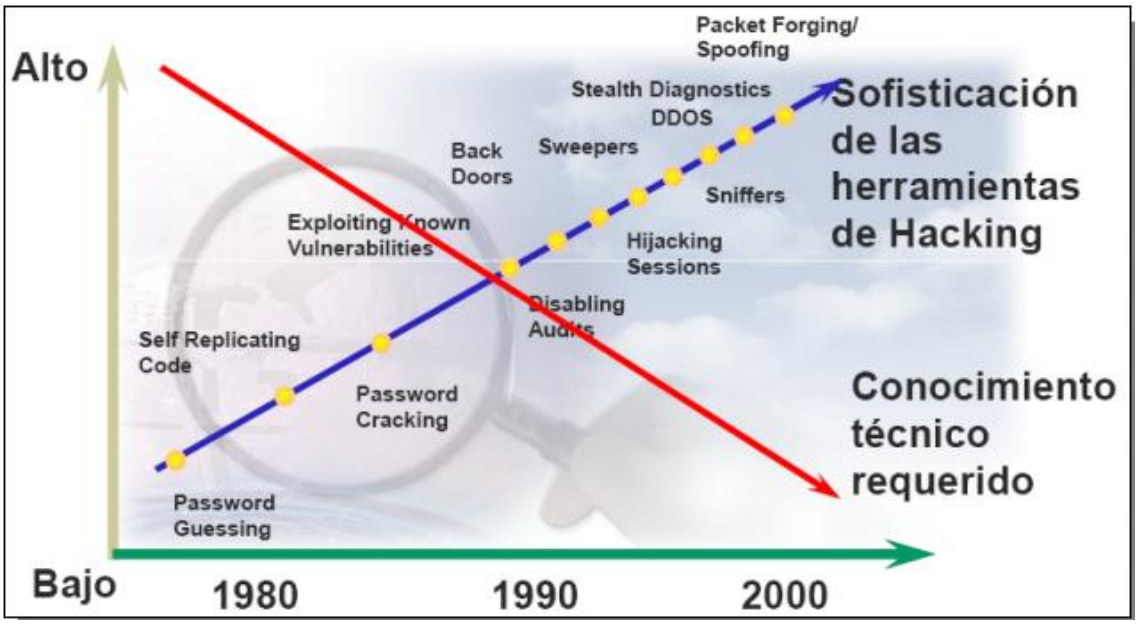


Figura 1: *Fuente: CÓCARO, Fernando y GARCÍA, Mauricio y ROUILLER, María José. Estado del Arte. [DVD]. 2.0. Montevideo. 21 de Enero de 2008*

2.3. Base teórica científicas

Se encontraron diversos aportes científicos en los siguientes libros:

Los aportes científicos que encontré de los siguientes libros son los siguientes:

C. Hoepers, Honeynets and Honeypots: Companion

Technology for Detection and Response, AusCERT2004 Conference, Technical Stream, Mayo 2004.

The Honeynet Project. Know your enemy: leaming about security threats. Segunda Edicion. Addison Wesley. Julio, 2004.

M. D. Katz, Redes y seguridad, Alfaomega Grupo Editor, pp. pp 1-100 2013.

2.2.2.1. Técnicas Orientadas a la Seguridad Informática

Sistemas de detección de intrusos: son sistemas que analizan las bitácoras de los sistemas de investigación de patrones de comportamiento o sucesos que puedan ser considerados susceptibles, en base a la información que fue sustentada anticipadamente. Pueden ser terminales de control.

Sistemas a conexión de red: estudian las conexiones pretenden establecer en una red o equipo en particular, capaces de realizar una acción sobre la base de métricas como: servicio solicitado, inicio y grado de la conexión, permisos, entre otros. Las gestiones pueden iniciar con el bloqueo de la conexión hasta la alerta al

administrador de la red. Dentro de esta categoría se pueden encontrar los cortafuegos (Firewalls) y los servicios de red (Wrappers).

Sistemas de análisis de vulnerabilidades: sistema que buscan vulnerabilidades acreditadas anticipadamente, se pueden usar por usuarios autorizados, así como por los que desean ingresar al sistema sin permiso.

Sistemas de protección a la integridad de información: sistemas que buscan aseverar que no existen variaciones negativas en la información, mediante criptografía y sumas de verificación. Algunos ejemplos de aplicaciones que crean algoritmos son Message Digest (MD5), o sistemas que manejan varios programas cifrados como Pretty Good Privacy (PGP), sistemas de protección a la privacidad Tripwire y DozeCrypt.

Sistemas de protección a la privacidad de la información: herramientas que usan criptografía para que su información pueda ser vista solo por personas autorizadas. Se utiliza principalmente en las comunicaciones entre dos identidades. Algunos ejemplos de este tipo de software son Pretty Good Privact (PGP), y los Certificados Digitales.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.2.2.2. Sistema de detección de intrusos (IDS)

El sistema de detección de intrusos se usa para encontrar intrusos o posibles intrusos en un entorno. Existen dos lugares posibles para poder poner en práctica este mecanismo:

Sistema de detección de intrusiones de red (NIDS)

Sistemas de detección de intrusiones en el host (HIDS)

2.2.2.3. Mecanismo de un IDS

Un IDS de red descubre patrones de ataque conocidos que se basan en una firma. Un IDS cuenta con dos habilidades importantes: una sirve para inspeccionar los paquetes en una trama de red y la segunda reconoce un patrón de ataque en un entorno específico. Ambas habilidades se centran en un motor rápido y robusto que detecta patrones complejos los más rápido posible. Se puede afirmar que un Honeypot es un IDS ya que es capaz de detectar a cualquier intruso o si existe alguna vulnerabilidad en las redes de datos o en el sistema informático.

2.2.2.4. Honeypot

La conceptualización de una Honeypot está basada en diversos estudios en el área de Seguridad de redes de las computadoras. La labor de los administradores de red reside en mantener todos los sistemas y servicios funcionales. Si los administradores analizaran periódicamente la red se podrían descubrir una gran cantidad de intrusos tratando de tener acceso al sistema o servicio, la detección de una vulnerabilidad en el sistema no siempre implica un fallo en este, los ciberataques y amenazas persistentes avanzadas necesitan de un nuevo enfoque de prevención y protección. Cuando se descubre un atacante en potencia, este permite tomar las medidas necesarias y oportunas para evitar que ingrese al sistema real o al servicio en ejecución. Cada uno de los sistemas trampa no se puede utilizar para fijar algún servicio, incluso peor, un Honeypot puede causar mayor interés en una red específica.

Un Honeypot es usado para ayudar a evitar riesgos y delitos informáticos dentro de una organización, y busca recaudar la mayor cantidad de información posible. Un Honeypot brinda niveles de seguridad para una organización, y puede ayudar a entender a la comunidad blackhat y los ataques, además de crear defensas contra las amenazas de seguridad informática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

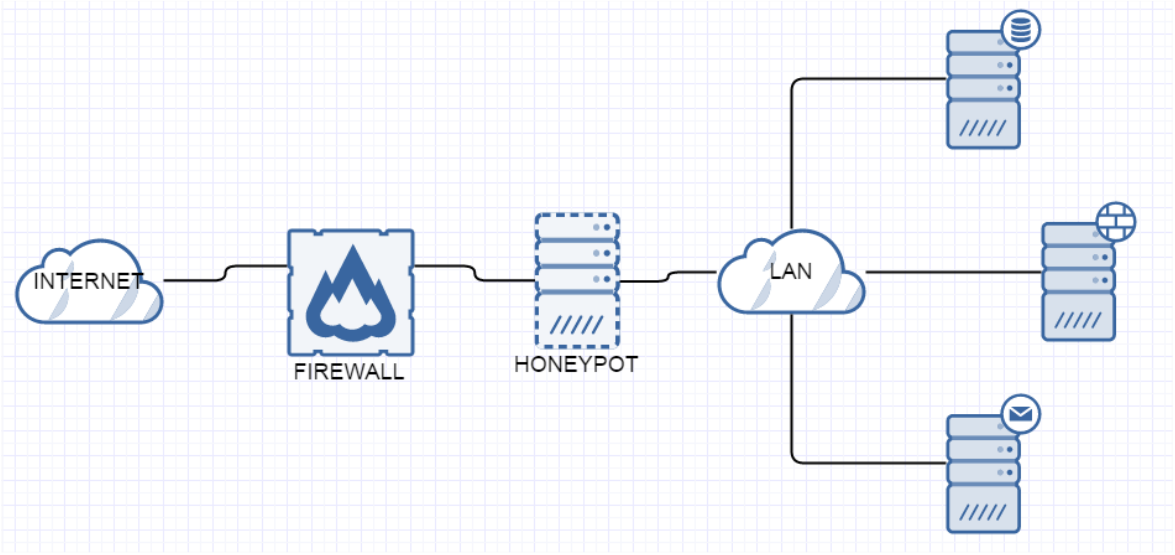


Figura 2: Honeypot diagrama general

2.2.2.5. Honeypot en la red

Cualquier tráfico desde y hacia un Honeypot es dudoso, por lo general es una actividad no autorizada. Es por ello, que todos los datos que brinda una honeypot están desordenados en primera instancia, esto datos deben ser tabulados después de ellos, El análisis de los datos debe ser fas fácil ya que los datos obtenidos de mayor valor y pueden modificare para poder comprendernos mejor y tener un mayor conocimiento para poder así aumentar la seguridad de la red.

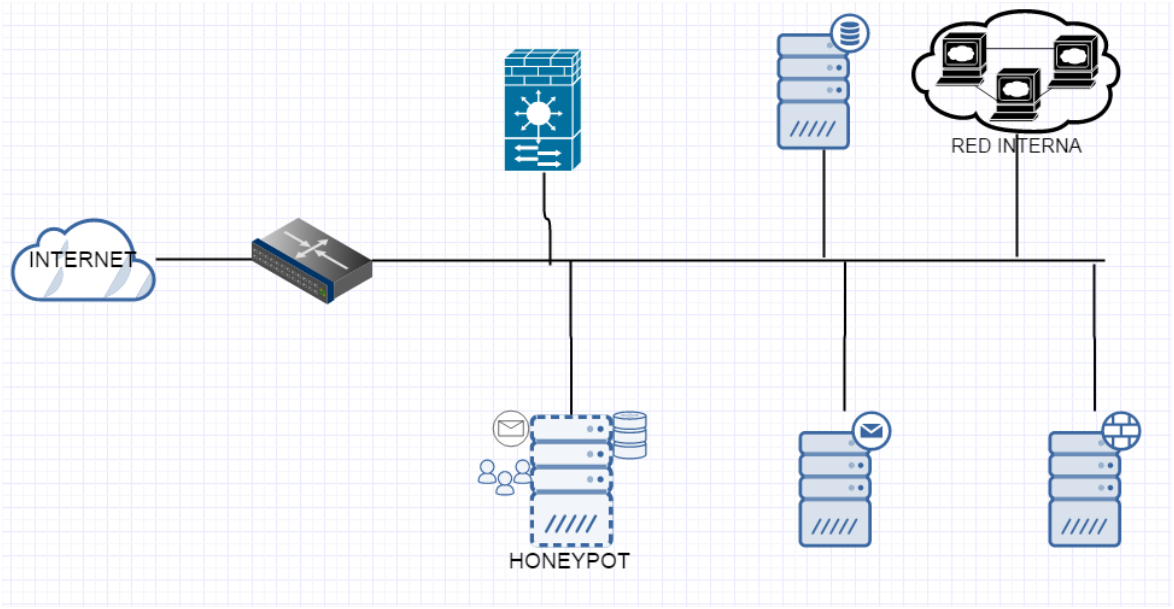


Figura 3: Honeypot como equipo físico en la red

2.2.2.6. Honeynet

Existen otros tipo de configuraciones Honeypots más simples, solo se ejecutan en una sola máquina para que los honeypots puedan reflejarse en los sistemas anfitriones. Los usuarios administradores utilizan sistemas más complejos de configuración los cuales tienen diversos honeypots IDS y componentes de cortafuegos. Estas configuraciones complejas se les llama redes trampa.

Asimismo, las redes Honeynets brinda una simulación de entornos productivos reales a costa de un gasto (administrativo y técnico) mayor o menor. Los archivos de registro de las redes trampa son más complejos en la interpretación en comparación con los de un Honeypot. Existen ocasiones en las que han sido atacados y mal utilizados por varios componentes de terceros. En el mercado existen honeypots gratuitos y comerciales, se diferencian en su complejidad y facilidad de uso.

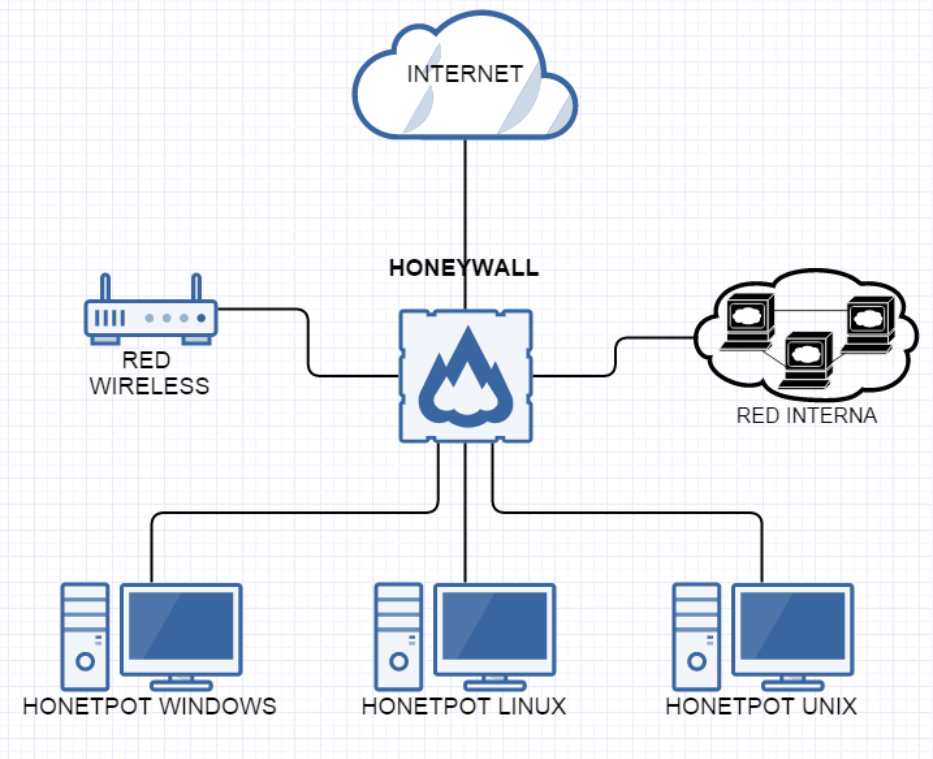


Figura 4: Diagrama Honeynet

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.2.2.7. Riegos e inseguridades informáticas más comunes

Las consecuencias vas desde poco involucramiento de Honeypots de alta participación de riesgo, prevención, detección, protección y respuesta a los ataques de poca interacción en los sistemas de producción, ayudan a que el proceso de recolección de información sea más bajo para así poder definir las tendencias de las actividades de los atacantes, activar los sistemas de alarma, predecir los ataques e investigar con mayor interacción. La utilización de redes trampa está disponible, a pesar de su alto riesgo, la necesidad de conocimientos para poder utilizar el sistema y el hecho que aún existan muchas incertidumbres, la investigación en proceso sobre dicho tema es una gran sorpresa. La evaluación de los riesgos mantiene un esquema ya estructurado, apuntando los análisis a las vulnerabilidades que se hallan en un sistema de información o red de datos.

Figura 5: Modelo evaluación de riesgos Fuente: https://seguridadinformaticaufps.wikispaces.com/file/view/8.JPG/329075810/531x342/8.JPG

2.2.2.8. Tipos de Honeypot

A) Honeypots de baja interacción

Los Honeypots de poca interacción trabajan esencialmente emulando servicios. Su característica principal es que soy fáciles de instalar, ya que no son un sistema real, la instalación de este tipo es “plug and play”, efectuando emulaciones de servicio que constituyen un sistema mas controlado y consecuentemente de riesgo más limitado.

Un ejemplo de ello es el Servicio FTP emulado que funciona en el puerto 21, simula un login FTP y algunos comandos básicos con los que cuenta el servicio y así el atacante muestre interés en este, pero la verdad es que no es un servicio real y no es un riesgo real debido a su capacidad limitada.

Una debilidad de este tipo de Honeypot es que cuenta con una limitada cantidad de información, al no permitirle una mayor interacción hacia el atacante, esta queda limitada en el ataque y solo muestra los primeros pasos dentro de la bitácora planificada para su ataque. Dentro del ejemplo de emulación e un Servicio FTP, con un honeypot de poca interacción solo se podría registrar algunos intentos de ingresar del atacante, sin embargo, nunca se sabría cuáles son las intenciones reales de riesgo, podría ser montar un servidor IRC, almacenar archivos, etc.

Entre los más comunes Honeypots de baja interacción se encuentran:

Specter, Honeyd, KFSensor, PatrioBox.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

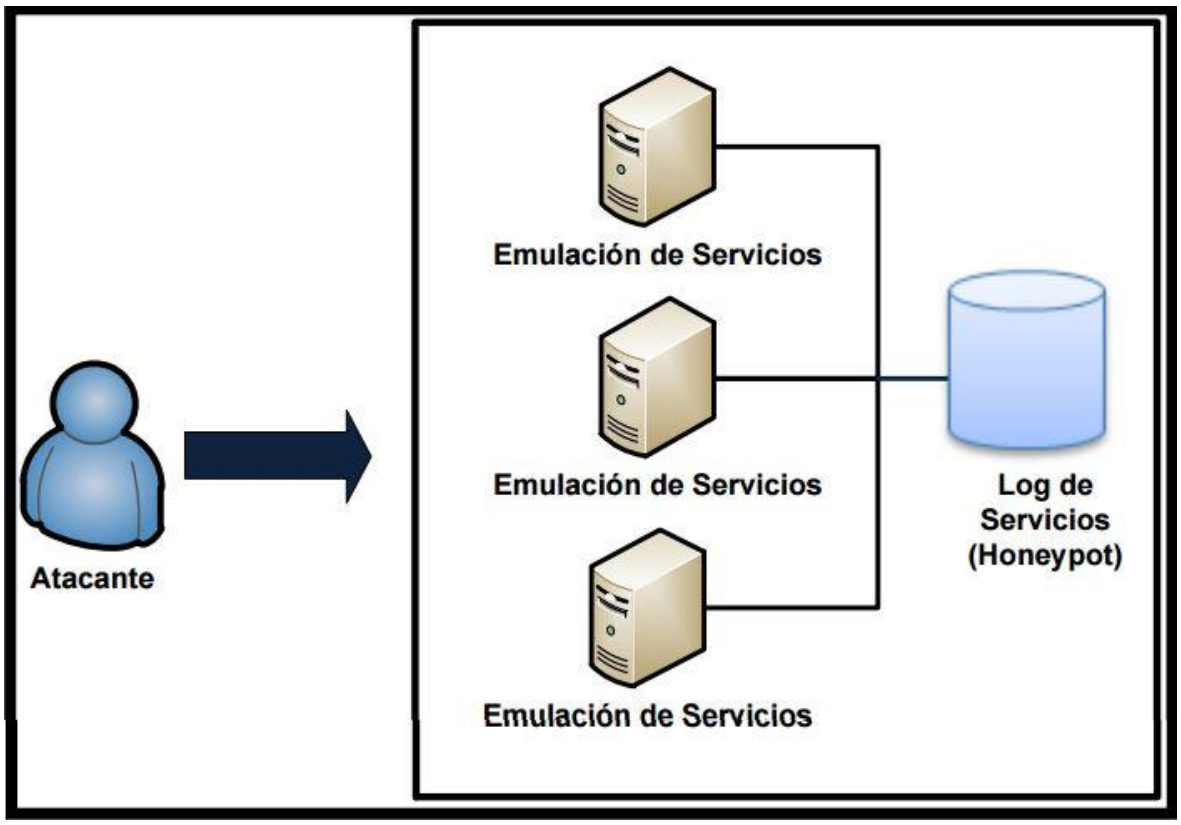


Figura 6: Honeypot de Baja Interacción

2.2.2.8.1. Specter

"Intrusion Detection System", es un Honeypot basado en sistemas de detección de intrusos, sensibles para a los atacantes, este sistema provee servicios web y servicios de correo, estos servicios atraen cómodamente a los atacantes, sin embargo, estas son trampas que intentan recoger información.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.2.2.8.2. Honeyd

Es un honeypot que brinda hosts virtuales en la red, los cuales pueden ser configurados para brindar servicios parciales y su naturaleza puede ser modificada de modo que aparenten estar estableciendo sistemas operativos. Honeyd aumenta la seguridad de autocontrol brindando mecanismos por la detección y evaluación de vulnerabilidades.

2.2.2.8.3. KFSensor

Honeypot de Windows, es un sistema de detección de intrusos (IDS) que detecta y atrae piratas informáticos y gusanos de red. Asimismo, descubre que sistemas son vulnerables a partir de la situación de los servicios del sistema y troyanos.

2.2.2.8.4. PatrioBox

Utiliza el sistema de protección de intrusos (IDS) como un señuelo, medios de red empresarial de forma segura para la detección de amenazas de intrusos. Además utiliza la asistencia para reducir el spam en Internet debido a que aparenta ser un servicio de correo de retransmisión directa.

B) Honeypots de Alta interacción

Los honeypots que cuentan con una alta relación forman una solución mucho más completa, son más complejas de implementar y mantener, porque los sistemas y servicios que ofrece no son emulados, son reales montados sobres sistemas operáticos y hardware, lo que acrecienta el riesgo de uso.

Tomando nuevamente el ejemplo del servicio FTP, en esta situación no se emula dicho servicio, y se instalaría un sistema operativo Windows o Linux, en el cual se instalaría el servidor FTP verdadero, al ponerlo en línea de sistemas de producción y ofrece al atacante una interactividad más real.

El beneficio que se obtiene de utilizar esta solución es la gran cantidad de información que se puede almacenar del atacante, dependiendo de la complejidad del Honeypot, se puede saber exactamente los pasos que tiene el intruso, herramientas y sus técnicas.

Los Honeypots de baja interacción más comunes son:

HoneyNet, ManTrap, HoneyWall.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

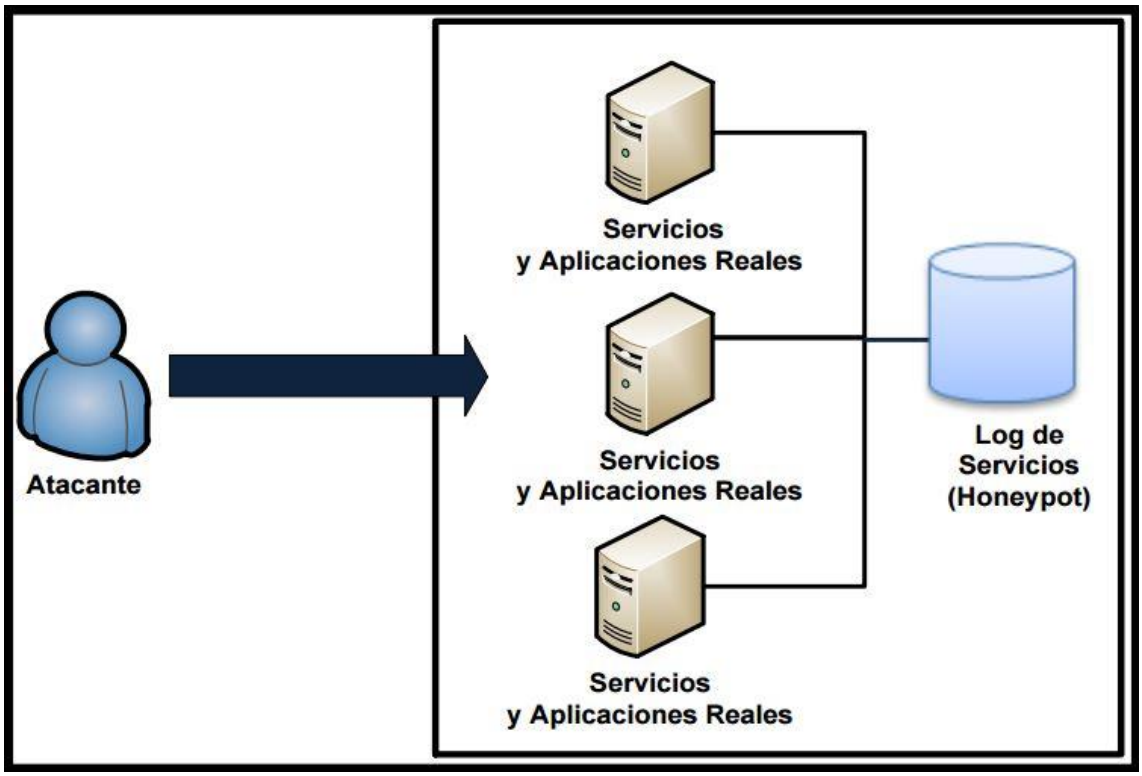


Figura 7: Honeypot de Alta Interacción

2.2.2.8.5. HoneyNet

Es una clase de Honeypot que tiene alta interacción y cuenta con un diseño para recaudar mucha información sobre las amenaza comprometidas en la organización, la Honeynet brinda un medio real de sistemas, servicios y aplicaciones para poder saber que planes tienen los atacantes, lo que convierte a una honeynet un conjunto de honeypots.

2.2.2.8.6. ManTrap

Es capaz de crear un “software jaula” que puede simular la red virtual de una máquina. Para lograr esto se emulan varios servicios en una ManTrap. Este tipo de Honeypot se adapta para que pueda notificar al administrador mediante alertas, correos electrónicos o un dispositivo con contenido SNMP, alertando de algún intruso en la “jaula”.

2.2.2.8.7. HoneyWall

El Honeywall CDROM es un CD que cuenta con las herramientas necesarias para poder configurar una Honeynet (red trampa) de tercera generación. El CDROM está hecho en base a una reducida versión de Linux y su diseño está hecho para que pueda usarse como aplicación: cuenta con las herramientas necesarias para controlar el Honeywall.

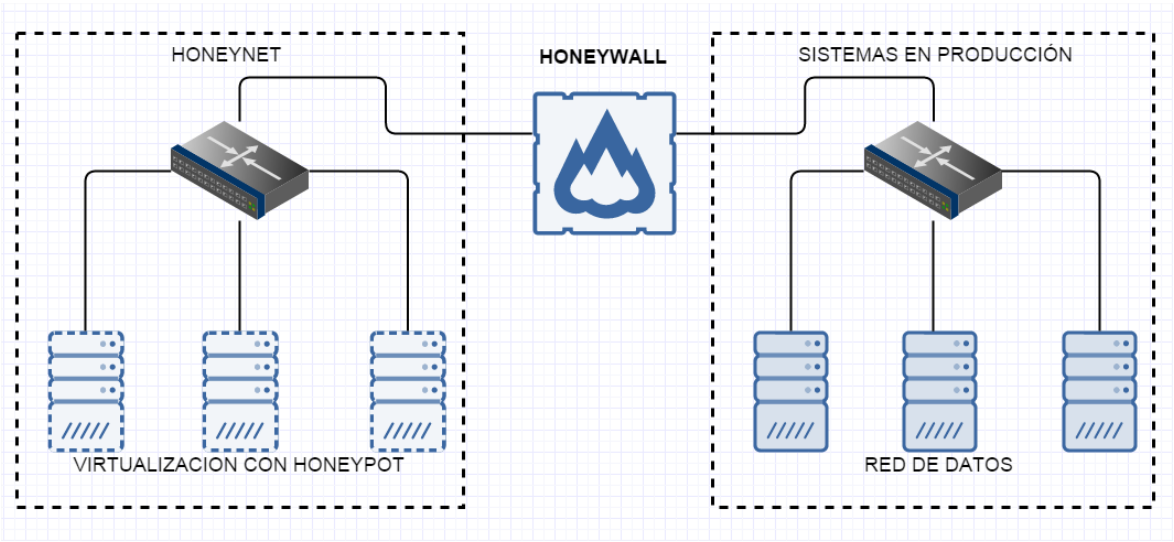


Figura 8*: Estructura de Honeywall*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.2.2.8.8. Procedimiento de captura y análisis

ManTrap utiliza un sniffer de red para acumular todos los paquetes de red dirigidas hacia o desde el Host ManTrap [14]. El módulo de reglamentarias presenta toda la lectura o escritura de información durante una sesión terminal.

```
192.168.1.96 68.177.102.20 / 0.170081
192.168.1.96 68.177.102.20 /stylesheets/smoothness-css 0.170682
192.168.1.96 68.177.102.20 /scripts/jquery 0.173387
192.168.1.96 68.177.102.20 /scripts/jquery-highlight 0.172521
192.168.1.96 68.177.102.20 /scripts/cookie_reader 0.175224
192.168.1.96 68.177.102.20 /scripts/snort 0.170195
192.168.1.96 68.177.102.20 /scripts/jquery-ui 0.173404
192.168.1.96 68.177.102.20 /scripts/rule-search 0.169380
192.168.1.96 68.177.102.20 /stylesheets/screen-css 0.164117
192.168.1.96 209.85.227.113 /ga.js 0.097584
```

Figura 9: Análisis del atacante en la red (Kali Linux)

2.2.2.8.9. Información recolectada

La minería de datos es un método para poder observar los datos en tiempo real e inspeccionar miles de alertas sin conexión. Un conjunto de herramientas de minería de datos es muy importante para un IDS para usar todo su potencial. Otras características de los sistemas de detección de intrusiones son “bajas tasas de falsas alarmas”.

2.4. FASES EN LA PENETRACIÓN DE UN SISTEMA

2.4.1. FOOTPRINTING

Footprinting se define como el análisis del perfil de seguridad de una empresa u organización, emprendido de una manera metodológica; se la considera metodológica debido a que se busca información crítica basada en un descubrimiento anterior.

No existe una sola metodología para realizar footprinting, un individuo puede escoger muchos caminos para llegar a la información, así mismo esta actividad es esencial debido a que toda la información crítica necesita ser recopilada antes de que el hacker pueda decidir sobre la mejor acción a realizar.

El footprinting necesita ser desarrollado correctamente y en una manera organizada, la información descubierta puede pertenecer a varias capas de red, por ejemplo, se puede descubrir detalles del nombre del dominio, direcciones de red, servicios de red y aplicaciones, arquitectura del sistema, IDS's, direcciones IP específicas, mecanismos de control de acceso, números telefónicos, direcciones de contacto, mecanismos de autenticación, entre otros.

Este listado puede incluir mucha más información, dependiendo de cómo los aspectos de la seguridad son tratados dentro de la organización. La información recolectada durante la fase de footprinting se puede utilizar como un puente para poder escoger la metodología del ataque. Un aspecto de la información es que casi todo se puede conseguir por medio del Internet, la mayoría disponible al público en general.

2.4.2. SCANNING

Una de las principales actividades que un atacante realiza cuando intenta penetrar a un sistema es reunir toda la información posible y realizar un inventario de puertos abiertos usando alguna técnica de escaneo de puertos.

El escaneo de puertos es una de las técnicas más populares de reconocimiento usada por hackers a nivel mundial. Una vez completado este proceso, esta lista ayuda al atacante a identificar algunos servicios que están ejecutándose en el sistema objetivo, usando una lista de puertos conocidos; esto permite posteriormente crear una estrategia que conduzca a comprometer el sistema.

Al escanear cuáles puertos están disponibles en el equipo de la víctima, el atacante encuentra potenciales vulnerabilidades que pueden ser explotadas.

2.5. IDENTIFICACIÓN DE VULNERABILIDADES

Una vulnerabilidad es cualquier falla inherente en el diseño, configuración o implementación de un sistema o una red que pueda desembocar en un evento que pueda comprometer la seguridad.

Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se utilizan para perpetrar ataques a la seguridad de un sistema. Hay que establecer las prioridades en los elementos a proteger, de acuerdo al valor que representan para la organización y de esta forma poder prevenir los diferentes tipos de ataques que pueden sufrir, detectando las vulnerabilidades que presentan estos elementos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.6. PENETRACIÓN AL SISTEMA

Esta es una de las fases más importantes para un hacker porque es la fase de penetración al sistema informático, en esta fase un hacker explota las vulnerabilidades que encontró. La explotación puede ocurrir localmente, [offline] sin estar conectado, sobre la red de área local (Local Area Network), o sobre el Internet y puede incluir técnicas como buffer overflows (desbordamiento de buffer), Denial-of-Service (denegación de servicio), sesión hijacking (secuestro de sesión), y password cracking (romper o adivinar claves usando varios métodos como: diccionary atack y brute forcé atack). En esta fase los factores que ayudarán a un hacker a tener una penetración con éxito a un sistema informático dependerá de:

- ✓ Cómo es la arquitectura del sistema informático y de cómo está configurado el sistema objetivo y/o víctima. Una instalación y configuración de seguridad informática simple significa un acceso más fácil a un sistema informático, nada que comentar si esta seguridad informática ni siquiera existe.
- ✓ Cuál es el nivel de destrezas, conjunto de habilidades y conocimientos sobre seguridad informática de los ingenieros, profesionales y auxiliares que instalen y configuren un sistema informático.
- ✓ Nivel de destrezas, conjunto de habilidades y conocimientos sobre seguridad informática y redes que tenga un hacker y el nivel de acceso que obtuvo al principio de la penetración

2.7. BORRADO DE HUELLAS

En esta fase es donde un hacker trata de destruir toda evidencia de cualquier posible rastreo de sus actividades ilícitas y lo hace por varias razones, entre ellas: seguir manteniendo el acceso al sistema informático comprometido, ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el hacker podrá seguir penetrando el sistema cuando quiera. Además borrando sus huellas evita ser detectado y por tanto, anula la posibilidad de ser atrapado por la policía informática y quedar así al margen del imperio de la ley.

2.8. Definición de la terminología

Ciberataques: Ataques ejecutados a través de computadores o dispositivos conectados en una red local o Internet.

IDS: Sistema de detección de intrusos, su función principal es detectar accesos no permitidos a un computador o en una red de datos.

VPNs: Grupo de redes o red privada virtual.

ACL: Son unas listas que permiten el control del acceso al medio, para aislar los niveles de privilegio.

DDoS: En seguridad informática, un ataque de denegación de servicios.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Honeypot: Denominado por ser un software o computadores, que simulan ser un sistema vulnerable, así distrayendo al atacante.

Firewall: Sistema de protección en una red, creado para bloquear o controlar el acceso no autorizado, permitiendo conexiones de confianza.

Wrappers: Sistema de alto nivel de seguridad, la funcionalidad principal es permitir o bloquear los servicios o procesos del Servidor o Sistema.

MD5: Algoritmo que utiliza un código propio de archivo para su protección.

SHA: Un conjunto de funciones o scripts diseñados para proteger una aplicación o un dispositivo, con la implementación de algoritmos.

PGP: Sistema desarrollado para resguardar la información en las comunicaciones de datos.

NIDS: Un sistema que permite la detección de intrusiones en una red local o una red virtual.

Advanced IP Scanner: Programa que escanea todos los dispositivos de red, le brinda acceso a las carpetas compartidas y a los servidores FTP.

HIDS: Un sistema que detecta posibles intrusiones en las maquinas conectadas en una red.

Honeynet: Es un grupo o un conjunto de Honeypots con alta interacción en una red diseñada para ser vulnerada. Se puede usar para conocer los tipos de ataques que se pueden producir en un Sistema determinado.

SNMP: Protocolo de administración de red, utilizado para un escaneo y diagnóstico de la red.

CDROM: Contiene la información de un Sistema de arranque e instalación, no puede ser utilizado para regrabar la información generada en la instalación.

IPsec: Grupo de protocolos, configurados para asegurar las conexiones en una red, seguridad en IP.

Logs: Registros temporales de la actividad de un software o un sistema en producción, el almacenamiento es generado por el comportamiento del mismo, pueden ser registros informativos, alertas o configuraciones necesarias.

AAA: Tres funciones principales; autentificación, autorización y contabilización.

GNU: Sistema operativo de tipo Unix, acrónimo recursivo que significa "GNU No es Unix".

FDL: Free Software Foundation.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

GUI: Una interfaz gráfica de usuario para lograr la interacción con el sistema.

HWCTL: Comando o herramienta para la ejecución de las órdenes para la administración del Honeywall.

Walleye: Modulo de administración del Honeywall, permite el uso de una interfaz web.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO III: MARCO METODOLÓGICO

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.1. Tipo y Diseño de Investigación

La presente investigación es de tipo Tecnológico y el diseño es cuasi-Experimental.

3.2. Población y Muestra

La población de este proyecto se encuentra en el local de la Municipalidad Distrital de Huambos, ubicada en el centro de Huambos.

Se contará con el personal administrativo que maneja SIAF tales como Tesorería, Contabilidad, Presupuesto, Abastecimiento, Informática y que a su vez se evaluarán las computadoras que se encuentran en las oficinas de la MDH y se usarán las guías de observación para la recolección de datos, de estas unidades de estudio se sacarán los datos a comparar en el pre y post test, se detallan a continuación en el siguiente cuadro:

ÁREA	Nº
Tesorería	3
Contabilidad	3
Presupuesto	2
Abastecimiento	5
Informática	2
Computadoras	15

Tabla 1: Componentes del sistema informático a analizar.

Figura 10: Población

3.3. Hipótesis

La implementación de Honeypot en la red de datos de la Municipalidad Distrital de Huambos, permitirá detectar y corregir las vulnerabilidades de la red informática.

3.4. Operacionalización:

VARIABLE INDEPENDIENTE	DIMENSIONES	INDICADORES	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS
Implementación de la Honeypot para para corregir vulnerabilidades.	Tipos de Honeypot y Honeynet.	Indicador de cuanto tráfico puede manejar el Honeypot o con cuantos adversarios Interactuar.	Registro de incidentes.

VARIABLE DEPENDIENTE	DIMENSIONES	INDICADORES	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS
Ataques a la red de datos de la Municipalidad de Huambos.	Lógica	Perdida de paquetes de datos. Accesos no autorizados	Registro de incidentes

Tabla 2: Operacionalización

3.5. Métodos, técnicas e instrumentos de recolección de datos

Método de la Observación:

La recolección de datos que se ha planteado para el caso es que se obtenga varias Honeynets en un entorno distribuido. Se puede dar para niveles de operadores en un Sistema SIAF o para varios sectores centralizando los datos obtenidos.

El análisis es cuando los datos obtenidos para la Honeynet son estudiados para encontrar varios patrones de ataque, nuevos ataques y lo que se determine como objetivo de investigación.

3.5.1. Método de la medición:

Los resultados obtenidos se validarán para verificar efectividad de la Honeypot y Honeynet dentro de una red de datos.

Para la recolección de datos se usará las siguientes técnicas.

a) Observación

Es el registro visual de que sucede en una situación real, ordenando los acontecimientos pertinentes de acuerdo con un esquema previsto y según el problema que se estudia.

b) Documentación

Se estudiará material bibliográfico (libros, papers, etc), así como las técnicas que rigen las características de las Honeypot y Honeynet.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.6. Procedimiento para la recolección de datos

Se realizarán encuestas, entrevistas a los usuarios del SIAF, tales como Tesorería, Contabilidad, Presupuesto, Abastecimiento, Informática de la Municipalidad de HUAMBOS.

TÉCNICAS	INSTRUMENTO
RECOLECCIÓN DE INFORMACIÓN	Registro de incidentes
PLANTEAMIENTO DE SOLUCIONES	Metodología de la Honeypots
ANÁLISIS DE LOS RESULTADOS	Microsoft Excel 2016

Tabla 3: Procedimiento para la recolección de datos

Fuente: Elaboración Propia.

El proceso para la recolección de los datos se establecerá por la siguiente ruta investigativa:

a. Observación de la realidad y recolección de datos

Para la recolección de los datos se utilizó herramientas de pre test y pos penetración al sistema donde se realizaron 750 ataques antes de la implementación y 750 ataques después de la implementación, elaborado por el tesista. Dichos ataques se encuentran en la sección de anexos de la presente tesis.

b. Problema

Luego de analizar la situación actual de la red de datos de la Municipalidad Distrital de Huambos, se plantea la implementación del honeypot que corregirá las vulnerabilidades encontradas en las pruebas del pre test.

c. Objetivo general y específico

Los beneficios de implementar un Honeypot que permitirá corregir vulnerabilidades en la red de datos.

d. Posibles soluciones

Al analizar y procesar los datos, se procederá a plantear estrategias para la solución del problema que se encontró.

e. Determinación de resultados

Al final se plantearán las conclusiones a las que se llegaron una vez concluido el proyecto de investigación.

3.7. Análisis Estadístico e Interpretación de los datos

Una vez obtenido el resultado de las pruebas realizadas en ataques a la red de datos MDH se emplearán tablas gráficas para obtener el resultado global de los ataques, para estos gráficos se utilizará el software Microsoft office Excel, donde se interpretará los resultados obtenidos de los ataques realizados.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.8. Criterios éticos

Para ejecutar esta investigación, se aplicarán tres principios éticos citados por Belmont Report (Informe Belmont), los que se centran en las normas de conducta ética en una investigación.

3.8.1. Principio de Beneficencia

"Por sobre todas las cosas, no dañar", utilizando este principio se pudo aplicar a la investigación sin dañar social, económica y psicológicamente al estudiante, por el contrario, el estudiante es beneficiado con nuevos recursos tecnológicos para incrementar sus conocimientos sobre la creación de compiladores visuales.

3.8.2. Principio de respeto a la Dignidad Humana

Este principio abarca el Derecho a la Autodeterminación y al Conocimiento Irrestricto de la Información. En esta investigación, los estudiantes fueron entendidos de los objetivos que la investigación en la que participaron de manera voluntaria, con el conocimiento y comprensión para tomar la decisión adecuada.

3.8.3. Principio de Justicia

Este principio contiene el Derecho del Sujeto a un trato justo y a la privacidad. Debido a lo establecido en este principio, se realizó una selección justa y no discriminadora de los estudiantes, quienes fueron tratados de manera justa y equitativa, antes, durante y después de su participación. A los que se rehusaron a participar se los trató sin prejuicios.

3.9. Criterios de rigor científico

Los criterios de rigor científico que se van a tomar en cuenta en la siguiente investigación son los mostrados a continuación:

Validez: el apropiado uso de las preguntas de investigación, de forma que las variables que se utilicen sean relevantes y que abarquen todas las dimensiones que contienen las preguntas de la investigación.

Generalizabilidad: también es llamada validez externa, ya que se enfoca en que la muestra sea una parte representativa de la población. Para esto se debe evitar sesgos mediante marcos muestrales adecuados y aleatorios.

Fiabilidad: deberá tener precisión suficiente. Está relacionada con la minimización del error aleatorio y necesita de un tamaño de muestra suficiente.

Replicabilidad: la posibilidad que se pueda repetir la investigación y evitar que los resultados se contradigan.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO IV: SELECCIÓN DE ATAQUES TÍPICOS EN UNA RED DE DATOS DE UNA MUNICIPALIDAD

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4.1 TIPOS DE ATAQUES TIPICOS EN UNA RED DE DATOS:

Según el autor (Soriano, Seguridad en redes y seguridad de la información, 2014) Los ataques a las redes pueden ser definidos como diferentes tipos de actividades sistemáticas dirigidas a disminuir o corromper su seguridad. Desde este punto de vista, un ataque puede ser definido como una amenaza sistemática generada por una entidad de una manera artificial, deliberada e inteligente.

Las redes de ordenadores pueden ser vulnerables a muchas amenazas utilizando distintas formas de ataque, entre ellas:

- Ingeniería social, alguien trata de acceder usando medios sociales (haciéndose pasar por un usuario legítimo o el administrador del sistema, engañando a la gente para que le revelen secretos o claves, etc.). Esta vía de ataque suele dar muchos resultados a los atacantes.
- Ataques de denegación de servicio, incluyendo todos los tipos de ataques destinados a saturar a un ordenador o a una red, de tal manera que los usuarios legítimos no pueden utilizarla.
- Ataques a determinados protocolos, aprovechando debilidades conocidas.
- Ataques a servidores, que aprovechan las vulnerabilidades de ciertos sistemas operativos de los ordenadores o vulnerabilidades en la configuración y administración del sistema.
- Adivinar contraseñas; las contraseñas son secuencias de símbolos, generalmente asociadas a un nombre de usuario, que proporcionan un mecanismo para la identificación y la autenticación de un usuario en particular.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

En casi todos los servicios son los propios usuarios quienes eligen sus contraseñas, y con frecuencia eligen secuencias que no pueden ser consideradas seguras (por ejemplo, nombre de la pareja, nombre de hijo/hija, fechas de nacimiento) Como regla general, las contraseñas que son fáciles de recordar son también fáciles de adivinar.

- Espionaje de todo tipo, incluyendo la captura de mensajes de correo electrónico, archivos, contraseñas y otra información a través de una conexión de red que permite capturar todos los mensajes de un usuario.

Los ataques de seguridad pueden clasificarse en:

- Ataques pasivos.
- Ataques activos.

4.4.1 ATAQUES PASIVOS

Según el autor (Soriano, Seguridad en redes y seguridad de la información, 2014) Un ataque pasivo es aquél en que el atacante monitoriza el canal de comunicación sin modificar ni añadir datos. Un atacante pasivo sólo pone en peligro la confidencialidad de los datos. El objetivo del atacante es obtener la información que se está transmitiendo.

Los ataques pasivos están relacionados con el contenido del mensaje y con el análisis de tráfico:

- Espionaje. En general, la mayoría de la información que se transmite utilizando una red de comunicaciones se envía de forma no segura (sin cifrar) permitiendo a un atacante "escuchar" o interpretar (leer) los datos intercambiados. Uno de los mayores problemas a los que se enfrenta un

administrador de una red deriva de la capacidad de un atacante para monitorizarla. Sin servicios de cifrado (basados en el uso de técnicas criptográficas), los datos pueden ser leídos por otras personas a medida que circulan por la red.

- Análisis de tráfico. Se refiere al proceso de interceptar y examinar los mensajes con el fin de deducir información de patrones en la comunicación. Se puede realizar incluso cuando los mensajes están cifrados. En general, cuanto mayor es el número de mensajes observados, interceptados y almacenados, más se puede inferir del tráfico. El análisis de tráfico, entre otras cosas, permite a un atacante verificar que dos entidades están manteniendo una comunicación en un determinado momento. La figura 11 muestra un modelo de ataque pasivo

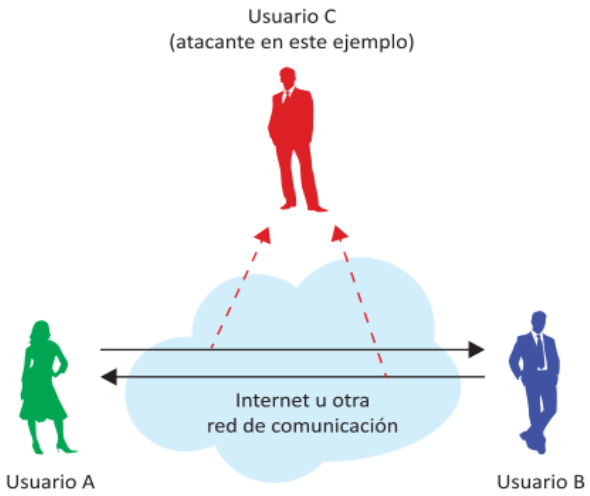


Figura 11: Modelo de ataque pasivo

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4.4.2 ATAQUES ACTIVOS

Según el autor (Soriano, Seguridad en redes y seguridad de la información, 2014) Un ataque activo intenta alterar los recursos del sistema o afectar a su funcionamiento. En este tipo de ataque el adversario intenta borrar, añadir, o modificar los datos transmitidos. Un atacante activo amenaza la integridad de datos y autenticación, así como la confidencialidad.

Los ataques activos engloban alguna modificación del flujo de datos o la creación de datos falsos. Puede dividirse en seis categorías:

- Suplantación de identidad. Es un tipo de ataque en el que el atacante suplanta la identidad de otro usuario.
- Repetición. En este tipo de ataque, una transmisión de datos válida es repetida o retardada de forma maliciosa. Este ataque lo puede provocar el mismo emisor de datos originales o bien un atacante que los intercepta y posteriormente los retransmite, posiblemente como parte de un ataque de suplantación de identidad.
- Modificación de mensajes. El atacante elimina un mensaje que atraviesa la red, lo altera, y lo reinserta.
- Hombre en el medio (Man in the Middle, MitM). En este tipo de ataques, un atacante intercepta las comunicaciones entre dos entidades, por ejemplo entre un usuario y un sitio web. El atacante puede utilizar la información que consigue para luego suplantar la identidad del usuario o realizar cualquier otro tipo de fraude.
- Denegación de Servicio (Denial of Service DoS) y Denegación de Servicio Distribuida (Distributed Denial of Service, DDoS). Una denegación de

servicio (DoS) es una situación en la que un usuario u organización se ve privado de los servicios o recursos que normalmente debería tener. En denegación de servicio distribuida, un gran número de sistemas comprometidos (a veces llamado botnet) atacan a un solo objetivo.

- Amenazas Avanzadas Persistentes (Advanced Persistent Threat, APT). Es un ataque a la red en el que un atacante consigue un acceso no autorizado a la red y permanece allí sin ser detectado durante un largo período de tiempo. La principal intención de un ataque APT es robar datos más que causar daños a la red u organización. Algunas organizaciones que pueden ser objetivo de ataques APT son sectores con alto valor informativo, como la defensa nacional, la industria financiera.

La figura 12 muestra un ejemplo de un ataque activo (en concreto, de un ataque de modificación)

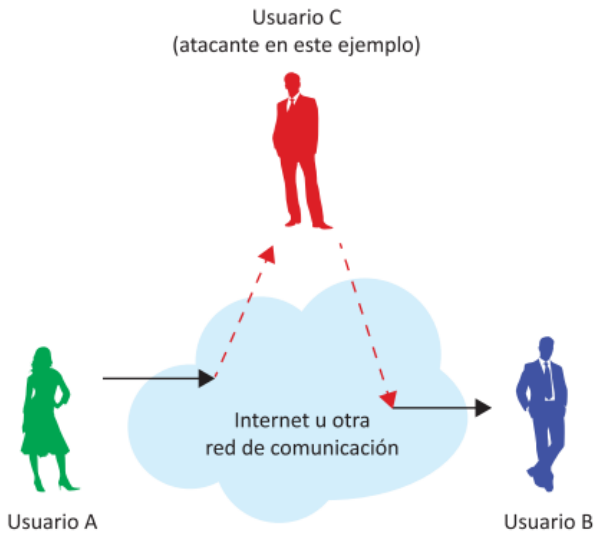


Figura 12: Ataque activo de modificación

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4.5 CLASIFICACIÓN DE ATAQUES

Las medidas de seguridad informática van en caminadas mantener la confidencialidad, autentificación, integridad, no repudio, control de acceso y disponibilidad dichos amenazas pueden provenir desde dentro o fuera y las podemos clasificar en: fabricación, intercepción, interrupción y modificación.

De los cuales tenemos los siguientes tipos de ataques más comunes;

Virus

Es un programa capaz de reproducir un error e insertarlo en programas o áreas del sistema de manera que altere su funcionamiento. Algunos de los elementos que pueden verse afectados por los virus son: archivos de datos, sectores de los discos duros, programas, tablas de particionado etc.

Tipos de virus

Virus del sector de arranque. Modifica el sector de arranque, suelen ser antiguos.

Parásitos (virus de archivo) Se alojan en archivos ejecutables. Primero se ejecuta el virus y luego este ejecuta el archivo para permanecer oculto. Suelen estar bastante extendidos.

Virus macro. Utiliza los macros (comandos de ciertos documentos que se ejecutan con él, como pueden ser los procesadores de texto. Pueden copiarse y trasmitirse de un documento a otro. Son independientes de los sistemas operativos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Troyanos.

Es un programa encubierto que realiza tareas no previstas. Otra variante son los troyanos de puerta trasera que permiten controlar otro ordenador.

Bombas lógicas. Son similares a los troyanos pero que se ejecutan en una determinada fecha o condiciones.

Gusanos. Son como los virus pero que no necesitan portador ya que se ejecutan y propagan por sí mismos. Son difíciles de programar. Los más habituales utilizan el correo electrónico.

Applets malignos. Los applet son programas realizados en java y que suelen ir incluidos en páginas web.

Puertas traseras. Programas que permiten saltarse los mecanismos habituales de acceso.

Monitorización

Por medio de esta se estudia para realizar el ataque. Los mecanismos más utilizados son.

Ingeniería Social. Para ello se utiliza las debilidades de las personas.

Exploit. Viene de to exploit “aprovechar”. Código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios.

Shell. Parte fundamental de un sistema operativo encargada de ejecutar las órdenes básicas para el manejo del sistema. Suelen incorporar características

tales como control de procesos, redirección de entrada/salida y un lenguaje de órdenes para escribir programas por lotes o scripts.

Shoulder Surfing. Por medio del espionaje físico de las personas.

Programas trampa p-e. La simulación de una página de un banco donde introducir los datos.

Easvesdropping. Captación de información. Suele utilizarse sniffers.

Ataques de autentificación. Por mecanismos de suplantación de la identidad.

Spoofing. Se entra con claves de acceso validas obtenidas de manera fraudulenta.

Ip spoofing en la que se generan paquetes con una ip falsa.

Web spoofing, se genera un sitio web falso.

Ip splicing en la que se contrala la sesión de otro.

Fuerza bruta en la que se localizan contraseñas por medio aleatorios o diccionarios.

Ataques de modificación.

Van desde daños al sistema hasta borrado de información. Ejemplos de ellos son.

Tampering Es la alteración de los datos o programas por otros maliciosos. Los mecanismos utilizados pueden ser Java applets y controles ActiveX (en java), masquering (suplantación de la identidad), Scavenging (búsqueda de la información en la basura).

4.6 Selección de ataque en la MDH

En la Municipalidad Distrital de Huambos, gran parte de los equipos de cómputo utilizan computadoras con sistema operativo Windows XP Profesional con Service Pack 2, de la cual es muy vulnerable a los ataques informáticos de las cuales seleccionaremos el ataque típico en la red de datos de la MDH

Valoración

ATAQUE	*RED DE DATOS*	*SERVIDORES*	*EQUIPOS MDH*	*SELECCIÓN MDH*
Parásitos	SI	SI	NO	NO
Virus Macro	SI	SI	NO	NO
Troyano	SI	SI	NO	NO
Bombas lógicas	SI	SI	NO	NO
Gusanos	SI	SI	NO	NO
Applets malignos	SI	SI	NO	NO
Puertas traseras	SI	SI	SI	SI
Exploit	SI	SI	SI	SI
Shell	SI	SI	SI	SI
Ingeniería social	NO	SI	NO	NO
Shoulder surfing	SI	SI	NO	NO
Programas trampa	SI	SI	NO	NO
Easvesdropping	SI	SI	NO	NO
Ataques de autentificación	SI	SI	NO	NO
Spoofing	SI	SI	NO	NO
Ip spoofing	SI	SI	SI	SI
Web spoofing	SI	SI	NO	NO
Ip splicing	SI	SI	NO	NO
Fuerza bruta	SI	SI	NO	NO

Tabla 4: Selección de ataques tipos a la MDH

Luego de seleccionar el ataque se procederá a realizar un análisis de la situación actual de la Municipalidad Distrital de Huambos

4.7 Diagnóstico de la Situación Actual

Actualmente en la red de datos de la Municipalidad Distrital de Huambos, cuentan con 15 computadas en la red las cuales son de; Tesorería, Contabilidad, Presupuesto, Abastecimiento e Informática, dentro de ello existe un servidor que se comprarte el Sistema SIAF (SISTEMA INTEGRADO DE ADMINISTRACION FINANCIERA). Para el análisis de vulnerabilidades de la red de datos de la Municipalidad Distrital de Huambos, se utilizarán fases de penetración en la red antes del diseño de la Honeypot. Las mismas que se detallan a continuación:

4.7.1 FOOTPRINTING

Simulando el primer paso de un atacante informático se procede al cambio de MAC-ADDRESS a fin de evitar cualquier seguimiento de nuestra verdadera dirección física.

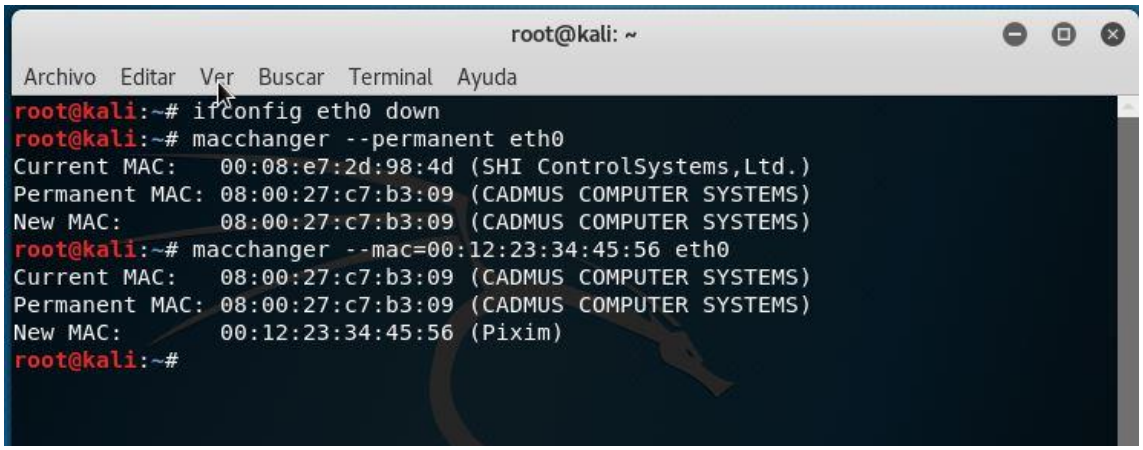


Figura 13: *Cambio de mac adrress*

Se procede a identificar los servidores DNS que han sido asignados a través de DHCP

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

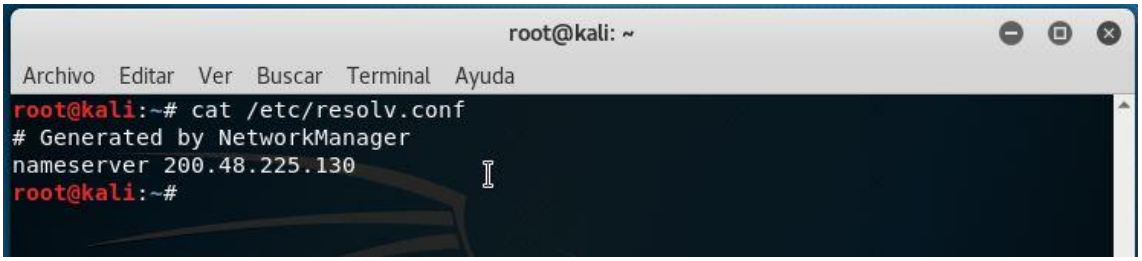


Figura 14: Verificación de los servidores DNS

Prueba de traceroute a www.google.com y protocolo ICMP a las direcciones de ip de red de datos de la MDH

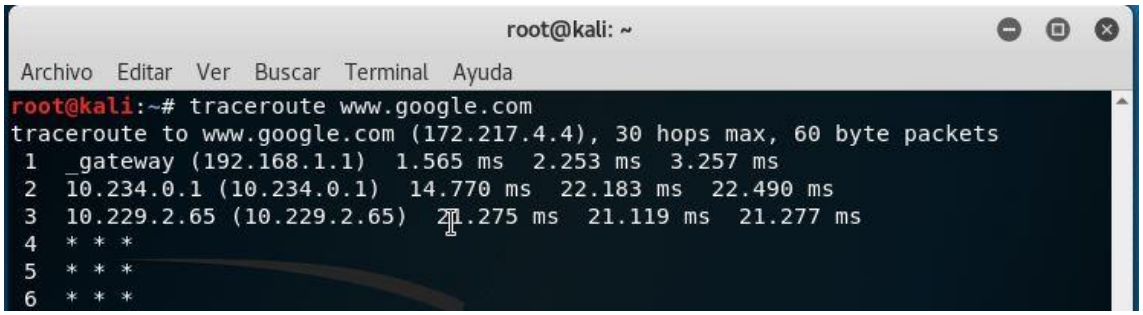


Figura 15: Prueba de Traceroute

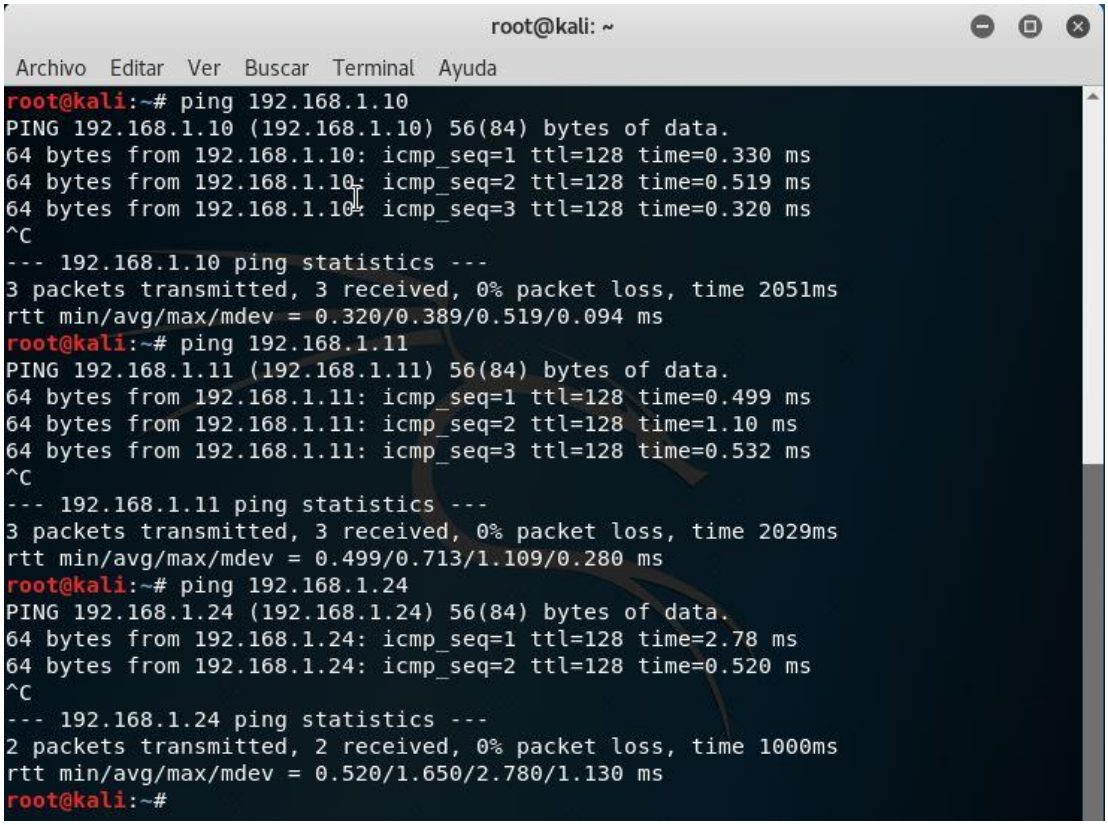


Figura 161: Prueba de ICMP a los host de la MDH

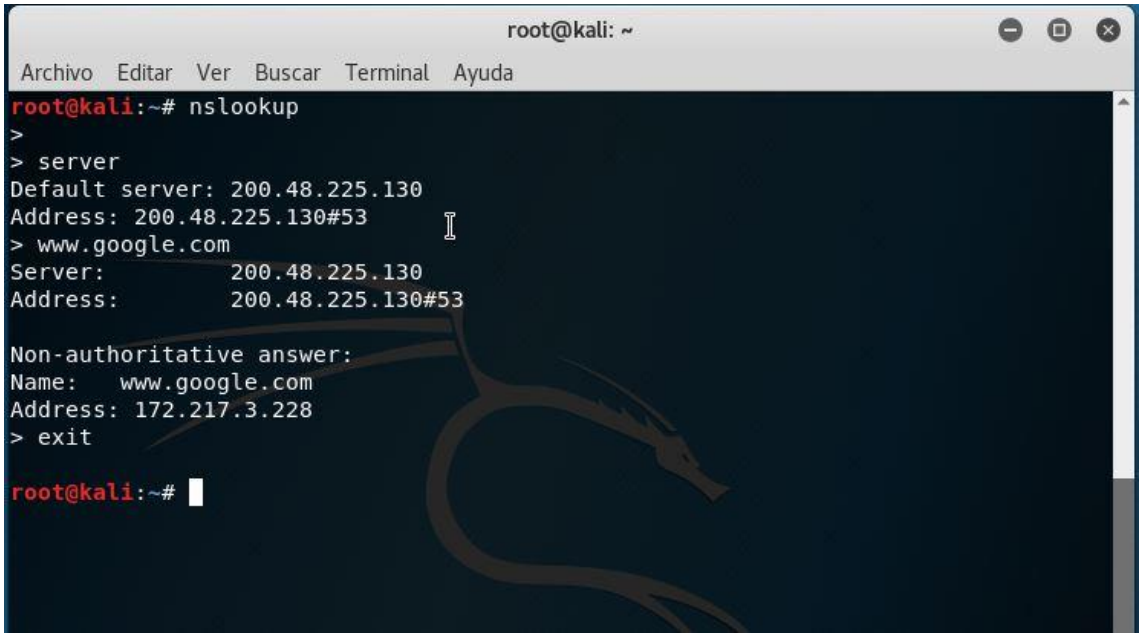


Figura 17: Búsquedas en el DNS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4.7.2 SCANNING

Una vez que se ha realizado un análisis de Footprinting pasivo, se procederá a la fase de Scanning de manera activa.

Para este ejemplo se utiliza la herramienta Angry IP Scanner, la cual nos permite visualizar de una manera gráfica los host que se encuentran activos en la red, además de su nombre y posibles puertos que se encuentran abiertos

De esta manera se puede tener una mejor idea de la topología existente y de los equipos activos que se encuentran presentes en la misma.

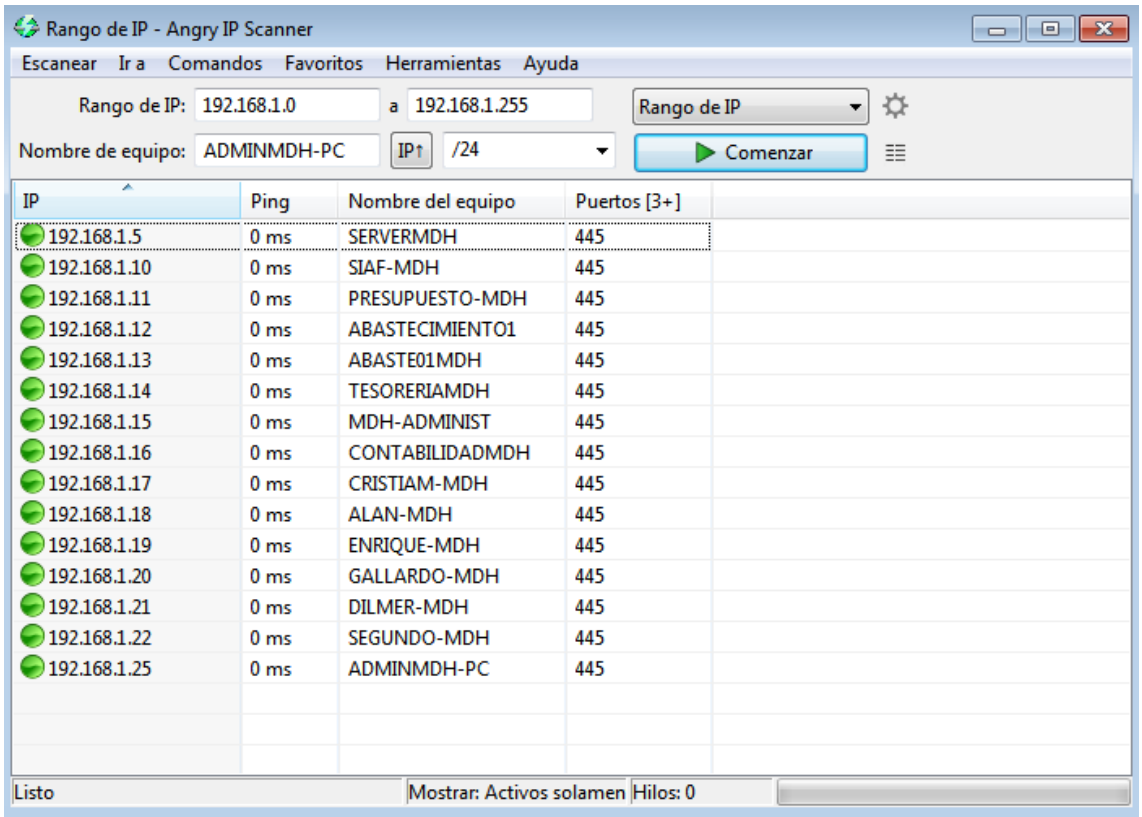


Figura 18: Hosts en la red de la MDH

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Una vez que se han seleccionado las víctimas se procederá a la búsqueda específica de puertos abiertos para determinar posibles vulnerabilidades a través de la herramienta Nmap.

root@kali:~# **nmap 192.168.1.0/24 --open -T4 -O**

Starting Nmap 7.60 (https://nmap.org) at 2018-01-23 20:15 -05
Nmap scan report for 192.168.1.1
Host is up (0.0036s latency).
Not shown: 992 filtered ports, 5 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https
MAC Address: 64:77:7D:7E:A7:22 (Hitron Technologies.)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.8 - 2.6.30
Network Distance: 1 hop

Nmap scan report for 192.168.1.10
Host is up (0.00066s latency).
Not shown: 984 closed ports
PORT STATE SERVICE
53/tcp open domain
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1025/tcp open NFS-or-IIS
1027/tcp open IIS
1037/tcp open ams
1040/tcp open netsaint
1048/tcp open neod2
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
MAC Address: 08:00:27:52:2B:4D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

cpe:/o:microsoft:windows_server_2003::sp1
cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop

Nmap scan report for 192.168.1.11
Host is up (0.00085s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:AF:DF:0D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003, Microsoft Windows XP SP2 or Windows Server 2003 SP2
Network Distance: 1 hop

Nmap scan report for 192.168.1.12
Host is up (0.00062s latency).
Not shown: 990 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
MAC Address: 08:00:27:77:5D:51 (Oracle VirtualBox virtual NIC)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_10 cpe:/h:microsoft:xbox_one cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One, Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

Nmap scan report for 192.168.1.13
Host is up (0.00072s latency).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:83:69:BC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003, Microsoft Windows XP SP2 or Windows Server 2003 SP2
Network Distance: 1 hop

Nmap scan report for 192.168.1.14
Host is up (0.00066s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:58:E4:C0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.1.15
Host is up (0.00074s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:51:4B:48 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Nmap scan report for 192.168.1.16
Host is up (0.00053s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:64:5A:9F (Oracle VirtualBox virtual NIC)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.1.17
Host is up (0.0012s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:D5:3A:08 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.1.18
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:90:E2:D4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.1.19
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:6B:0C:04 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.1.20
Host is up (0.00094s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:86:7C:57 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003, Microsoft Windows XP SP2 or Windows Server 2003 SP2
Network Distance: 1 hop

Nmap scan report for 192.168.1.21
Host is up (0.00099s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:AE:C0:5F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003, Microsoft Windows XP SP2 or Windows Server 2003 SP2
Network Distance: 1 hop

Nmap scan report for 192.168.1.22
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:AE:E3:8D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003, Microsoft Windows XP SP2 or Windows Server 2003 SP2
Network Distance: 1 hop

Nmap scan report for 192.168.1.23
Host is up (0.0012s latency).
Not shown: 997 closed ports

PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:FF:75:85 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.1.25
Host is up (0.00094s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:5E:07:65 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.1.200
Host is up (0.00086s latency).
Not shown: 994 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE
443/tcp open https
554/tcp open rtsp
902/tcp open iss-realsecure
912/tcp open apex-mesh
10243/tcp open unknown
49156/tcp open unknown
MAC Address: D8:5D:4C:CD:83:34 (Tp-link Technologies)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (19 hosts up) scanned in 117.63 seconds
root@kali:~#

4.8 IDENTIFICACIÓN DE VULNERABILIDADES

Para la identificación de vulnerabilidades se utilizarán los hosts que han sido extraídos del Scanning previamente realizado, teniendo en cuenta que únicamente se puede realizar un análisis de vulnerabilidades de puerto en los hosts que presenten puertos abiertos. Se utiliza la herramienta Nessus, la cual se la puede descargar en su versión Home desde su sitio web. Por ende se utilizará el sistema kali.

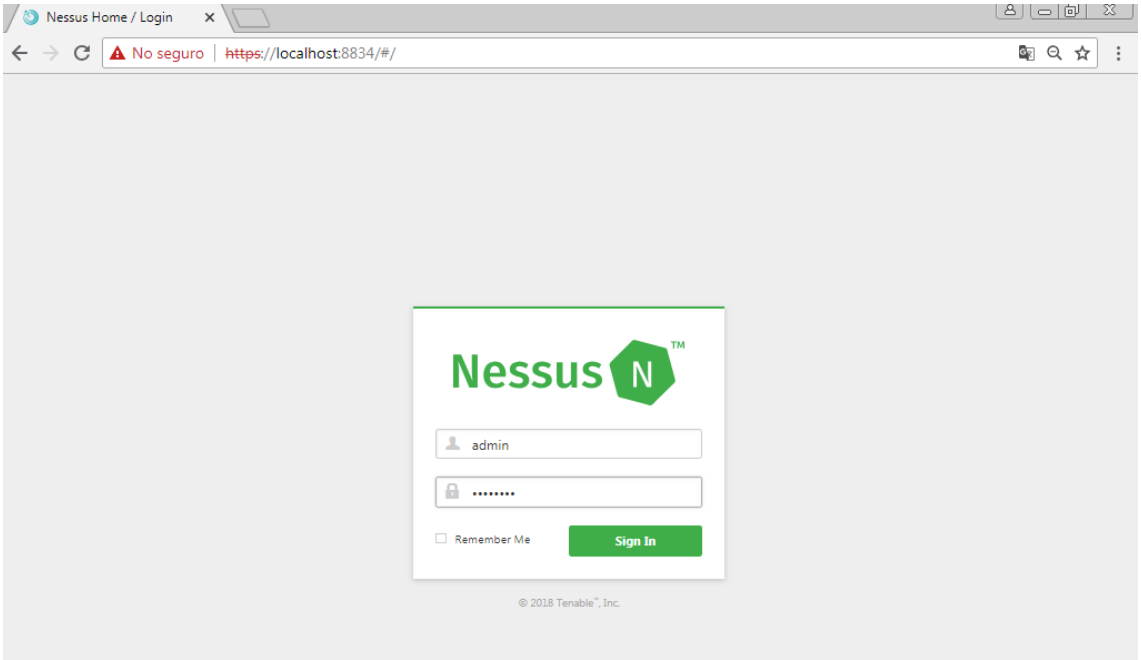


Figura 19: Login en Nessus

A continuación, se seleccionan los plugins a utilizar y la lista q contiene los hosts que serán analizados, se toma como ejemplo la red de datos de la MDH.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

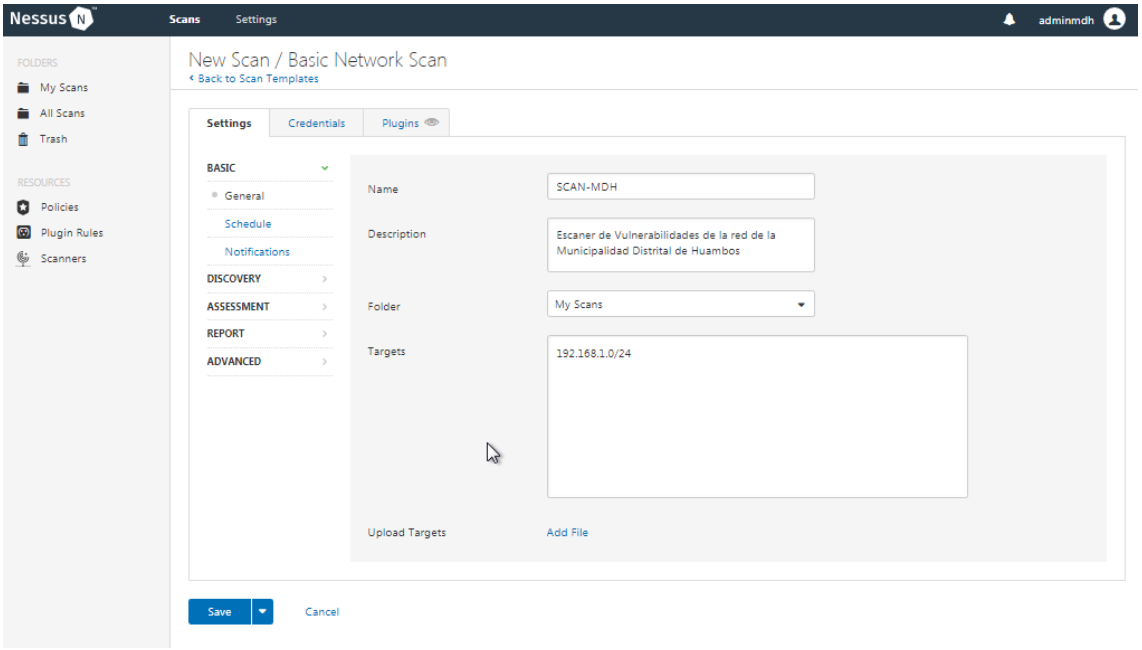


Figura 20: Selección de Hosts y Plugins en Nessus

Iniciamos el proceso de escaneo de vulnerabilidades

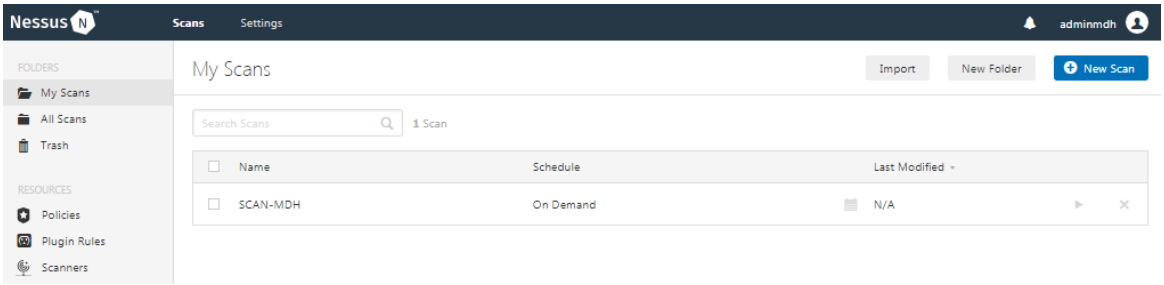


Figura 21: Iniciar el escaneo en Nessus

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Deberemos esperar hasta que el análisis finalice

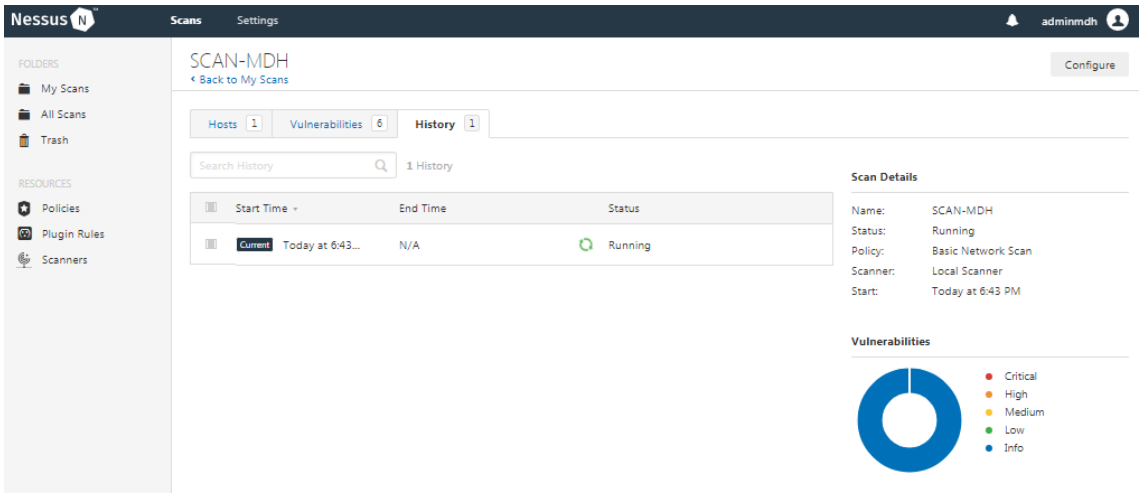


Figura 222: Análisis de vulnerabilidades en curso

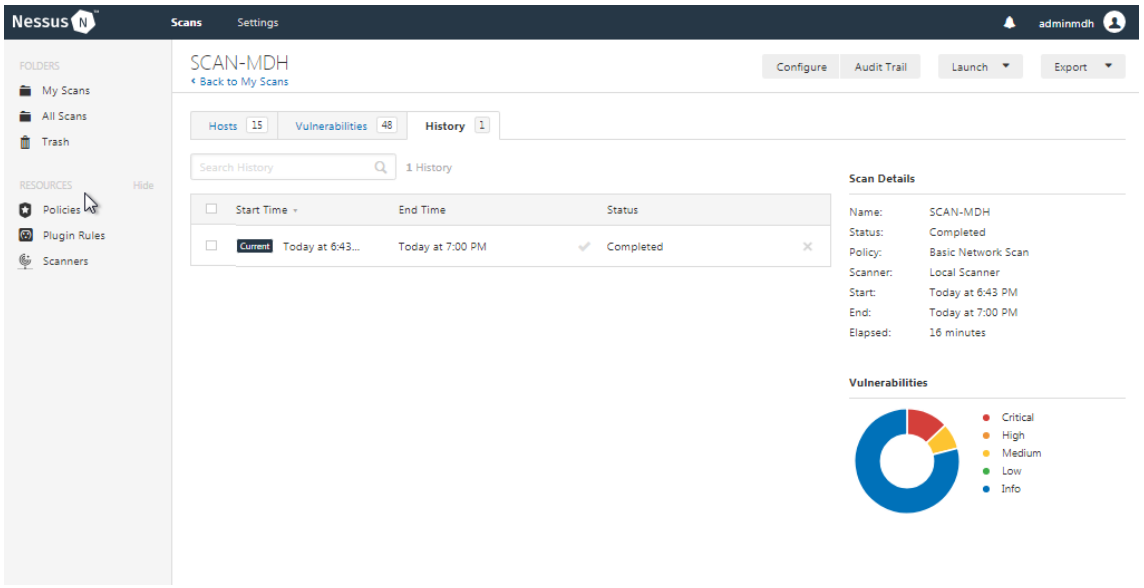


Figura 23: Análisis de vulnerabilidades completo

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

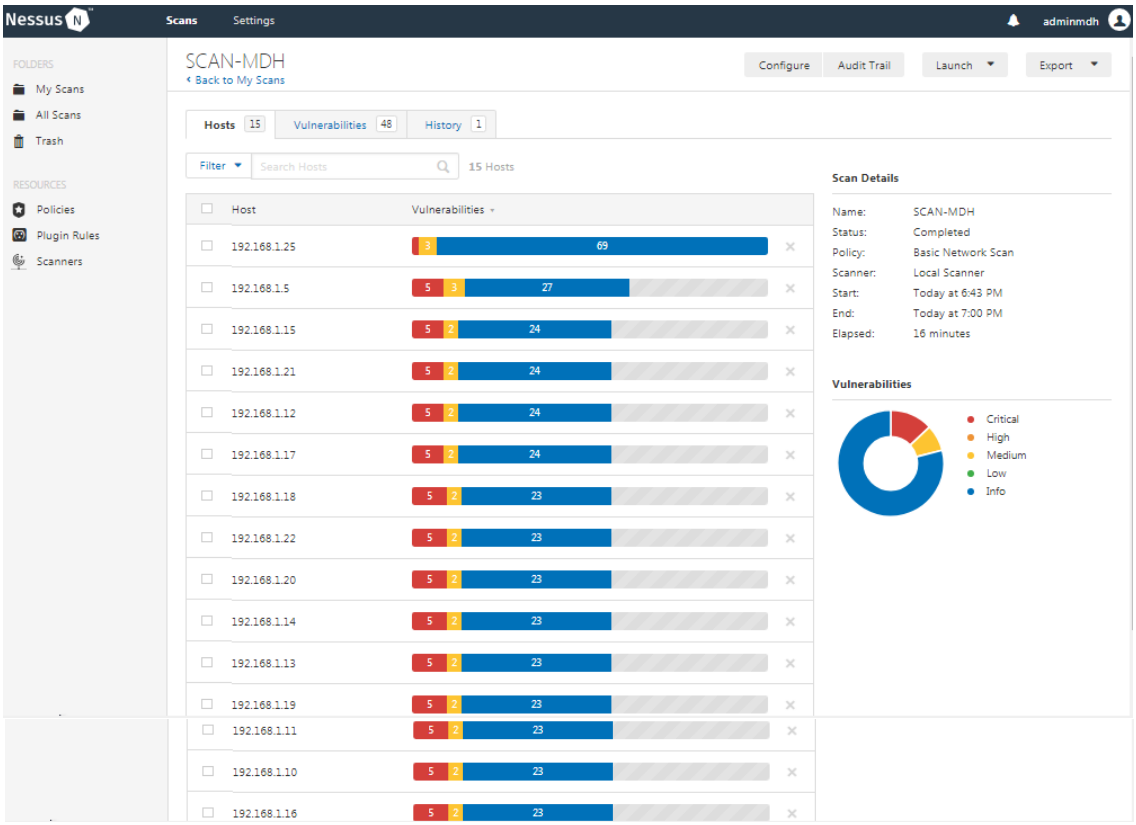


Figura 24: *Análisis de vulnerabilidades en la red de la MDH*

Una vez que el análisis ha finalizado podemos mostrar un resumen de las vulnerabilidades encontradas o a su vez podremos mostrar un informe ejecutivo y un informe técnico en el que nos detallara las mismas.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

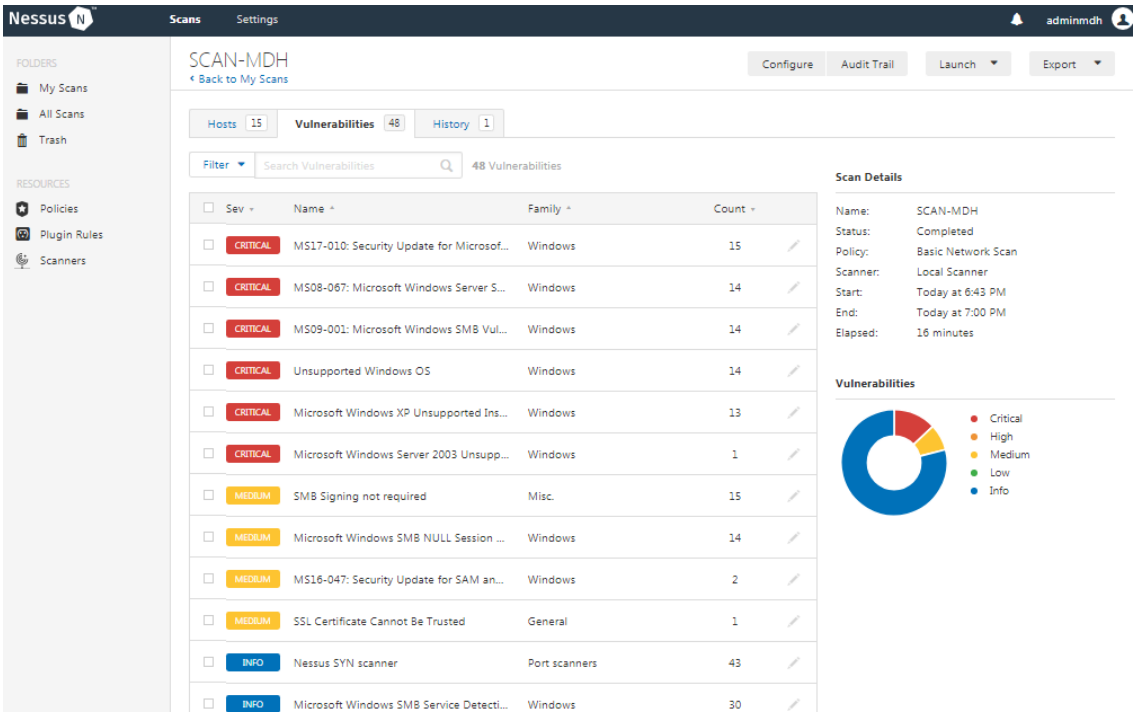


Figura 25: Informe ejecutivo de vulnerabilidades

Como se pudo observar la mayoría de vulnerabilidades críticas pertenecen al servicio SMB de Windows, esto es muy importante al momento de seleccionar el exploit a ejecutar, esto se analizará en la siguiente fase del pentest.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4.9 PENETRACIÓN AL SISTEMA

Una vez que se ha realizado el escaneo de hosts, puertos abiertos, e identificación de vulnerabilidades se procede a explotar dichas vulnerabilidades a fin de ganar acceso desautorizado a los recursos informáticos vulnerables como ejemplo se muestra la vulnerabilidad encontrada en el puerto 445, correspondiente al servicio SMB, **Figura 24**. Esta ha sido descrita como ms08_067_netapi. La cual realiza un buffer overflow en el sistema y permite inyectar código malicioso a través de un payload.

Para explotar dicha vulnerabilidad se utilizar el framework Metasploit, el mismo que se lo puede descargar de manera gratuita, pero con la diferencia de que únicamente cuentas con Exploits mantenidos por la comunidad, si se desea los Exploits privativos, es necesaria la compra de la licencia express.

Se procede a configurar la herramienta como se muestra a continuación:

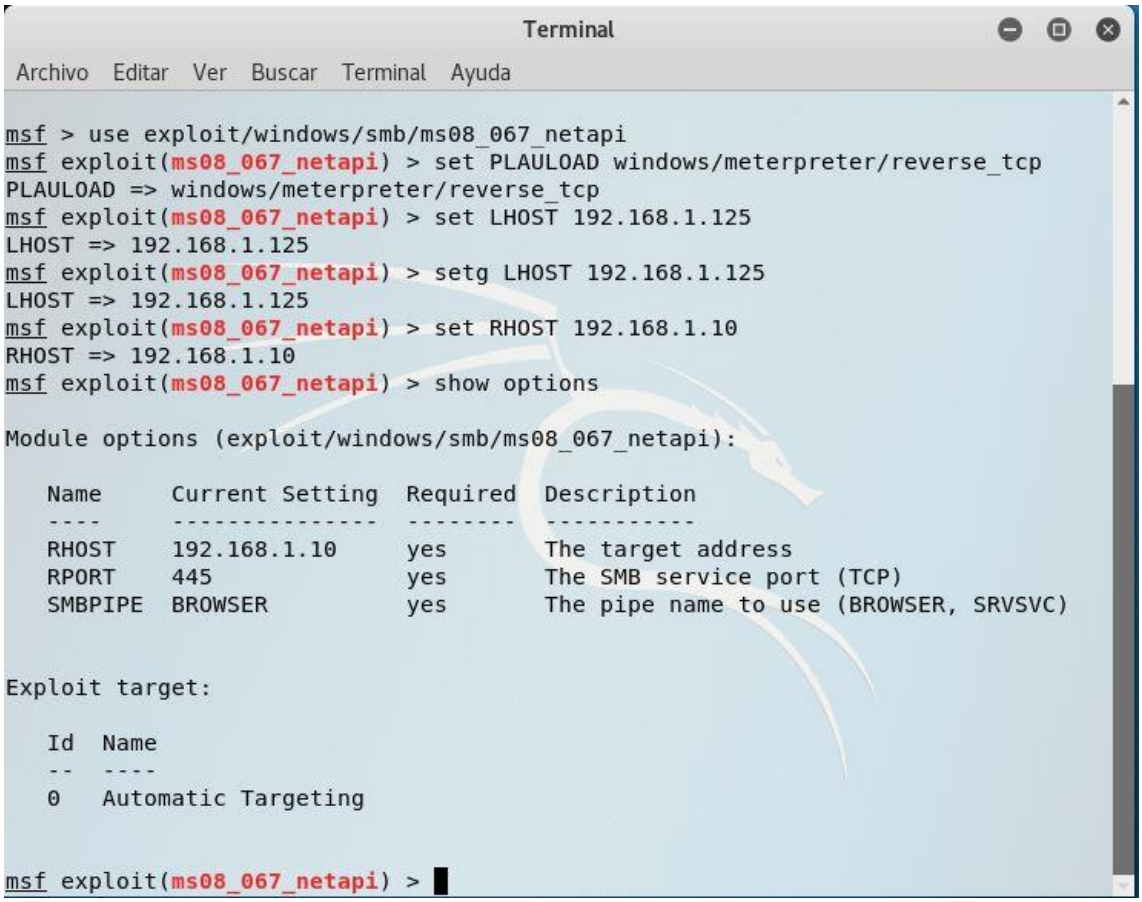


Figura 26: Configuración del exploit ms08_067_netapi

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Una vez que las direcciones IP de origen y destino se encuentran correctamente configuradas, se debe escoger un PAYLOAD que servirá para inyectar el código que posteriormente nos permitirá realizar acciones remotas en la victima a través de simples comandos en el atacante. Si no se escoge un Payload adecuado, es posible que no se pueda obtener una Shell remota en el atacante. La recomendable cuando se trabaja con Metasploit es el famosísimo Payload Meterpreter, comparado como la navaja suiza de los hackers, este es un payload que permite entre otros, capturar la pantalla de las víctimas, mostrar los procesos corriendo en el host, matar los procesos de un antivirus, crear backdoors, subir un keylogger indetectable, entre otras funciones, o si se desea se podría crear un propio ejecutable y enviarlo a través de Meterpreter, como es el caso del famosísimo no, utilizado para crear backdoors a través de un puerto registrado, a continuación se procede a explotar la vulnerabilidad como se detalla:

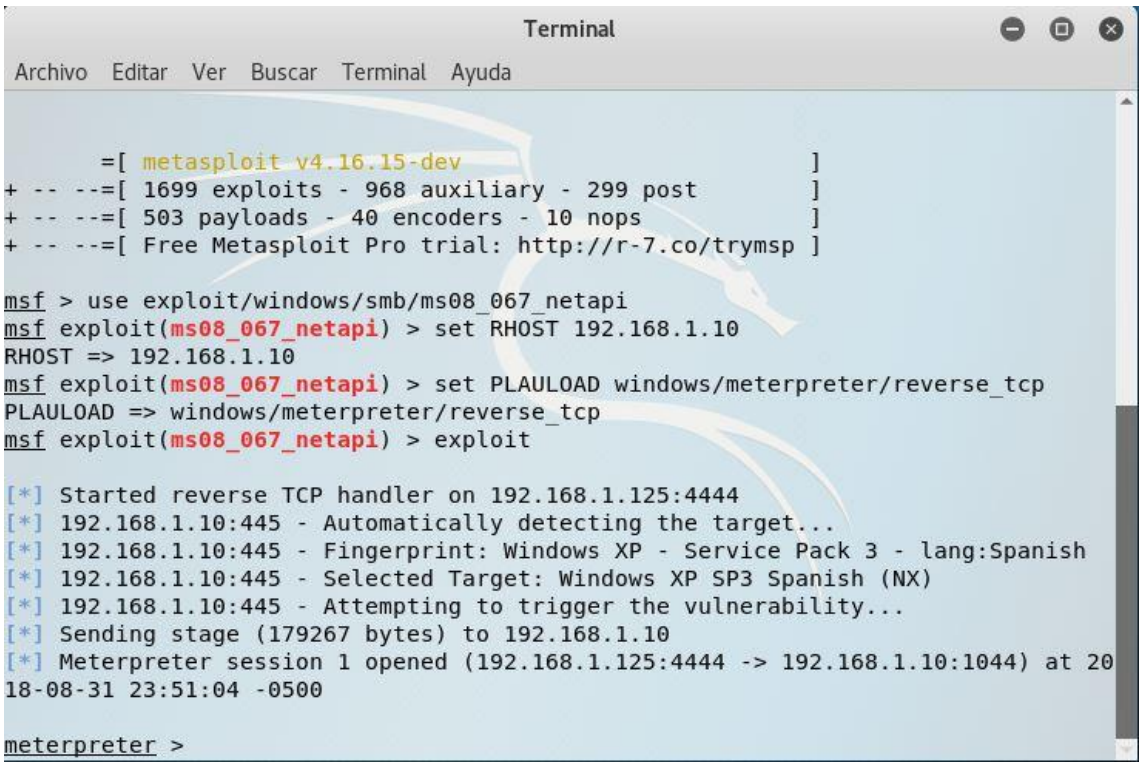


Figura 27: Explotando la vulnerabilidad ms08_067_netapi

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Una vez que se ha comprometido el sistema empezaremos mostrando los procesos q se encuentran corriendo en la victima a través del script psi, posteriormente se inyecta el comando sysinfo a fin de recibir información del SO, hostname y arquitectura

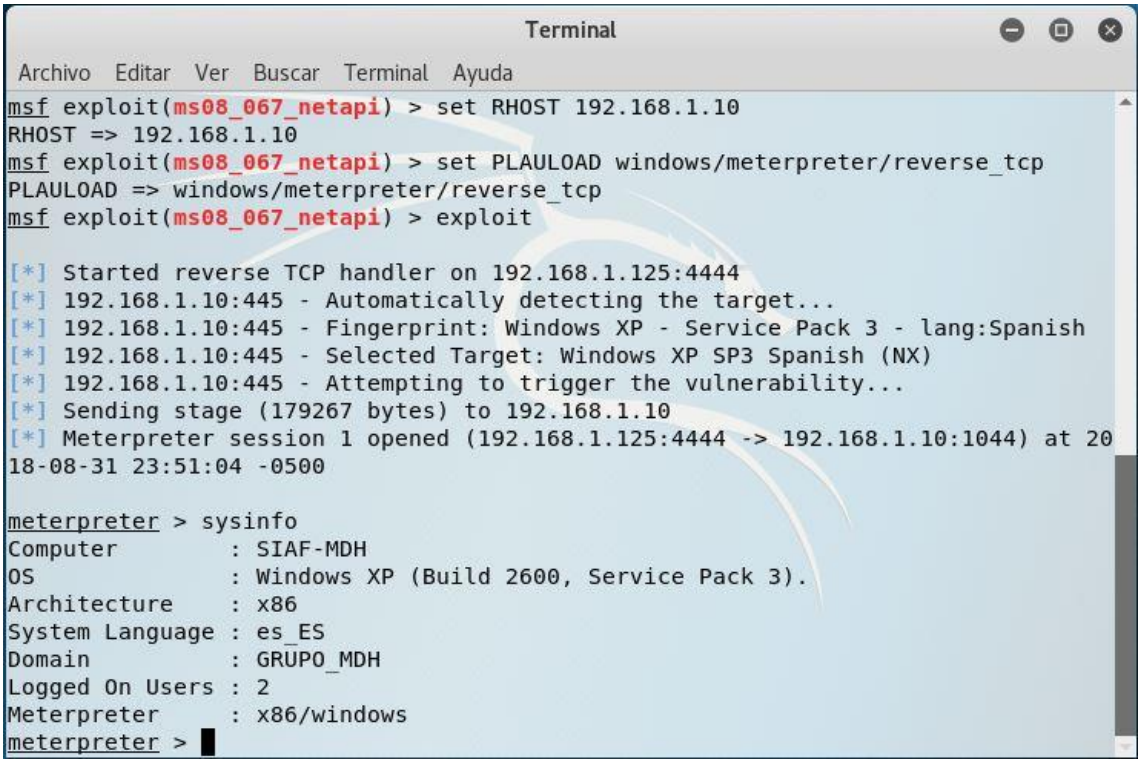


Figura 28: Listado de procesos e información del host comprometido

Inyectando el script screenshot se puede obtener la captura de pantalla del host

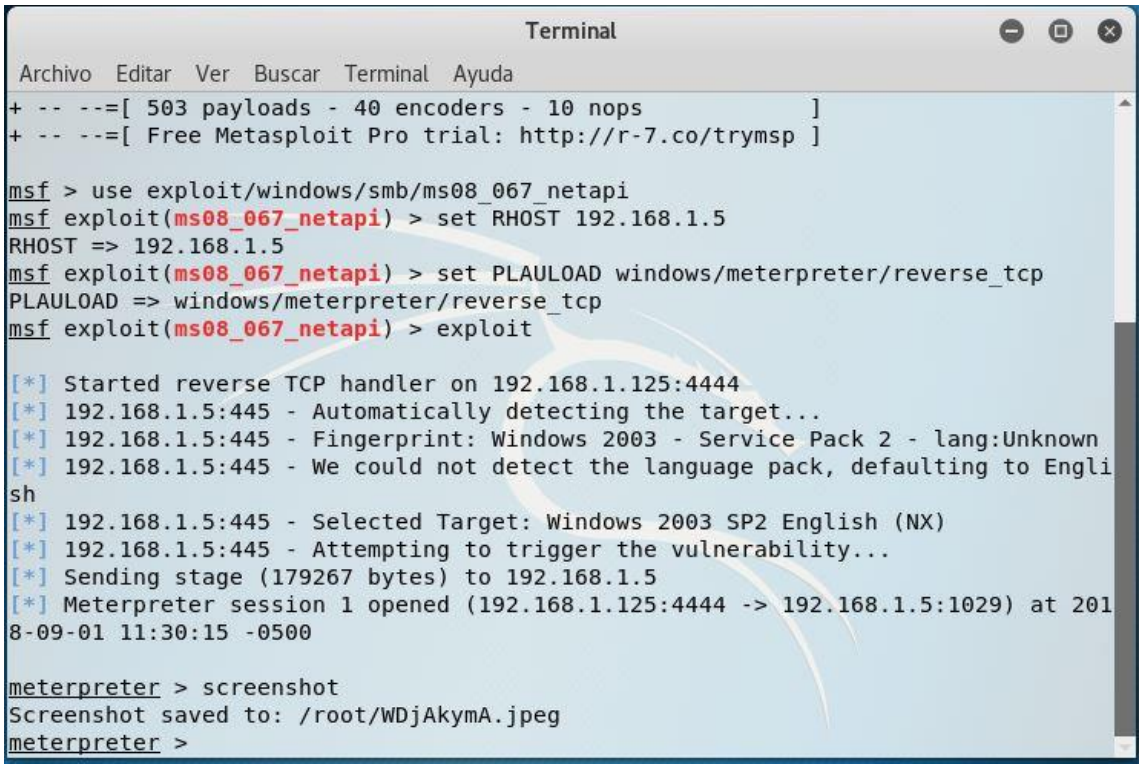


Figura 29: Inyectando el script screenshot

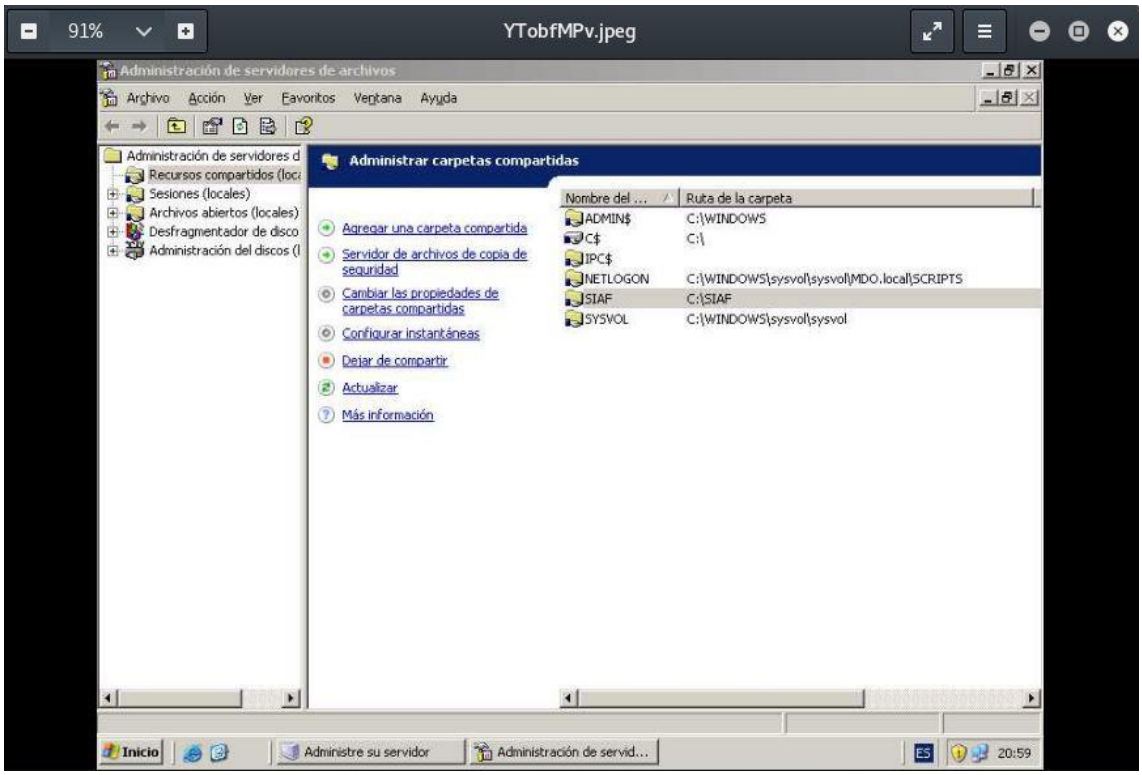


Figura 30: Pantalla capturada remotamente

Inyectando el script run vnc se puede obtener una sesión de vnc en el host

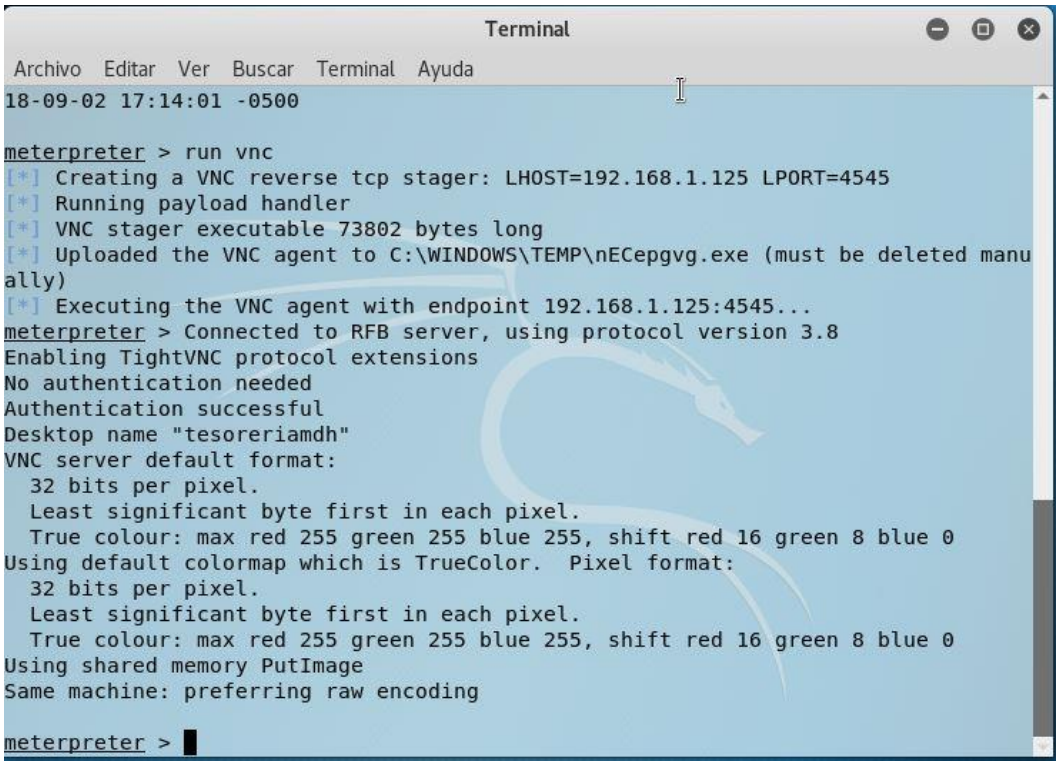


Figura 31: Inyectando el script run VNC

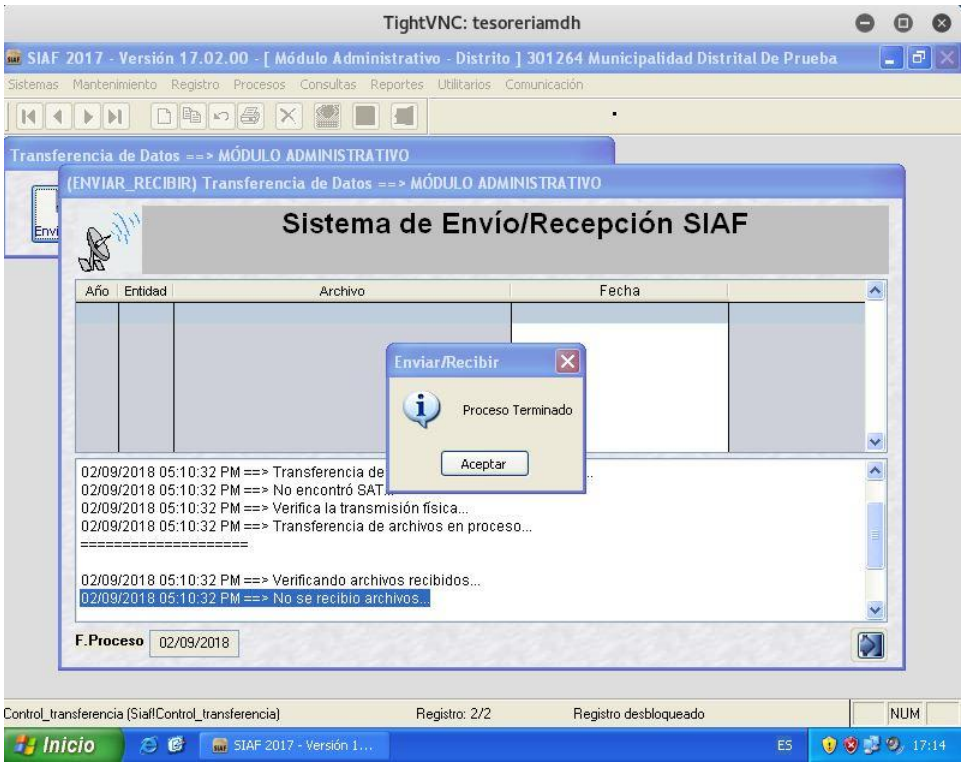


Figura 32: Acceso VNC a la victima

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Con el script run multicommand -cl "msg * Error del Sistema" podemos enviar mensajes a los usuarios de ese host como administrador

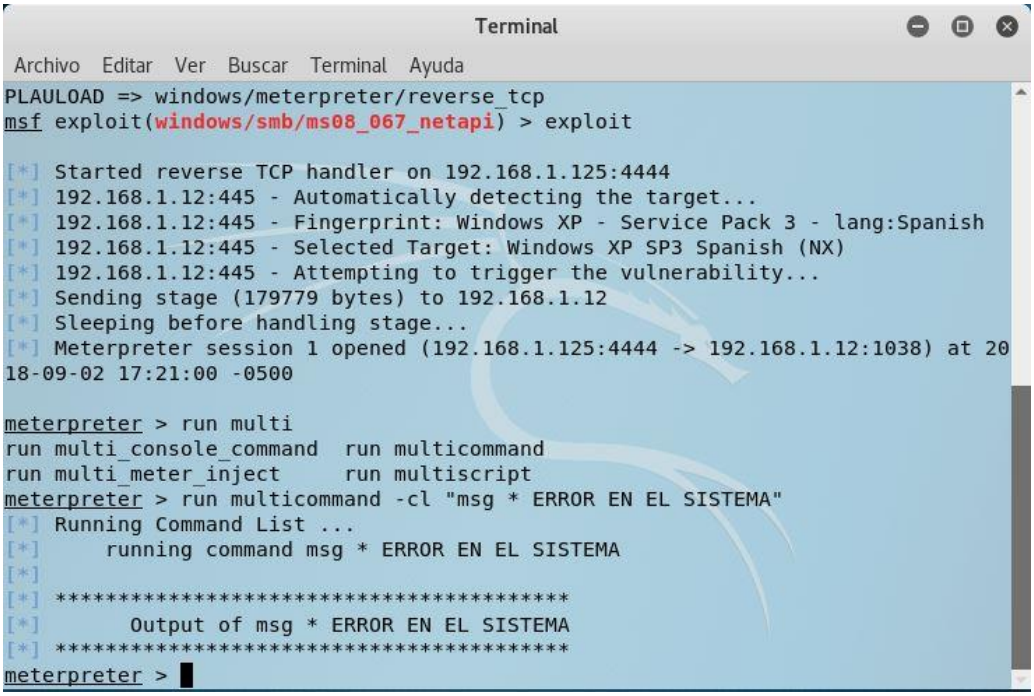


Figura 33: Inyectando el script run multicommand –cl “msg * ERROR DEL SISTEMA”

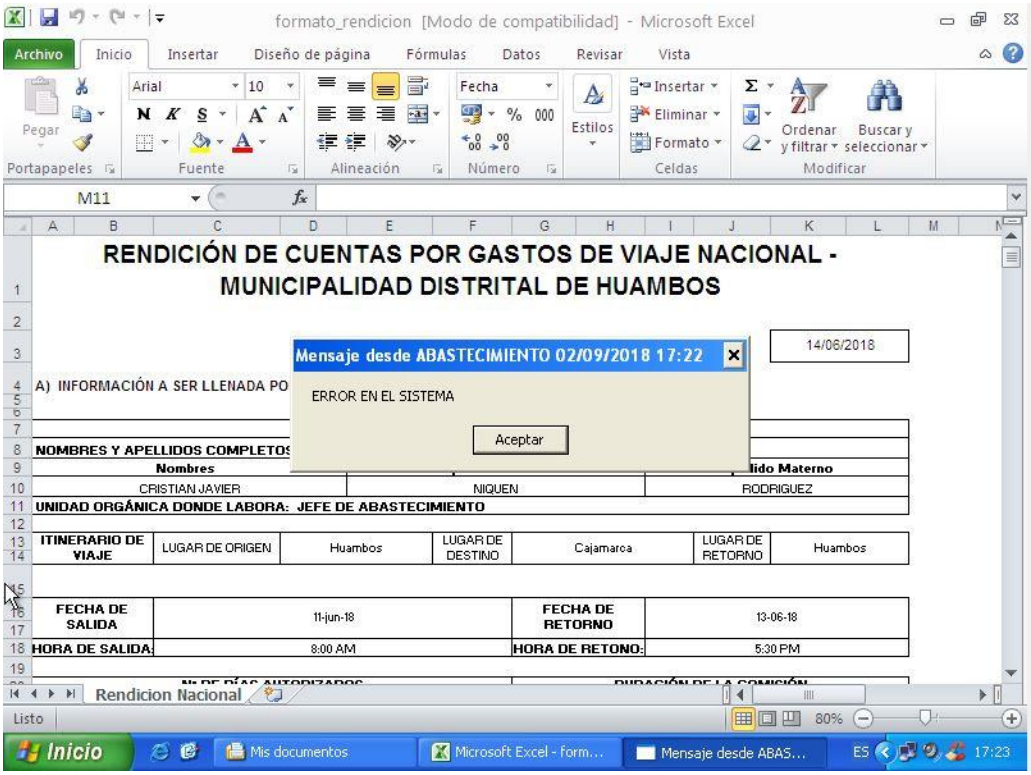


Figura 34: Envío de mensaje vía consola

4.9.1 BORRADO DE HUELLAS

Cabe recalcar que en el presente análisis de vulnerabilidades y hacking ético no es necesaria la realización de la fase de borrador de huellas, puesto que todas las pruebas, accesos y ataques, fueron realizados en un ambiente seguro, bajo la autorización, Administrador de la Red De Datos de la Municipalidad Distrital de Huambos.

4.10 Resultados en tablas y gráficos.

Para la comprobación resultados se muestran las tablas que contienen los datos de las vulnerabilidades encontradas actualmente antes de la implementación de la Honeypot, de los cuales muestran el escaneo generado además de los intentos de ataques informáticos que ha sufrido la red de datos de la Municipalidad Distrital de Huambos, durante los meses de enero, febrero y marzo del 2016.

En el escaneo realizar por el software NESSUS se pudo demostrar que en la población de las computadoras de la Municipalidad Distrital de Huambos se comprobó que el 70 % corresponde a MS09-001 Microsoft Windows SMB Vulnerabilidad, 20 % corresponde a MS08-067 Microsoft Windows Server Service Crafted RPC, y un 10 % corresponde a MS17-010 Security Update for Microsoft Windows SMB Server, todas estas vulneravilidades correspondientes al puerto 445 TCP.

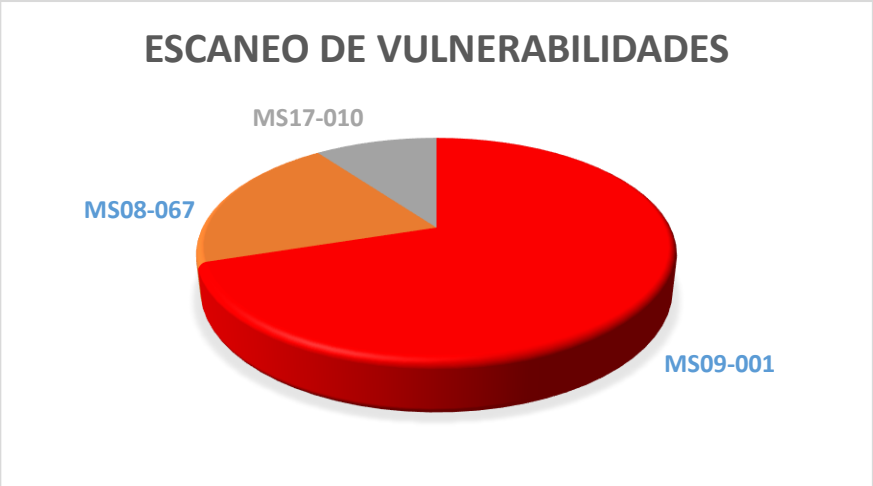


Figura 35: Escaneo de Vulnerabilidades

Luego de haber encontrado las vulnerabilidades en la red de datos de la MDH, se realizaron ataques previamente seleccionados mencionadas en el Capítulo 4, seccion 4.6 Selección de ataques. El cual se empezó a realizar los ataques al servicio SMB Netbios al puerto 445, se realizaron 50 ataques por computadora en la población de 15 computadoras de los cuales se clasifican con el nombre de ataques; scribt sysinfo, script screenshot, script run vnc, script multicommand -cl "msg" y srcrip reboot, en la tabla 5 y figura 36 se muestra los ataques realizados en un computador donde acido atacado 50 veces. Ver Anexo A2

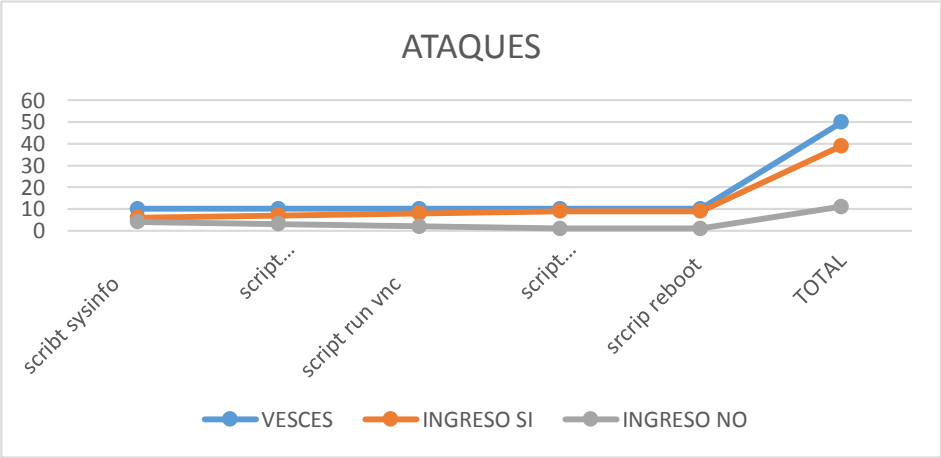


Figura 36: Ataques realizados a un computador

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 01

Computador 01

REGISTRO DE INCIDENCIAS EN LA RED DE DATOS DE LA MDH			
ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	6	4
script screenshot	10	7	3
script run vnc	10	8	2
script multicommand -cl "msg"	10	9	1
srcrip reboot	10	9	1
TOTAL	50	39	11

Tabla 5: Descripción de los ataques realizados a un computador

El resultado 750 pruebas muestra que el 79 % de ataques fueron ejecutados con éxito y un 21 %, fallo por tiempo de espera, entonces esto muestra a la red de datos de la Municipalidad Distrital de Huambos que es muy vulnerable a los ataques y pueden ingresar sin problema alguno. Ver Figura 37 y 38. Ver el Anexo 2

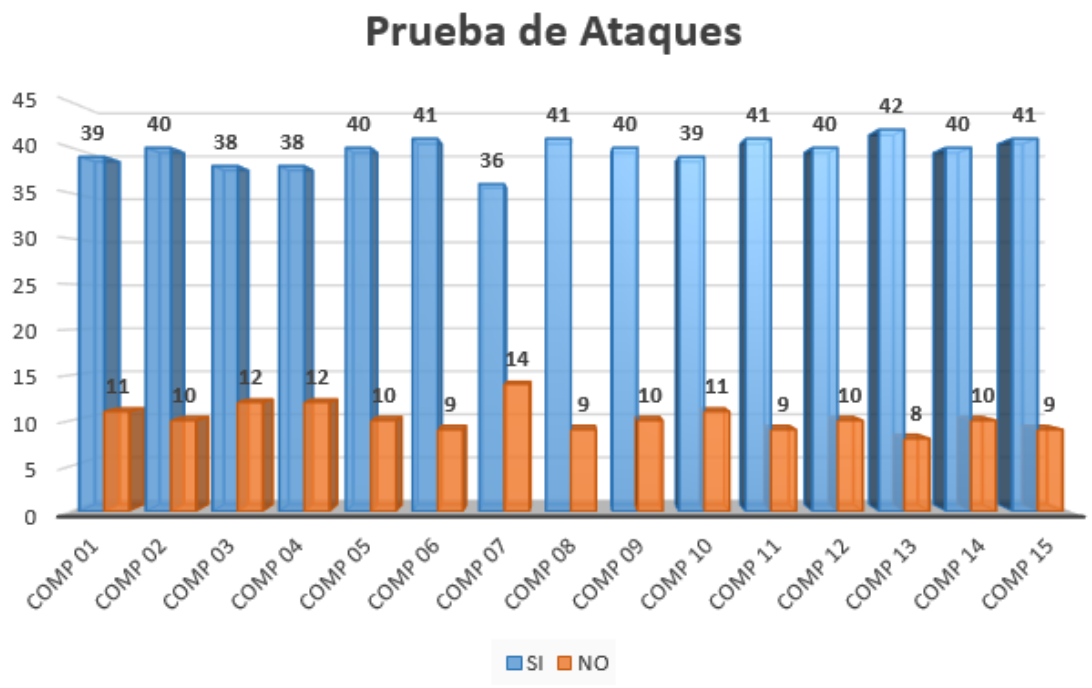


Figura 37: Veces de ingreso

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Figura 38: Veces de ingreso

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO V: PROPUESTA DE INVESTIGACION

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.1 Requerimientos de la solución

La presente tesis busca implementar la red Honeypots llamada Honeynet en la Municipalidad de Huambos.

Para que la solución propuesta cumpla con los objetivos deben cumplir con los siguientes requisitos:

Requisitos de las Honeynet

La Honeynet debe tener las siguientes características:

- **a)** Control de datos.
- **b)** Captura de datos.
- **c)** Análisis de datos.
- **d)** Recolección de datos

Requisitos de nuestra Honeynets

Uno de los objetivos que tiene la Honeynet es copiar todo lo posible a la red de producción a la que se conecta, con la diferencia que se conservarán los costos bajos y para poder lograrlo se deben considerar tecnologías como la visualización de sistemas.

Requisitos de Red

Adicionalmente a las medidas de Control de Datos brindadas por el Honeywall, todo el tráfico de red creados por nuestras Honeynet debe pasar por un dispositivo (switch), el cual puede ser desactivado por el administrador de red en caso de emergencia.

Para que los honeypots dentro de la Honeynet puedan ser observados a nivel mundial, cada uno debe ser configurado con una IP pública, la cual debe existir dentro del mismo rango de red de la LAN a la que pertenece.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Las IPs públicas deben ser brindadas por los administradores de red de la MDH, asimismo, las IPs obtenidas deben tener habilitados los puertos principales de TCP, UDP, hasta los que no son tradicionales y que son utilizados para ataques lo cual maximizará la efectividad de los datos obtenidos y la interacción con los atacantes.

Conjuntamente, se debe tener un acceso físico o virtual hacia la red de la municipalidad.

Requisitos de Hardware

La solución necesita los siguientes dispositivos de hardware:

Dos redes de computadoras constituidas opcionalmente por un switch o hub, cada red de computadoras pertenece a una de las Honeynet a implementar, y cada computador a un Honeypot.

Dos computadores para que hagan el papel de Honeywall en cada Honeynet, y que cada uno cuente con tres tarjetas de red. Además, se debe tener en cuenta que los datos obtenidos y el tiempo de recolección pueden requerir gran capacidad de almacenamiento. Por esta razón es necesario tener discos duros adicionales o uno con capacidad mínima de 120 GB.

5.2 Estudio de las arquitecturas y selección de la más apropiada

En la Municipalidad de Huambos se implementarán Honeynets de tercera Generación, ya que es la generación más segura, estable y se encuentra vigente como herramienta de análisis.

Se debe optar por un tipo de Honeynet de tercera generación que se va a implementar en la red. Con relación a la arquitectura de la Honeynet tenemos dos tipos para los que optar:

a) Implementar una Honeynet con las mismas exigencias de hardware que una red de computadores de producción, en la cual todos sus equipos son físicos y reales.

b) Aplicar una Honeynet Virtual, virtualizando sistemas operativos o servicios en un solo equipo o en varios.

Por las razones ya planteadas y en base al análisis de los tipos de Honeynet, en el cual se han mostrado las ventajas y desventajas de usar soluciones virtuales para el desarrollo de las Honeynet y teniendo en cuenta que ninguna de las desventajas atentan con la calidad de la solución, debido a que todas son a nivel de seguridad y pueden ser controladas con un mantenimiento periódico de la Honeynet y con la elección de una buena herramienta de virtualización, se ha decidido usar Honeynets Virtuales para el desarrollo de la Honeynet pronosticada para esta tesis.

Dentro de las Honeynet Virtuales existen dos opciones para elegir:

a) Honeynet virtual auto-contenida.

b) Honeynet virtual híbrida.

Para poder optar por una se deben considerar las diferencias principales entre ambas Honeynets virtuales las cuales son el número de equipos que usan, la portabilidad y la facilidad en la administración.

Se definirá la solución como:

a. Honeynet MUNIHUAMBOS: Virtual auto-contenida.

A continuación, listaremos los equipos que están disponibles para el desarrollo de la presente tesis para poder establecer la arquitectura en la que serán usados de acuerdo con sus características.

Hardware disponible

Se dispone de los siguientes equipos:

- Computadores de escritorios clones
- 1 Router switch de 4 puertos
- 4 Tarjetas de red PCI 10/100
- 2 Laptops LENOVO ThinkPad E470 de uso personal

Características de las computadoras disponibles

Para poder establecer en qué Honeynet será colocado cada equipo se deben analizar sus características. Se usarán tres computadores de escritorio con las siguientes características:

a) Computador A: Core i3, 4 GB RAM, 500 GB disco duro, 1 puerto de red 10/100/1000
b) Computador B: Core i3, 4 GB RAM, 500 GB disco duro, 1 puerto de red 10/1000
c) Computador C Core i3, 4 GB RAM, 500 GB disco duro, 3 puertos de red 10/1000

El Computador A puede levantar un mayor número de máquinas virtuales ya que tiene las mejores características en procesamiento, memoria, y espacio de disco, haciéndolo candidato perfecto para formar parte de la Honeynet MUNIHUAMBOS. En la Figura 1.1. se puede observar cómo quedaría un modelo preliminar de la arquitectura para esta Honeynet.

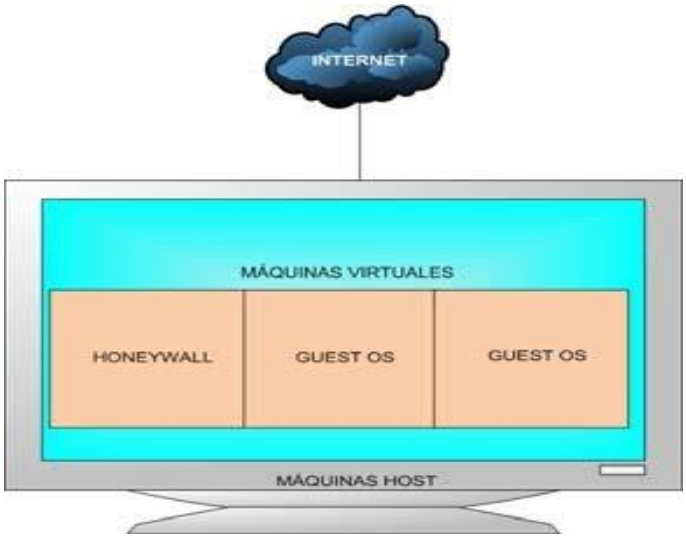


Figura 39: Honeynet Virtual auto-contenida

Con esta disposición de equipos el router-swicth no entraría en nuestra solución. Las cuatro tarjetas de red PCI serán colocadas en los Honeywall de cada red. Las dos Laptops HP de uso personal serán usadas para tareas de administración y almacenamiento de datos recogidos por los Honeywall.

5.3 Análisis de las herramientas

Cada Honeypot levantará sistemas operativos con sus servicios de acuerdo con la red que se esté emulando. De acuerdo con ello se ha obtenido:

a. Sistemas Operativos Linux edición de Servidor y edición de escritorio, con los servicios levantados como: ftp, ssh, http, etc.
b. Sistema Operativo Windows XP con servicios levantados como: ftp, telnet, http.

5.3.1. Herramientas de Captura de la Honeynet

La función principal de esta herramienta es el Honeywall, el cual tendrá una distribución de Linux ROO 1.4 basada en CentOS, la que es una herramienta para el desarrollo de Honeynets.

Entre otras herramientas de captura instaladas en los Honeypots están: Sebek cliente, Nepenthes. Estas herramientas se analizarán en detalla a continuación:

ROO 1.4

ROO v1.4 (FORMATO: **roo-1.4.hw-20080424215740.iso**) basada en Centos.

El Honeywall CD-ROM ROO es un CD que contiene todas las herramientas útiles para crear y administrar un Honeywall de tercera generación. Es un CD auto ejecutable que se basa en la distribución de Linux Centos que instala las herramientas para poder levantar y administrar el Honeywall y desde su última versión contiene una herramienta de análisis de datos.

Componentes del Honeywall Roo V1.4

En la tabla 03 se detallarán los componentes del Honeywall.

Componentes	Descripción
Snort	Es un sistema de detección de intrusos basado en reglas, es capaz de hacer un análisis del tráfico de la red en tiempo real y al mismo tiempo registrar paquetes de redes IP.
Snort_inline	Es la versión modificada del Snort el cual toma decisiones sobre el tráfico saliente, con la condición de que tenga ataques conocidos.
Session Limit	Control de límite de sesiones.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Sebek	Es una herramienta de captura de datos diseñada para atrapar al atacante sobre las actividades de un Honeypot.
Walleye	Brinda al administrador herramientas de análisis de datos. Estos tienen acceso a todos los datos capturados por snort-inline y Sebek, los cuales incluyen la dirección IP, datos transferidos y acciones de los atacantes en los Honeypots. Walleye es ejecutado en un servidor web (apache) el cual es instalado con la distribución de ROO.
Pcap	Interfaz de captura de datos del kernel de Linux.
Iptables	Firewall de Linux integrado en el kernel, se usa para limitar los paquetes en el control de datos y llevar un registro de los datos en la captura de datos.
Swatch	Esta herramienta comunica al administrador, a través de un correo electrónico, en caso suceda un incidente.
Argus + Hflow	Información de flujos de tráfico y relaciones.
Menú	Interfaz gráfica que se usa para el mantenimiento y control de la Honeynet
Mysql	Es un servidor de base de datos que se usa para almacenar y relacionar el contenido capturado.

Tabla 6: componentes del Honeywall.

5.3.2 Sebek

Sebek es una herramienta que obtiene datos y está diseñada para capturar la actividad de los atacantes en los Honeypots. Esta herramienta es una solución

que está conformada por dos componentes, un cliente y un servidor. El Sebek cliente es instalado y ejecutado en los Honeypots, es el que se encarga de obtener todas las actividades de los atacantes (pulsaciones de teclado, carga de archivos, contraseñas), estos datos captados no se almacenan localmente ya que esto revelaría al atacante que su actividad es monitoreada. Los datos son enviados de forma oculta al servidor Sebek, el cual se encarga de recoger los datos y almacenarlos en un repositorio central. El servidor Sebek puede estar ubicado en el mismo Honeywall o en un servidor remoto.

Nepenthes

Nepenthes es una opción de Honeypot virtual de baja interacción, la cual se encarga de recolectar malware de forma automática.

Trabaja emulando las vulnerabilidades en servidores de red. Este reduce el riesgo en un Honeypot comprometido, a diferencia de un honeypot normal que solo levanta los servicios de red.

Ya que el proceso de ataque es una emulación, es más práctico para los ataques anónimos. El objetivo del Nepenthes es recolectar y descargar la herramienta usada para realizar el ataque, esencialmente gusanos, que luego se podrán usar para realizar un análisis del mismo.

El malware es descargado al disco duro del Honeypot pero no es ejecutado.

Nepenthes corre bajo Linux, pero busca vulnerabilidades de Windows y los gusanos principales son ejecutables para Windows. De esta manera se tiene un Honeypot para recolectar malwares para Windows sin ser comprometidos en el proceso.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.4 IMPLEMENTACIÓN DE LAS HONEYNETS EN LAS REDES DE DATOS DE LA MUNICIPALIDAD DE HUAMBOS

5.4.1. Implementación de la Honeynet – MUNIHUAMBOS

Hardware

Para elaborar la Honeynet virtual auto-contenida dentro de la red de la MUNIHUAMBOS se necesita un computador con las siguientes características:

Procesador Core i5 2.5 GHz

Memoria RAM de 4 GB

Disco duro de 500 GB

Tarjeta de Red de 10/100/1000 Mbps

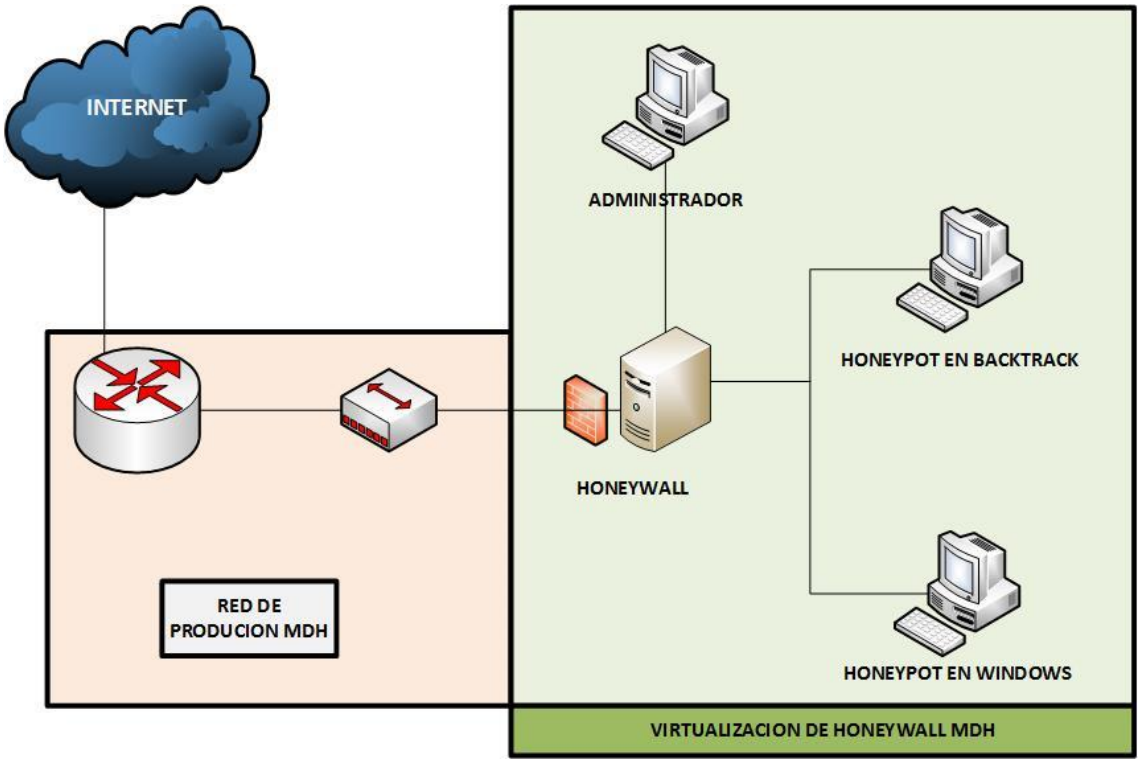


Figura 40: Honeynet virtual auto-contenida en la red MUNIHUAMBOS

Los dispositivos virtuales que serán levantados elaborarán una red virtual dentro de la máquina host, y se configurarán con los requerimientos de hardware que serán detallados en la tabla 1.2.

Sistema Operativo(s)	Disco Duro (s)	Memoria (s)

Windows Xp SP3	100 GB	2048 MB
BackTrack Linux 7	100 GB	2048 MB
Honeywall (Roo V1.4)	100 GB	2048 MB

***Tabla 7*:** Sistemas operativos

5.5 Configuración de la red

En el diagrama de red de la figura 37, se muestra la Honeynet de la MUNIHUAMBOS con sus componentes físicos y virtuales necesarios.

Solo una máquina física se encuentra conectada directamente al switch, conjuntamente a la red de producción, y cuenta con una distribución Linux Fedora 8 y un software VirutalBox que es usado para levantar 3 máquinas rque se usan en la Honeywall.

La máquina virtual Honeywall usa tres diferentes interfaces virtuales de red: (una en solo-anfitrión y dos Adaptador puente), los Honeypots emplean cada uno una interfaz de red.

El modo solo-anfitrión ayuda a interconectar máquinas virtuales entre sí, así como también el sistema que las contiene, estableciendo una red privada interna separada del resto de la red externa.

En Adaptador puente está relacionado con una interfaz física de red del sistema host por la cual las máquinas virtuales usan su propia IP, les da acceso y pertenecer al mismo segmento de red a la cual está conectada la máquina que la contiene.

La arquitectura y la configuración de la red está detallada en la Figura 38 que muestra una máquina física (Host) junto a la red de producción conectada directamente al switch, la cual contendrá las máquinas virtuales Honeypots y también el Honeywall.

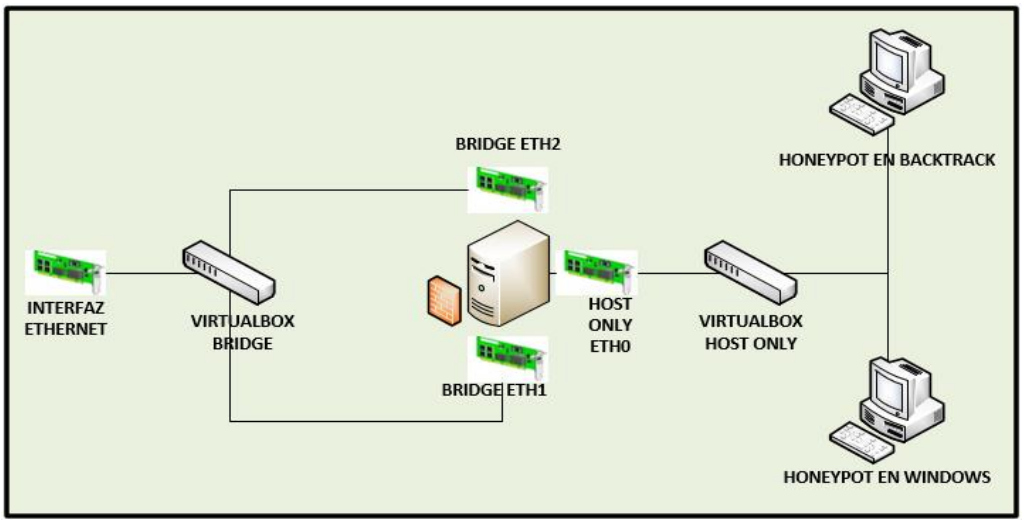


Figura 41: Diagrama lógico de Honeynet virtual auto-contenida
Fuente: ANHMB

En la Figura 15, se puede observar la configuración de un diagrama lógico de la orientación de las máquinas virtuales y cómo los Honeypots se conectan por medio del Honeywall a la red externa, usando el modo host-only, el cual obliga a elaborar una red entre el Honeywall y los Honeypots dándole el paso de los paquetes a través del Honeywall. Si se usara el modo bridge para las interfaces de red de los Honeypots, estos estarían conectados hacia la red externa, sin embargo, sus paquetes no serían registrados ni atravesarían el Honeywall.

La máquina virtual Honeywall tiene tres interfaces de red, dos en modo bridge para unirse directamente con la red externa y darle un uso administrativo, y una en modo host-only que le brinda una conexión directa con las interfaces de red (host-only) de los Honeypots.

Las interfaces de red en modo bridge y host-only en el Honeywall pertenecen al enlace de la red externa con los Honeypots. El Honeywall funciona como un bridge de capa 2, diseñando sus interfaces de red como "bridge".

No se debe que confundir el "modo bridge" utilizado para crear un dispositivo virtual de red en Virtualbox el cual pertenece al nombre de las propiedades de

conexión entre las tarjetas en un entorno Virtualbox. Como vemos en este caso, hay dos tarjetas en el Honeywall, una utiliza el “modo bridge”para obtener una conexión directa con la interface de red de la maquina Host y la otra tarjeta utiliza el “modo host-only” para lograr una conexión virtual con el resto de tarjetas en “modo host-only”dentro de la red virtual.

Esta configuración pertenece sólo a la conexión administrada por el Virtualbox. Hablando de configuraciones dentro del Sistema Operativo, el kernel del Honeywall utilizará ambas tarjetas como bridge.

Detalle de las interfaces de red: donde se muestra la configuración de las tres tarjetas de red “eth”

Eth0: Adaptador solo-anfitrión

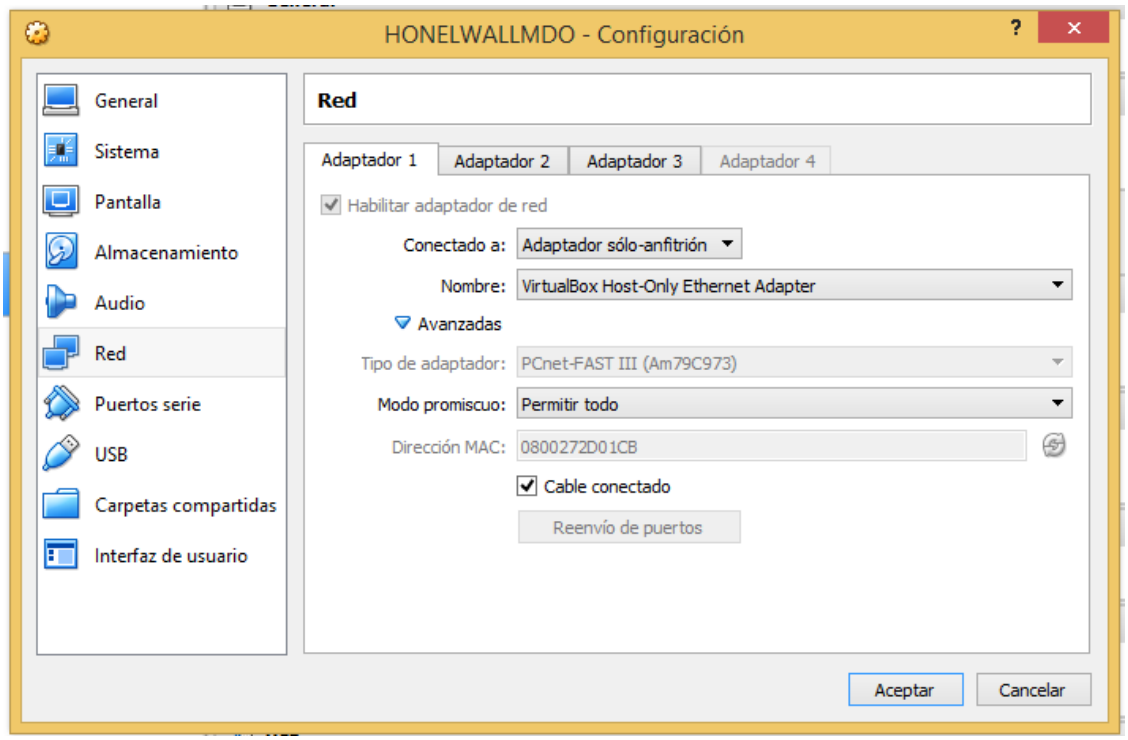


Figura 42: adaptador eth0

Eth1: Adaptador puente

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

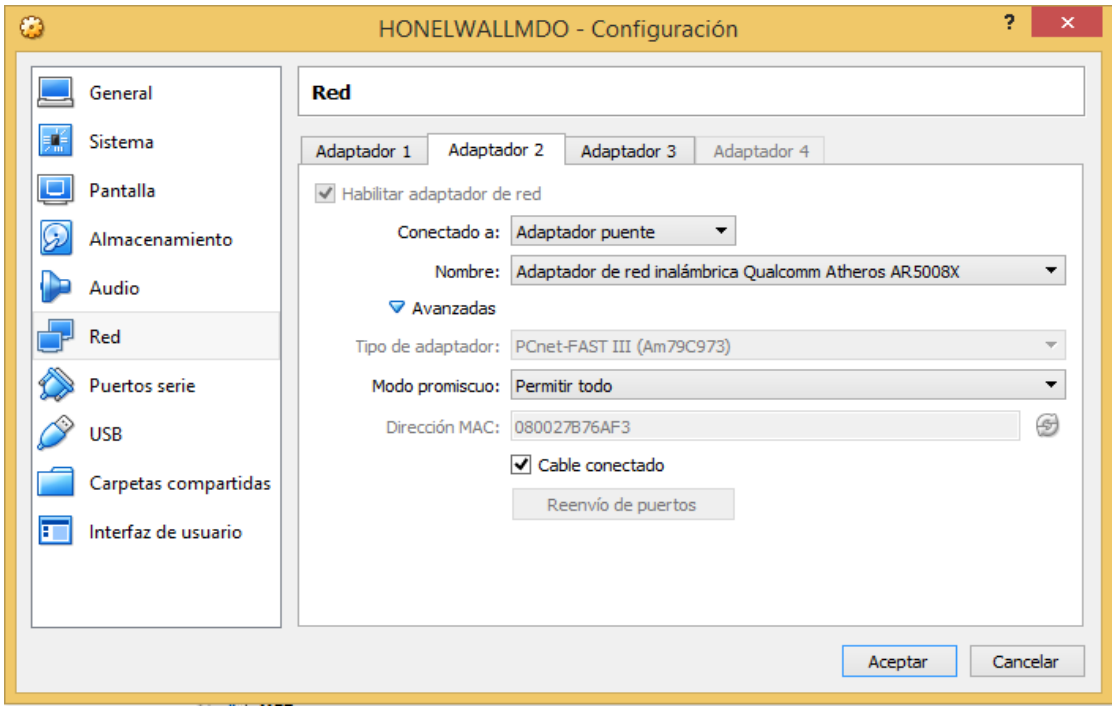


Figura 43: Adaptador eth1

Fuente: ANHMB

Eth2: Adaptador puente

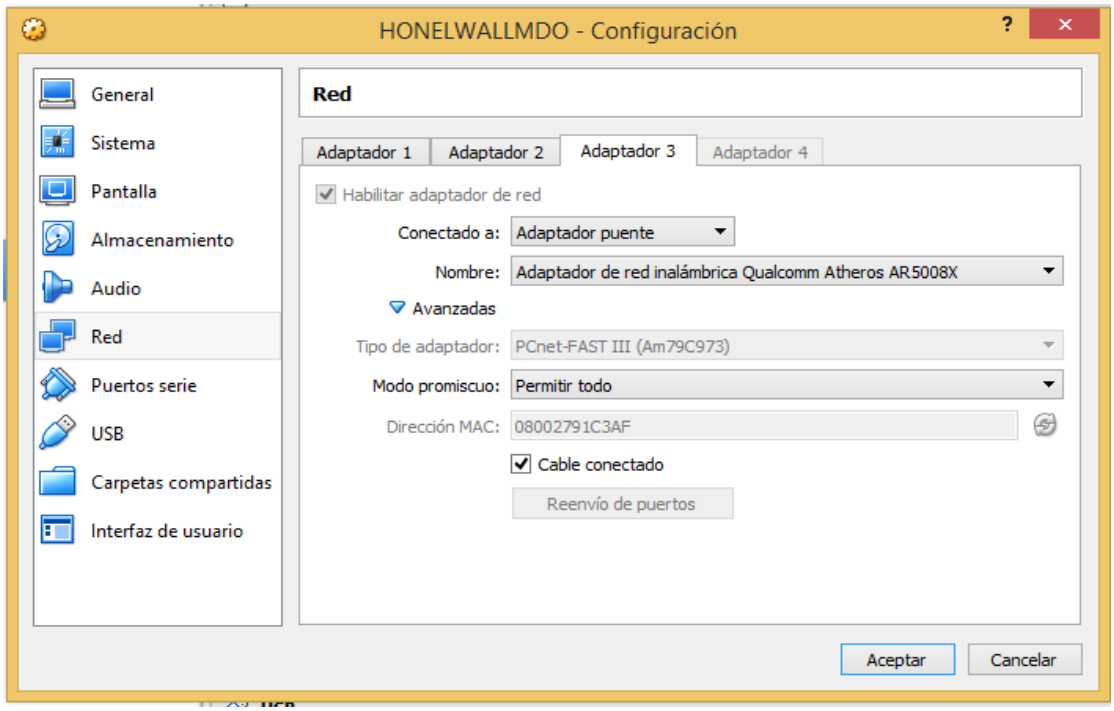


Figura 44: adaptador eth2

Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

En la Tabla 06. y 07., se detallará la configuración de red que utilizan para ambos Honeypots:

COMPUTADOR:	**HONEYPOT**
IP Adress:	192.168.1.20
Subnet Mask:	255.255.255.0/24
Gateway:	192.168.1.1
Broadcast:	192.168.1.255
IP Network:	192.168.1.0
SO Base	CentOS
Card	Eth0

***Tabla 8*:** Configuración de Honeypot
Fuente: ANHMB

COMPUTADOR:	**Honeywall Salida Internet / Red Local**
IP Adress:	192.168.1.21
Subnet Mask:	255.255.255.0/24
Gateway:	192.168.1.1
SO Base	Linux/Windows
Card	Eth1
COMPUTADOR	**Honeywall Administrador**
IP Adress:	192.168.1.3
Subnet Mask:	255.255.255.0/24
Gateway:	192.168.1.1
SO Base	Windows
Card	Eth2

***Tabla 9*:** Configuración de Honeypot
Fuente: ANHMB

5.6 Instalación y configuración del Honeywall

El software de virtualización que se utilizará para la creación de las máquinas virtuales es VirtualBox, este debe estar instalado y configurado adecuadamente en todas las computadoras que levantarán máquinas virtuales.

En primer lugar, se creará una máquina virtual Honeywall utilizando VirtualBox y será configurada con las exigencias de hardware (memoria y disco) que están establecidos en la Tabla 5. Se deberá cambiar el tipo de disco duro virtual a IDE, de lo contrario no podrá soportar el sistema que se instalará, el cual se basa en Centos.

Luego, se adicionarán dos tarjetas de red adicionales (de tal manera que eth0 y eth2 enten en modo bridge y eth1 en modo host-only), como se muestra en la **Figura 45**

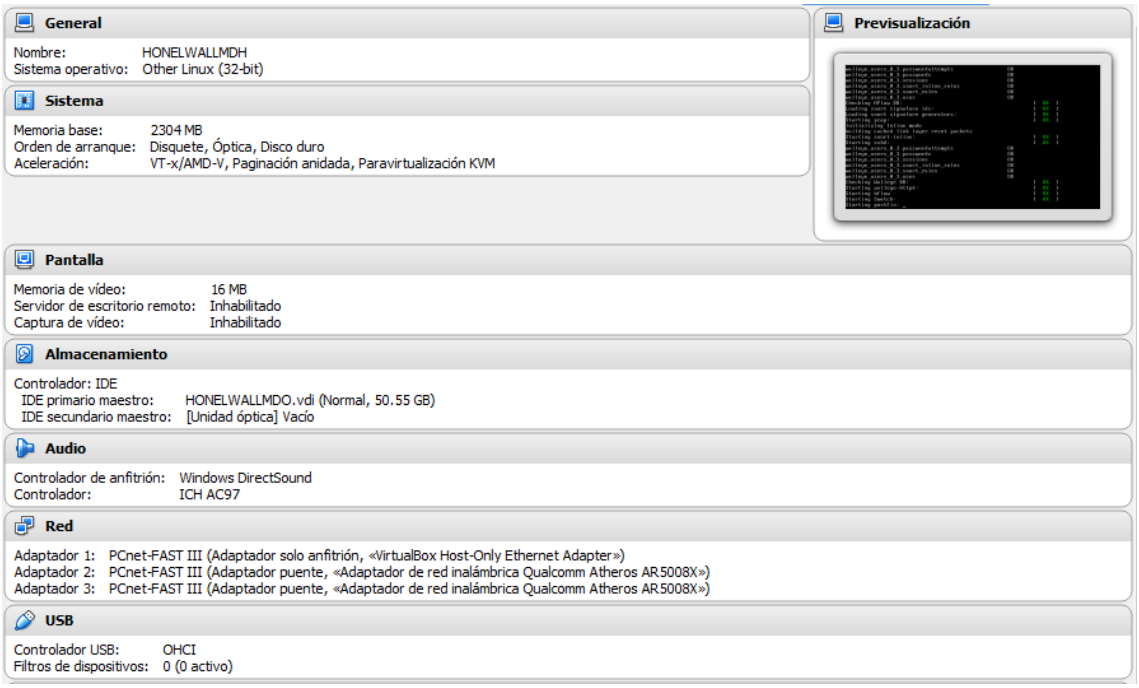


Figura 45: Diagrama lógico de Honeynet virtual auto - contenida
Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.7 Instalación y configuración del CD-ROM Honeywall en la máquina virtual

La versión del Honeywall que se utilizará es <<roo-1.4.hw-20090425114542.iso >>, la cual está disponible en el sitio web www.honeynet.org. Instalación y configuración detallada ver **Anexo A1**.

Se levantará la máquina virtual y se bootear para la imagen del disco CD-ROM Roo que fue descargado previamente, con ello se da inicio al proceso de instalación automático, después que la instalación esté completa el sistema se reiniciará, dando inicio al sistema desde el CD-ROM.

El Honeywall cuenta con dos cuentas de sistemas por defecto: roo y root, las cuales tienen el mismo password “honey” y pueden ser modificados en cualquier comento.

Para poder dar inicio al sistema se debe ingresar con el usuario roo, pero para poder iniciar la configuración se necesita pasar a la cuenta root con el comando su-, luego con el comando menú se ingresará al panel de administración del Honeywall, desde el cual se puede configurar parámetros como: información sobre la red y datos de los Honeypots.

5.7.1 LÍNEA DE COMANDOS

Linux en las versiones trata todo tipo de administración por línea de comandos, órdenes o bash (interpretador de órdenes) de configuración. La cual se estable en el **Anexo A1**, donde se encuentra el archivo raíz “/” y la carpeta “etc”, con el nombre honeywall.conf, para el cual modificamos el archivo se realiza mediante

el uso de algún editor de texto preinstalado en el Sistema o uso del comando de ejecución, accediendo a la configuración de las variables de archivo:

[root@MDHhost roo]# vi /etc/honeywall.conf

```
#################################################################
#
# Copyright (C) <2005> <The Honeynet Project>
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or (at
# your option) any later version.
#
# This program is distributed in the hope that it will be useful, but
# WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU
# General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307
# USA
#
################################################
```

```
#
# This file is the Honeywall import file (aka "honeywall.conf").
# It is a list of VARIABLE=VALUE tuples (including comments as
# necessary, # such as this) and whitespace lines.
#
# note: DO NOT surround values in quotation marks
#
#####################################################################
#####################################################################
# Site variables that are  #
# global to all honeywalls #
# at a site.               #
#####################################################################

# Specify the IP address(es) and/or networks that are allowed to connect
# to the management interface.  Specify any to allow unrestricted access.
# [Valid argument: IP address(es) | IP network(s) in CIDR notation | any]
HwMANAGER=192.168.1.0/24
# Specify the port on which SSHD will listen
# NOTE: Automatically aded to the list of TCP ports allowed in by IPTables
# [Valid argument: TCP (port 0 - 65535)]
HwSSHD_PORT=22
# Specify whether or not root can login remotely over SSH
# [Valid argument: yes | no]
```

HwSSHD_REMOTE_ROOT_LOGIN=no

NTP Time server(s)

[Valid argument: IP address]

HwTIME_SVR=

################################

Local variables that are

specific to each

honeywall at a site.

################################

Specify the system hostname

[Valid argument: string]

HwHOSTNAME=MDHhost

Specify the system DNS domain

[Valid argument: string]

HwDOMAIN=localMDH

#Start the Honeywall on boot

[Valid argument: yes | no]

HwHONEYWALL_RUN=yes

To use a headless system.

[Valid argument: yes | no]

HwHEADLESS=no

This Honeywall's public IP address(es)

[Valid argument: IP address | space delimited IP addresses]

HwHPOT_PUBLIC_IP=192.168.1.20

DNS servers honeypots are allowed to communicate with

[Valid argument: IP address | space delimited IP addresses]

HwDNS_SVRS=

To restrict DNS access to a specific honeypot or group of honeypots, list

them here, otherwise leave this variable blank

[Valid argument: IP address | space delimited IP addresses | blank]

HwDNS_HOST=

The name of the externally facing network interface

[Valid argument: eth* | br* | ppp*]

HwINET_IFACE=eth0

The name of the internally facing network interface

[Valid argument: eth* | br* | ppp*]

HwLAN_IFACE=eth1

The IP internal connected to the internally facing interface

[Valid argument: IP network in CIDR notation]

HwLAN_IP_RANGE=192.168.1.0/24

The IP broadcast address for internal network

[Valid argument: IP broadcast address]

HwLAN_BCAST_ADDRESS=192.168.1.255

Enable QUEUE support to integrate with Snort-Inline filtering

[Valid argument: yes | no]

HwQUEUE=yes

The unit of measure for setting oubtbound connection limits

[Valid argument: second, minute, hour, day, week, month, year]

HwSCALE=hour

The number of TCP connections per unit of measure (HwScale)

[Valid argument: integer]

HwTCPRATE=20

The number of UDP connections per unit of measure (HwSCALE)

[Valid argument: integer]

HwUDPRATE=20

The number of ICMP connections per unit of measure (HwSCALE)

[Valid argument: integer]

HwICMPRATE=50

The number of other IP connections per unit of measure (HwSCALE)

[Valid argument: integer]

HwOTHERRATE=10

Enable the SEBEK collector which delivers keystroke and files

to a remote system even if an attacker replaces daemons such as sshd

[Valid argument: yes | no]

HwSEBEK=yes

Enable the Walleye Web interface.

#[Valid argument: yes | no]

HwWALLEYE=yes

Specify whether whether to drop SEBEK packets or allow them to be sent

outside of the Honeynet.

[Valid argument: ACCEPT | DROP]

HwSEBEK_FATE=ACCEPT

Specify the SEBEK destination host IP address

[Valid argument: IP address]

HwSEBEK_DST_IP=192.168.1.21

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Specify the SEBEK destination port

[Valid argument: port]

HwSEBEK_DST_PORT=1101

Enable SEBEK logging in the Honeywall firewall logs

[Valid argument: yes | no]

HwSEBEK_LOG=yes

Specify whether the dialog menu is to be started on login to TTY1

[Valid argument: yes | no]

HwMANAGE_DIALOG=yes

Specify whether management port is to be activated on start or not.

[Valid argument: yes | no]

HwMANAGE_STARTUP=yes

Specy the network interface for remote management. If set to br0, it will

assign MANAGE_IP to the logical bridge interface and allow its use as a

management interface. Set to none to disable the management interface.

[Valid argument: eth* | br* | ppp* | none]

HwMANAGE_IFACE=eth2

IP of management Interface

[Valid argument: IP address]

HwMANAGE_IP=192.168.1.3

Netmask of management Interface

[Valid argument: IP netmask]

HwMANAGE_NETMASK=255.255.255.0

Default Gateway of management Interface

[Valid argument: IP address]

HwMANAGE_GATEWAY=192.168.1.1

DNS Servers of management Interface

[Valid argument: space delimited IP addresses]

HwMANAGE_DNS=192.168.1.1

TCP ports allowed into the management interface.

Do NOT include the SSHD port. It will automatically be included

[Valid argument: space delimited list of TCP ports]

HwALLOWED_TCP_IN=22 443

Specify whether or not the Honeywall will restrict outbound network

connections to specific destination ports. When bridge mode is utilized,

a management interface is required to restrict outbound network connections.

[Valid argument: yes | no]

HwRESTRICT=yes

Specity the TCP destination ports Honeypots can send network traffic to.

[Valid argument: space delimited list of UDP ports]

HwALLOWED_TCP_OUT=22 25 43 80 443

Specity the UDP destination ports Honeypots can send network traffic to.

[Valid argument: space delimited list of UDP ports]

HwALLOWED_UDP_OUT=53 123

Specify whether or not to start swatch and email alerting.

[Valid argument: yes | no]

HwALERT=yes

Specify email address to use for email alerting.

[Valid argument: any email address]

HwALERT_EMAIL=root@localhost.localdomain

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

NIC Module List - Set this to the number and order you wish

to load NIC drivers, such that you get the order you want

for eth0, eth1, eth2, etc.

[Valid argument: list of strings]

#

Example: eepro100 8139too

HwNICMODLIST=

Blacklist, Whitelist, and Fencelist features.

[Valid argument: string]

HwFWBLACK=/etc/blacklist.txt

[Valid argument: string]

HwFWWHITE=/etc/whitelist.txt

[Valid argument: string]

HwFWFENCE=/etc/fencelist.txt

[Valid argument: yes | no]

HwBWLIST_ENABLE=no

[Valid argument: yes | no]

HwFENCELIST_ENABLE=no

The following feature allows the roo to allow attackers into the

honeypots but they can't send packets out...

[Valid argument: yes | no]

HwROACHMOTEL_ENABLE=yes

Disables BPF filtering based on the contents of HwHPOT_PUBLIC_IP

and the black and white list contained within HwFWBLACK and HwFWWHITE

if the HwBWLIST_ENABLE is on. Other wise, it just filters based on

the contents of HwHPOT_PUBLIC_IP

[Valid argument: yes | no]

HwBPF_DISABLE=no

This capability is not yet implemented in roo. The variable

has been commented out for this reason. dittrich - 02/08/05

Options for hard drive tuning (if needed).

[Valid argument: string]

Example: -c 1 -m 16 -d

HwHWPARMOPTS=

Should we swap capslock and control keys?

HwSWAP_CAPSLOCK_CONTROL=no

##

Snort Rule Update Variables

##

Enable or disable automatic snort rule updates

[Valid argument: yes | no]

HwRULE_ENABLE=no

Automatically restart snort and snort_inline when automatic updates are

applied and when calls to update IDS or IPs rules?

[Valid argument: yes | no]

HwSNORT_RESTART=no

Oink Code - Required by Oinkmaster to retrieve VRT rule updates

See: /hw/docs/README.snortrules or

http://www.honeynet.org/tools/cdrom/roo/manual/

for instructions on how to obtain it (Free registration).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
# [Valid argument: ~40 char alphanum string]
HwOINKCODE=
# Day automatic snort rule updates should be retrieved (for weekly updates)
# For daily updates, set this to ""
# [Valid argument: sun | mon | tue | wed | thu | fri | sat]
HwRULE_DAY=sat
# Hour of day snort rules updates should be retrieved
# [Valid argument: 0 | 1 | 2 | ... | 23] (0 is Midnight, 12 is noon, 23 is 11PM)
HwRULE_HOUR=3
#####################################################################
# Pcap and DB data retention settings
# Currenrly ONLY used when Pcap/DB purge scripts are called
# Pcap/DB data *is NOT* automatically purged
#####################################################################
# Days to retain Pcap data.  This will be used *IF* /dlg/config/purgePcap.pl
# is called with NO arguments.
# NOTE: Override this by supplying the number of days as an argument ala:
# /dlg/config/purgePcap.pl <days>
HwPCAPDAYS=45
# Days to retain DB data.  This will be used *IF* /dlg/config/purgeDB.pl
# is called with NO arguments.
# NOTE: Override this by supplying the number of days as an argument ala:
# /dlg/config/purgeDB.pl <days>
HwDBDAYS=180
#####################################################################
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

NAT mode is no longer supported.

Don't mess with anything below here unless you know what you're

doing! Don't say we didn't warn you, and don't try logging a bugzilla

request to clean up the mess!

##

Space delimited list of Honeypot ips

NOTE: MUST HAVE SAME NUMBER OF IPS AS PUBLIC_IP VARIABLE.

[Valid argument: IP address]

#HwHPOT_PRIV_IP_FOR_NAT=

Specify the IP address of the honeywall's internal (i.e. gateway

IP for NAT) IP address. This is only used in NAT mode.

[Valid argument: IP address ex: 192.168.10.1]

#HwPRIV_IP_FOR_NAT=

Specify the IP netmask for interface alises. One aliases will be created

on the external interface for each Honeypot when in NAT mode only.

[Valid argument: IP netmask]

#HwALIAS_MASK_FOR_NAT=255.255.255.0

End of honeywall.conf parameters

#

Newly defined variables as of Thu Dec 7 01:02:22 GMT 2017

#

HwHFLOW_DB=3

HwSENDOR_ID=1147415589

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El archivo de configuraciones, manifiestan la administración del Honeypot, cada modificación o configuración del archivo crea un registro copia, para que no se pierda la síntesis de control y mantenimiento.

Menú de diálogos

Al usar menús para la configuración es la más adecuada el cual se interactúa con el Sistema Honeywall, en que la administración cuenta con 6 tipos de acceso el cual pueden ser modificados para una mejor gestión:

- **Status.**
- **OS Administration.**
- **Honeywall Administration.**
- **Honeywall Configuration.**
- Documentation.
- Exit

Para poder acceder al menú, se debe ingresar como **"su -"** y autentificando como usuario **"root"** y el comando "/dlg/dialogmenu.sh"

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

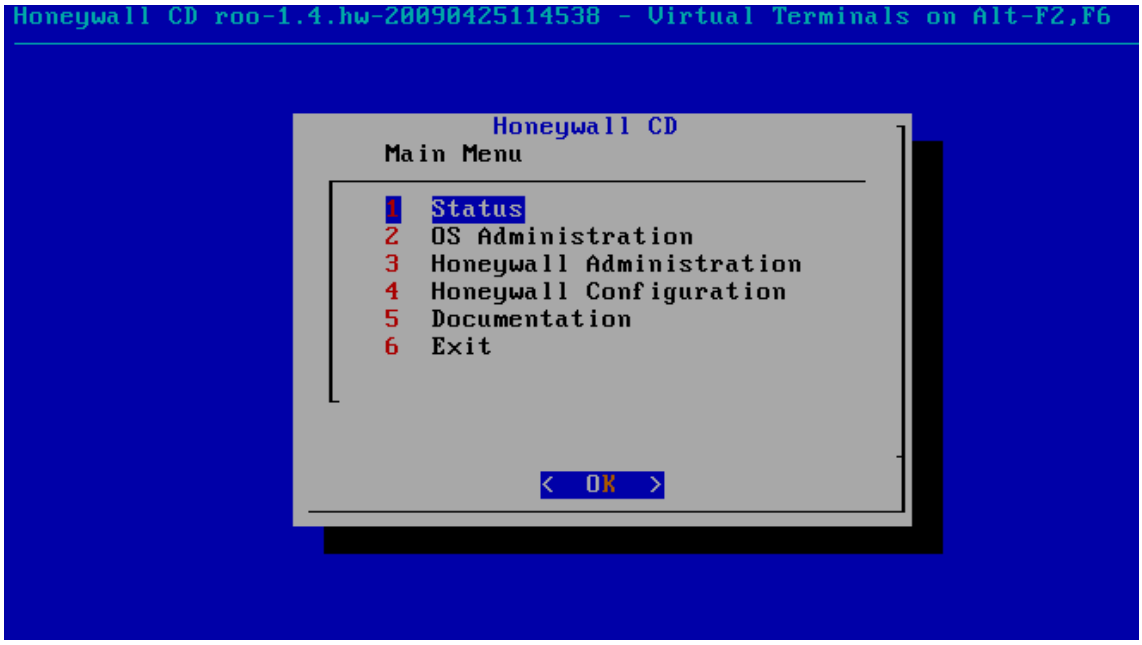


Figura 46: Menú del Honeywall
Fuente: ANHMB

Status: muestra el estado actual del Honeywall, las direcciones IPs configuradas, alertas, reglas del Firewall, conexiones entrantes y salientes, y toda la configuración del Honeywall.

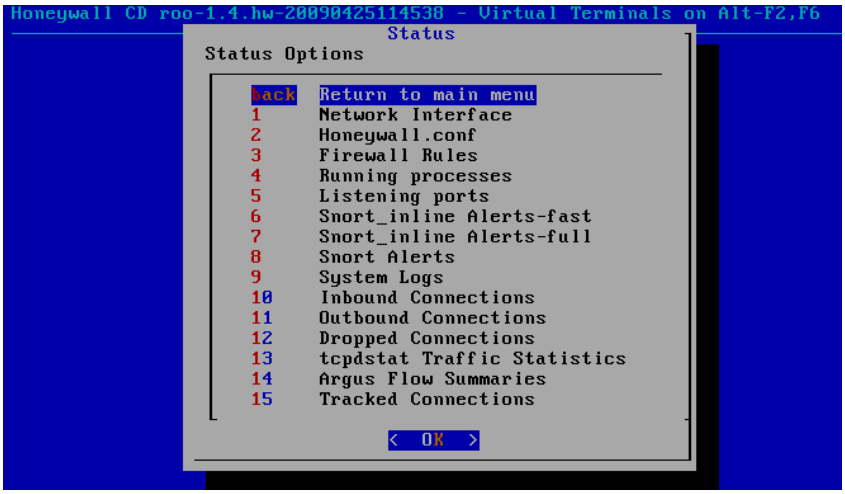


Figura 47: Opciones de Estatus
Fuente: ANHMB

Honeywall Administration: Es sustancial las configuración realizadas en los demás menús no se verán reflejadas, debido a que la edición de los archivos ".conf", y al reiniciar el Honeywall en general o se recargan las disposiciones por

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

apartado para no detener los servicios prestados o por la actualización de las reglas en conexiones entrantes y salientes.

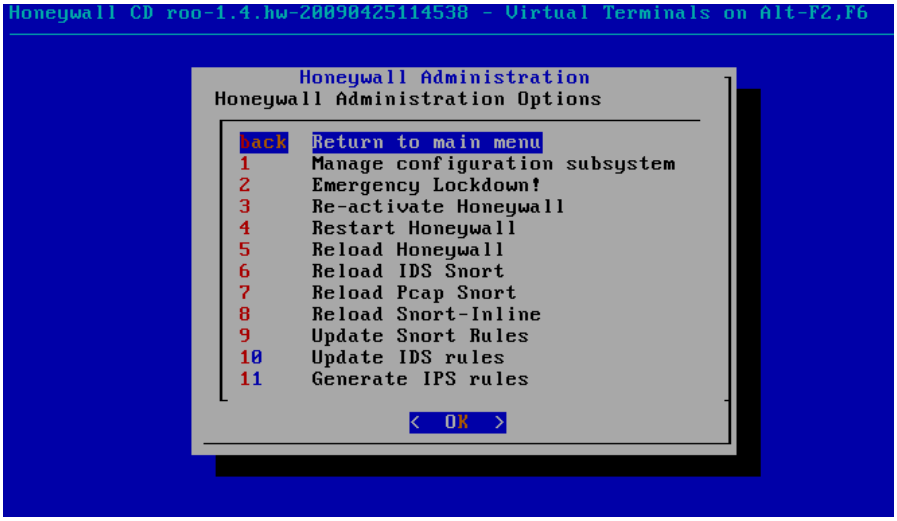


Figura 48: Opciones de Administrador del Honeywall
Fuente: ANHMB

Honeywall Configuration: donde se encuentra la configuración básica del Honeywall, es importante ya que se encuentran las reglas y las alertas del Snort_Inline, además el servicio de las listas negras y blancas (Black list and White list). El tiempo de escaneo se estable en esta sección o menú por medio de “Connection Limiting”, depende funcionalmente de la escala establecida, es horas, TCP/UDP/ICMP determinados por intervalos de tiempo.

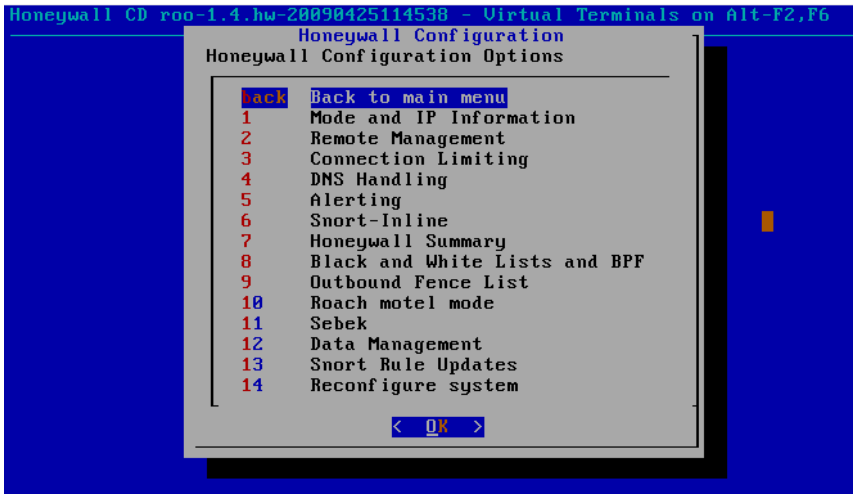


Figura 49: Opciones de Configuración del Honeywall

Fuente: ANHMB

Interfaz del navegador GUI

La administración de los servicios de monitoreo, es accedido por medio del navegador WEB que permite un mejor control, y se estable una dirección de acceso, únicamente al administrador de red, el cual se podrá modificar el Honeywall, consumiendo el Honeypot para detectar los tipos de intrusos existentes en primer monitoreo, desarrollando las reglas del Firewall o bloqueando conexiones malignas hacía la red de datos de la Municipalidad Distrital de HUAMBOS.

5.7.2 Walleye

El Servidor Web se accede por la seguridad por el puerto 443, utilizando listas generadas por el Honeypot, y la gestión se controla por medio del walleye.py archivo de configuración estándar, para acceder establemente en el archivo "honeywall.conf", mediante la dirección IP de acceso debe estar restringida por las reglas entrantes y salientes del Honeywall.

Accediendo por medio de la URL:

https://192.168.1.3

La contraseña: "honey", y al ingresar por vez primera es necesario cambiar las contraseñas del roo y root.

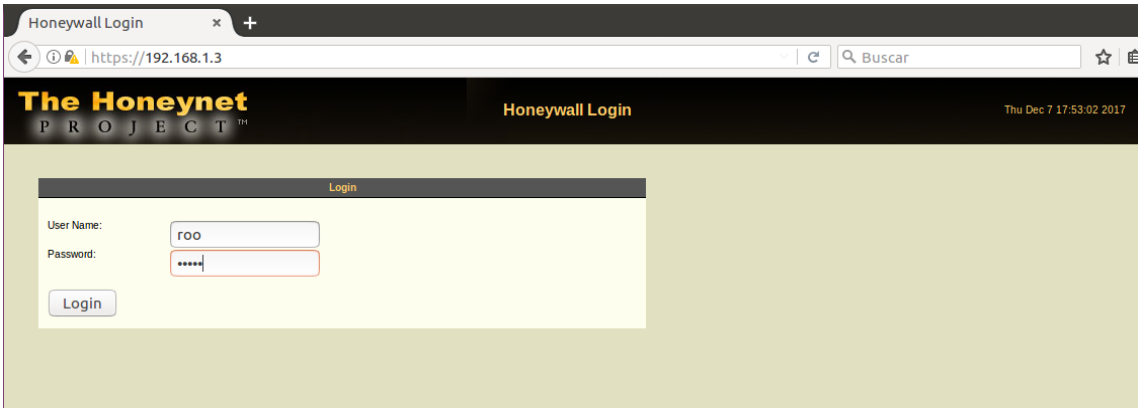


Figura 50: Ingreso del Honeywall web
Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

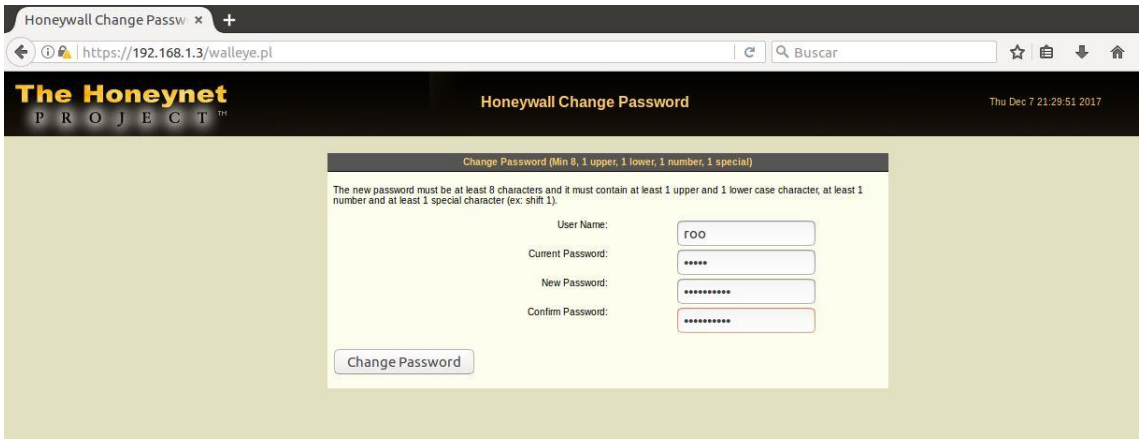


Figura 51: Cambio de contraseña del Honeywall
Fuente: ANHMB

En la Interfaz admin del Honeywall, se muestran los módulos de control y análisis de resultados, y se establecen las fechas almacenando en base de datos exportando un archivo con extensión ".pcap".

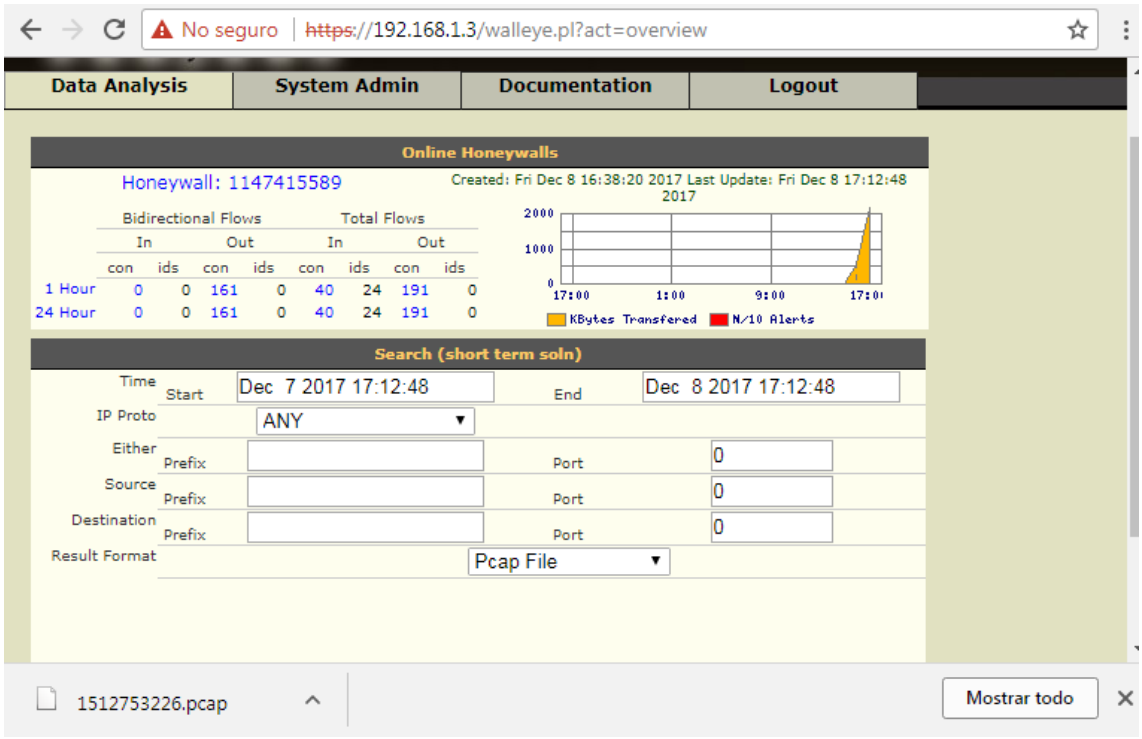


Figura 52: Interface admin del Honeywall
Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO VI
EVALUACIÓN DE RESULTADOS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6.1 PRUEBAS A TRAVÉS DE ATAQUES INFORMÁTICOS SIMULADOS

Para la realización de las pruebas de desempeño, se utilizarán la metodología analizada en el Capítulo 4, sección 4.3, el cual demuestra las vulnerabilidades existentes en la red de datos de la Municipalidad Distrital de HUAMBOS.

1. Para la realización de los ataques informáticos simulados empezaremos por realizar un escaneo de la red a través de Nmap, de esta manera podemos ver que ya se están simulando hosts en la red.

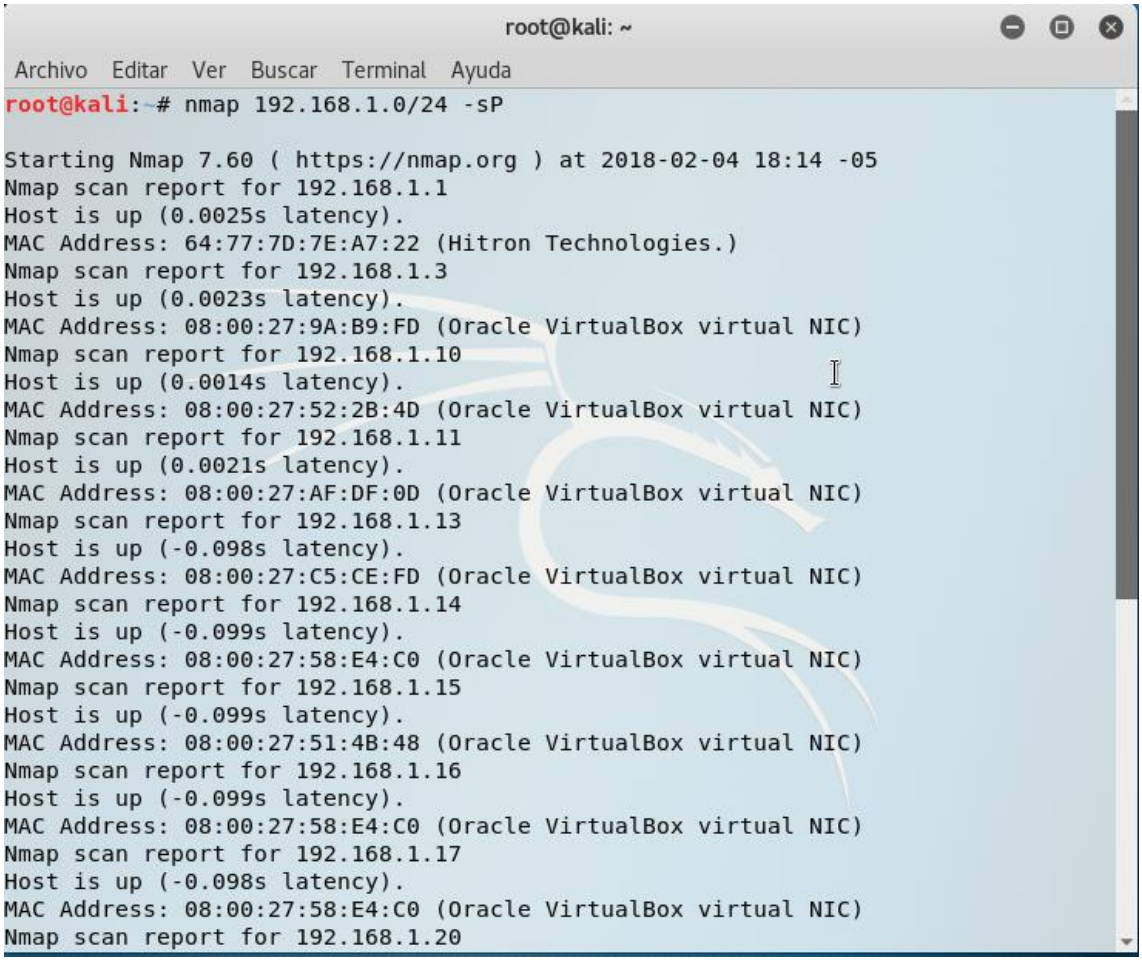


Figura 53: Escaneo de la Red
Fuente: ANHMB

2. Se procederá a verificar los servicios y puertos que se encuentran abiertos en los equipos simulados

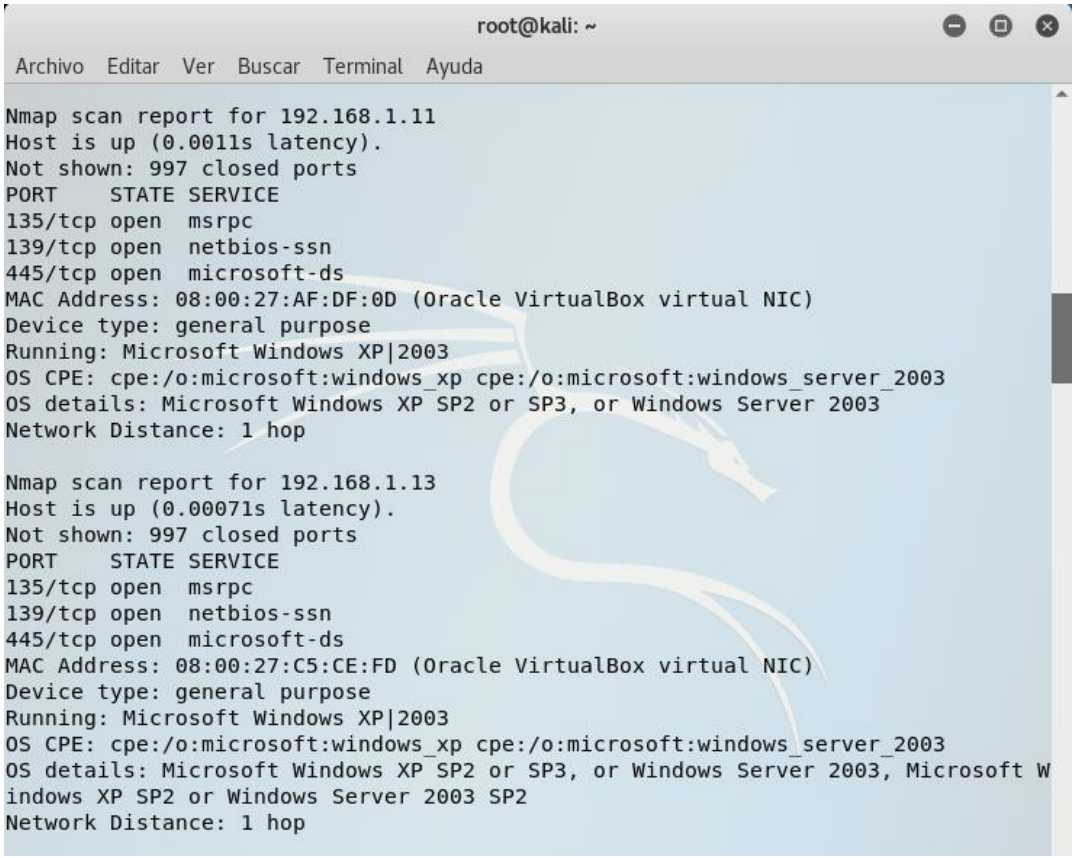


Figura 54: Verificación de puertos y servicios
Fuente: ANHMB

3. En este momento ya podemos empezar a verificar las entradas en el Honeywall

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

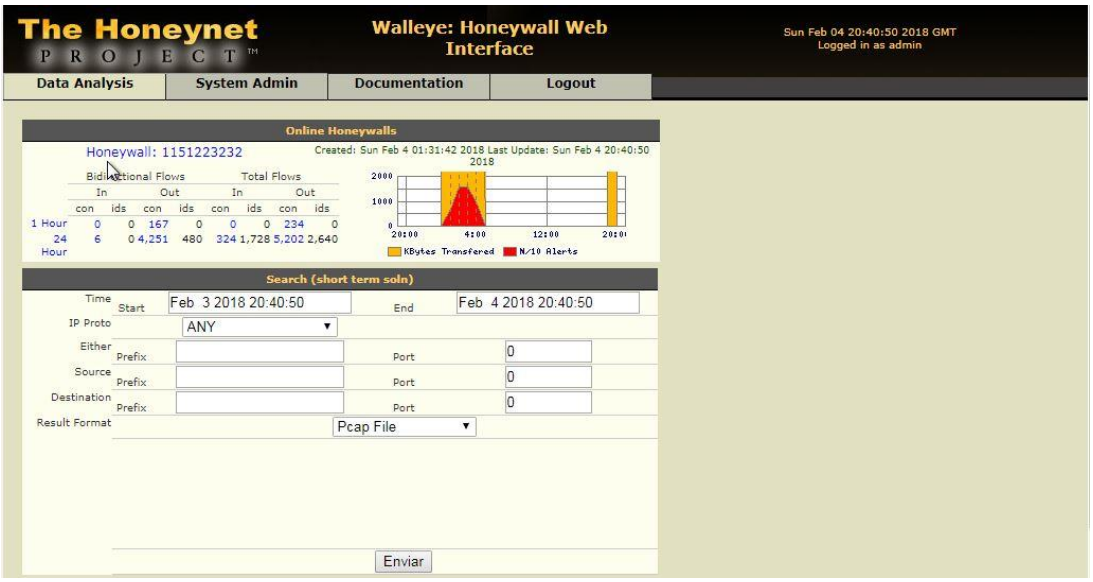


Figura 55: Verificación de conexiones
Fuente: ANHMB

4. Como podemos observar se ha identificado un patrón en el tráfico generado, el cual corresponde a al escaneo realizado por NMAP

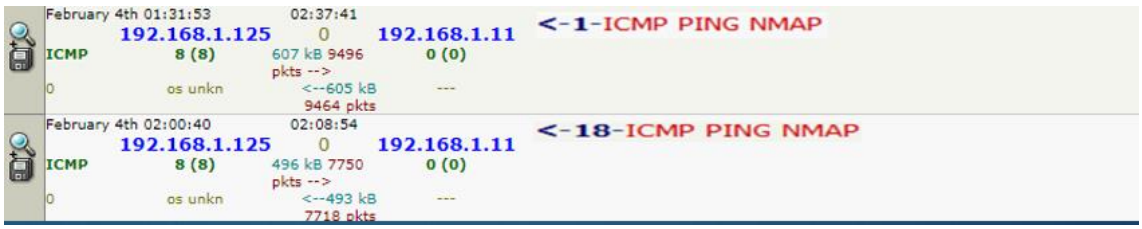


Figura 56: Patrón de NMAP identificado
Fuente: ANHMB

5. Se procederá a realizar una ejecución del exploit, ms08_067_netapi, como se demostró en el capítulo 4 sección 4.3

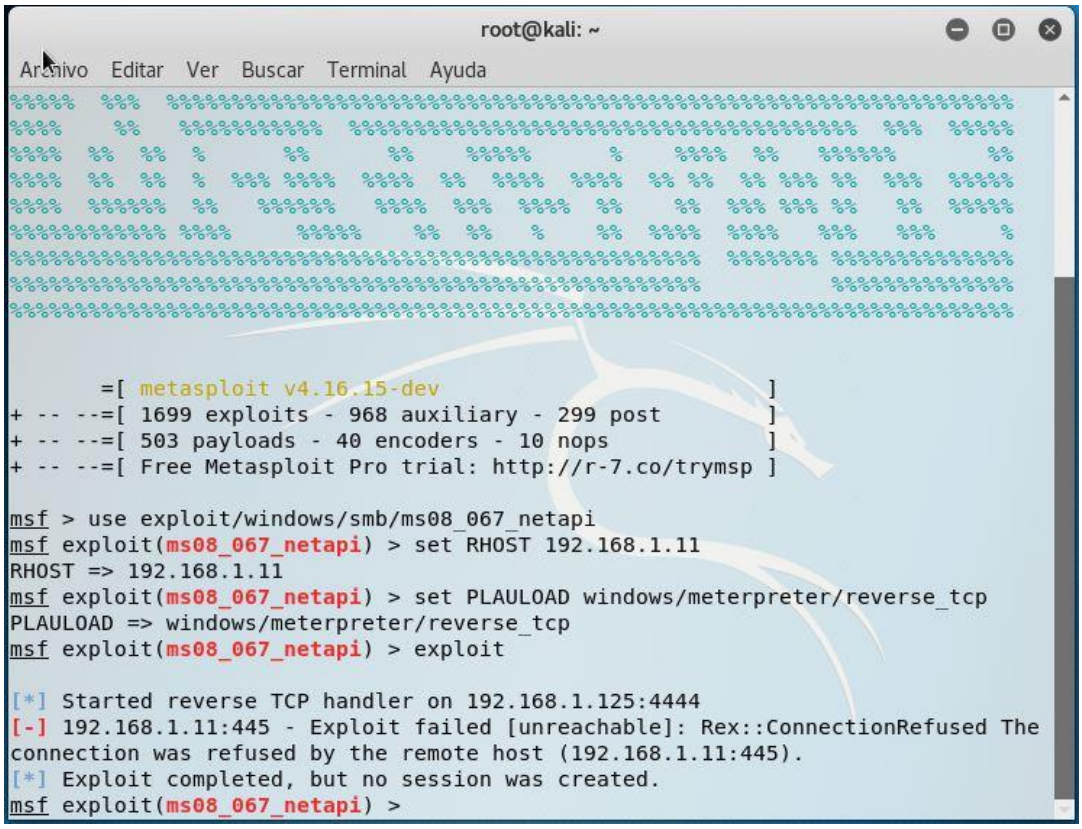


Figura 57: Ejecución del exploit ms08_067_netapi
Fuente: ANHMB

Se puede apreciar que al ejecutar al exploit no se puede acceder al computador y arroja el siguiente error **([-] 192.168.1.11:445 – Exploit faled [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.1.11:445).**

6. Una vez que se ha lanzado el exploit, se puede ver el seguimiento que el Honeywall le da a esta ejecución de código remota, la cual pertenece a un buffer overflow.

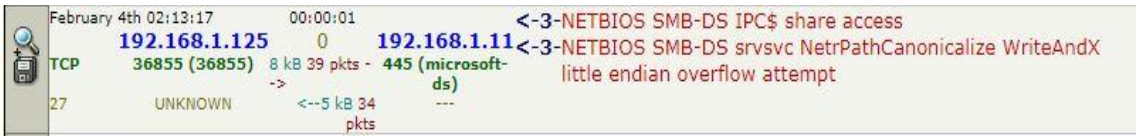


Figura 58: Seguimiento del paquete con Honeywall

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Fuente: ANHMB

7. En el visor detallado de paquetes tenemos una descripción más específica del ataque realizado, así como la referencia para un posible fallo a dicha vulnerabilidad.

February 4th 02:59:15 | 192.168.1.125 | TCP | 46443 (46443) | 27 | UNKNOWN | 00:00:01 | 0 | 9 kB 45 pkts --> | <--6 kB 39 pkts | 192.168.1.11 | 445 (microsoft-ds) | ---

<-3-NETBIOS SMB-DS IPC$ share access
<-3-NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt

IDS details

(Previous Page) Start 1 - - - - - - - - - - - - End (Next Page) 1 / 1

Timestamp	Priority	Classification	Type	Name	Revision	Generator	Reference
February 4th 02:02:16	1	Attempted Administrator Privilege Gain		NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt	6	rules_subsystem	bugtraq,19409 || cve,2006-3439 || url,www.microsoft.com/technet/security/bulletin/MS06-040.mspx
February 4th 02:02:16	1	Attempted Administrator Privilege Gain		NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt	6	rules_subsystem	bugtraq,19409 || cve,2006-3439 || url,www.microsoft.com/technet/security/bulletin/MS06-040.mspx
February 4th 02:02:16	1	Attempted Administrator Privilege Gain		NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt	6	rules_subsystem	bugtraq,19409 || cve,2006-3439 || url,www.microsoft.com/technet/security/bulletin/MS06-040.mspx
February 4th 02:02:15	3	Generic Protocol Command Decode		NETBIOS SMB-DS IPC$ share access	7	rules_subsystem	
February 4th 02:02:15	3	Generic Protocol Command Decode		NETBIOS SMB-DS IPC$ share access	7	rules_subsystem	
February 4th 02:02:15	3	Generic Protocol Command Decode		NETBIOS SMB-DS IPC$ share access	7	rules_subsystem	

Flow Examination

Snort	Packet Decode
Snort	Rule Evaluation

Figura 59: Visor detallado del paquete con Honeywall
Fuente: ANHMB

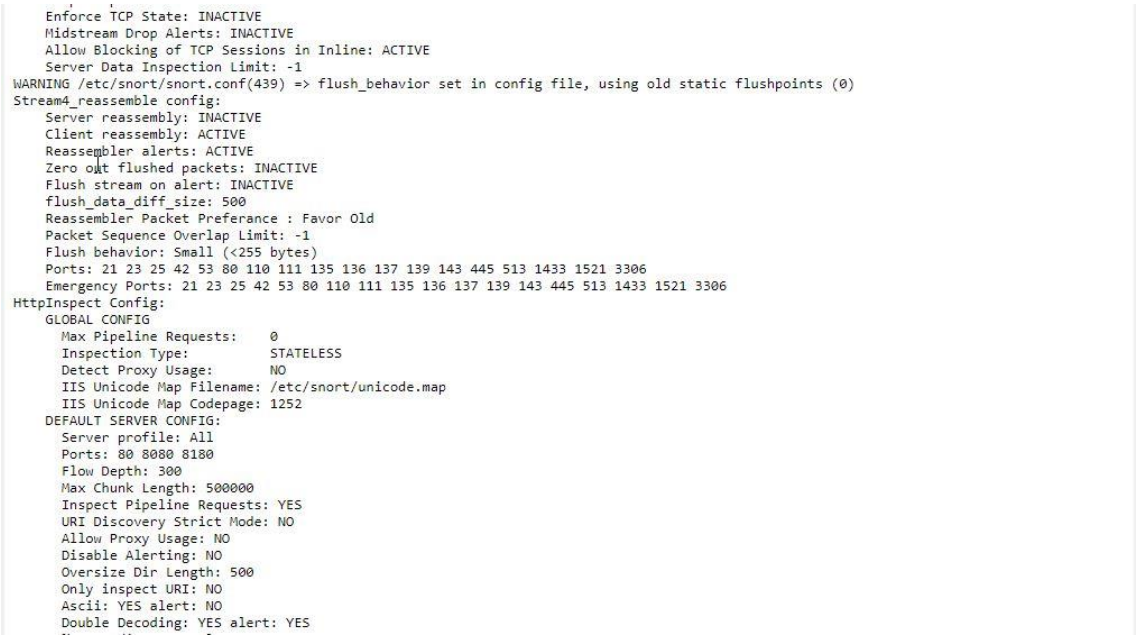
8. Captura del paquete que contiene el código malicioso

```
02/04-02:13:17.356454 8:0:27:C7:B3:9 -> 8:0:27:AF:DF:D type:0x800 len:0x4A
192.168.1.125:36855 -> 192.168.1.11:445 TCP TTL:64 TOS:0x0 ID:3502 IpLen:20 DgmLen:60 DF
******S* Seq: 0xE612549A  Ack: 0x0  Win: 0x7210  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1065024788 0 NOP WS: 7

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/04-02:13:17.357084 8:0:27:AF:DF:D -> 8:0:27:C7:B3:9 type:0x800 len:0x4E
192.168.1.11:445 -> 192.168.1.125:36855 TCP TTL:128 TOS:0x0 ID:21207 IpLen:20 DgmLen:64 DF
***A**S* Seq: 0xBD1EA5C5  Ack: 0xE612549B  Win: 0xFFFF  TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/04-02:13:17.357451 8:0:27:C7:B3:9 -> 8:0:27:AF:DF:D type:0x800 len:0x42
192.168.1.125:36855 -> 192.168.1.11:445 TCP TTL:64 TOS:0x0 ID:3503 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xE612549B  Ack: 0xBD1EA5C6  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1065024789 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/04-02:13:17.359108 8:0:27:C7:B3:9 -> 8:0:27:AF:DF:D type:0x800 len:0x9A
192.168.1.125:36855 -> 192.168.1.11:445 TCP TTL:64 TOS:0x0 ID:3504 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0xE612549B  Ack: 0xBD1EA5C6  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1065024790 0
00 00 00 54 FF 53 4D 42 72 00 00 00 00 18 01 28  ...T.SMBr......(
00 00 00 00 00 00 00 00 00 00 00 00 00 00 63 9D  ..............c.
00 00 74 4E 00 31 00 02 4C 41 4E 4D 41 4E 31 2E  ..tN.1..LANMAN1.
30 00 02 4C 4D 31 2E 32 58 30 30 32 00 02 4E 54  0..LM1.2X002..NT
20 4C 41 4E 4D 41 4E 20 31 2E 30 00 02 4E 54 20   LANMAN 1.0..NT
4C 4D 20 30 2E 31 32 00                          LM 0.12.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figura 60: Captura del paquete con código malicioso
Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

9. Regla de Snort con la que analizo dicho exploit



```
    Enforce TCP State: INACTIVE
    Midstream Drop Alerts: INACTIVE
    Allow Blocking of TCP Sessions in Inline: ACTIVE
    Server Data Inspection Limit: -1
WARNING /etc/snort/snort.conf(439) => flush_behavior set in config file, using old static flushpoints (0)
Stream4_reassemble config:
    Server reassembly: INACTIVE
    Client reassembly: ACTIVE
    Reassembler alerts: ACTIVE
    Zero out flushed packets: INACTIVE
    Flush stream on alert: INACTIVE
    flush_data_diff_size: 500
    Reassembler Packet Preferance : Favor Old
    Packet Sequence Overlap Limit: -1
    Flush behavior: Small (<255 bytes)
    Ports: 21 23 25 42 53 80 110 111 135 136 137 139 143 445 513 1433 1521 3306
    Emergency Ports: 21 23 25 42 53 80 110 111 135 136 137 139 143 445 513 1433 1521 3306
HttpInspect Config:
    GLOBAL CONFIG
      Max Pipeline Requests:    0
      Inspection Type:          STATELESS
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports: 80 8080 8180
      Flow Depth: 300
      Max Chunk Length: 500000
      Inspect Pipeline Requests: YES
      URI Discovery Strict Mode: NO
      Allow Proxy Usage: NO
      Disable Alerting: NO
      Oversize Dir Length: 500
      Only inspect URI: NO
      Ascii: YES alert: NO
      Double Decoding: YES alert: YES
```

Figura 61: Regla de Snort para la vulnerabilidad ms08_067_netapi
Fuente: ANHMB

6.2 VERIFICACIÓN DEL DISEÑO

Para la verificación del diseño se realizarán las siguientes pruebas, las cuales se han establecido a fin de garantizar el correcto funcionamiento de los dispositivos en la Honeynet y la integridad de los datos capturados.

1. Configuración de Fecha y hora

Propósito: Correcta configuración de la fecha y hora del Honeywall y Honeypots.

Descripción: La instalación de los Sistemas Operativos por lo general nunca configura la hora y fecha actual, podemos tener una Honeynet con dispositivos con horas y fechas diferentes. Esto afecta en la recolección de datos, las

estampas de tiempo en los logs no corresponderían impidiendo realizar un rastreo de un ataque.

Pasos:

- Chequear la fecha y hora en el Honeywall, usando el comando “date”.
- Verificar que corresponde la fecha y hora actual, caso contrario configurarla usando “date””.
- Chequear la fecha y hora en los Honeypots, usando el comando “date” para Linux y “time” Windows.
- Verificar que corresponde la fecha y hora actual, caso contrario configurarla usando “date” o “time”.

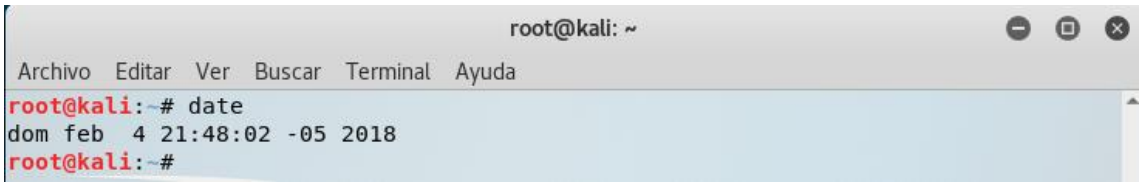


Figura 62: Fecha en el Honeywall
Fuente: ANHMB

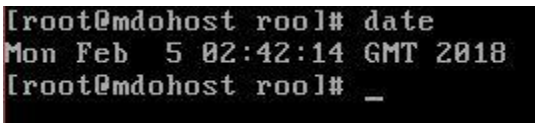


Figura 63: Fecha en el Honeypot
Fuente: ANHMB

2. Los Honeypots deben poder establecer conexiones entrantes y salientes a la red interna usando el protocolo IP.

Propósito: Los Honeypots accedan en ambas direcciones a la red interna.

Descripción: Cuando una máquina no tiene acceso a la red lo primero que se verifica es su conexión, verificar el cableado, para las conexiones lógicas hay

que revisar que correspondan las configuraciones de las interfaces de red virtuales (modo bride o modo host-only), revisar que la máquina física (Host) este correctamente conectada a la red, luego revisar si el firewall de Honeywall está funcionando, revisar que no esté bloqueando paquetes, revisar algún firewall instalado en los Honeypots (como el firewall de Windows.)

Pasos:

- ✓ Ping a cada Honeypot desde la máquina de pruebas, ejecutando ping <IP>
- ✓ Verificar que se obtiene respuesta con mínimo 4 ECHO replies desde la Honeypot.
- ✓ Ping la máquina de pruebas desde los Honeypots, ejecutando ping <IP>
- ✓ Verificar que se obtiene respuesta con mínimo 4 ECHO replies desde la máquina de pruebas.

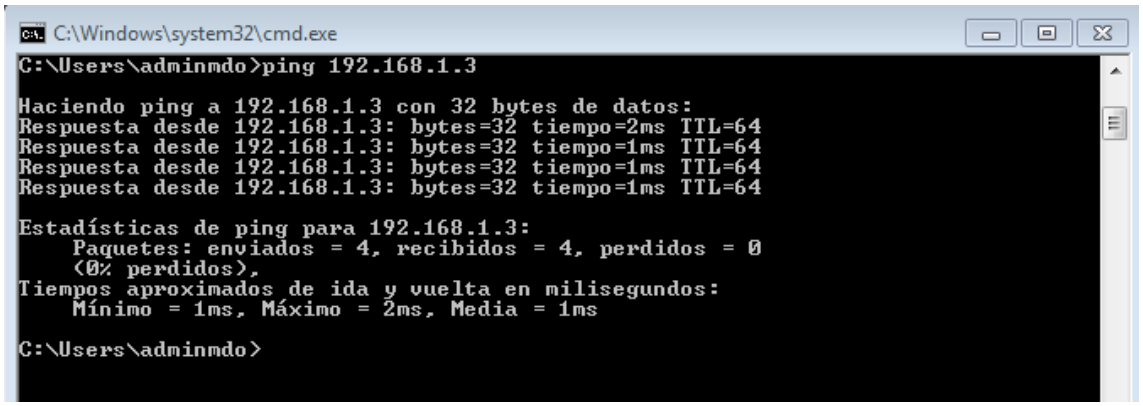


Figura 64: Ping hacia los Honeypots
Fuente: ANHMB

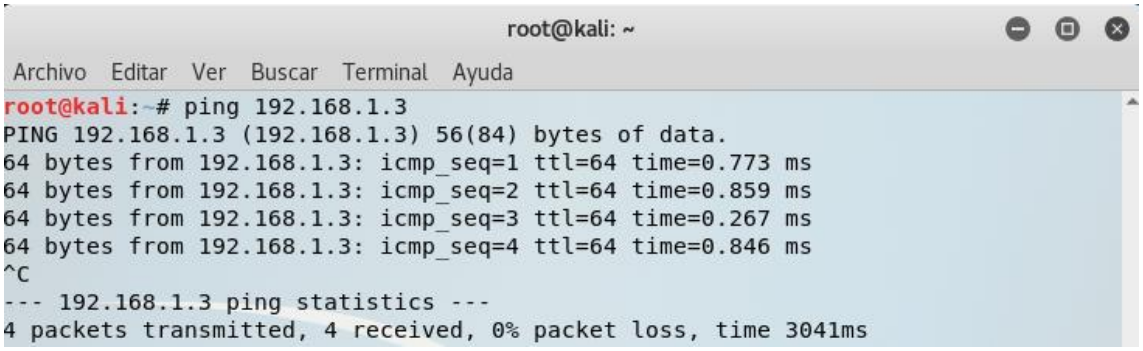


Figura 65: Ping desde los Honeypots
Fuente: ANHMB

3. Los Honeypots deben resolver nombres de dominio usando los DNS.

Propósito: Los Honeypots deben resolver los nombres de dominio.

Descripción: Es necesario para el correcto funcionamiento de los Honeypots, que puedan resolver nombres de dominio.

Pasos:

- ✓ Ejecutar “nslookup www.google.com” o “ping www.google.com” en los Honeypots.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

- ✓ Verificar la correcta resolución de nombre para el dominio www.google.com

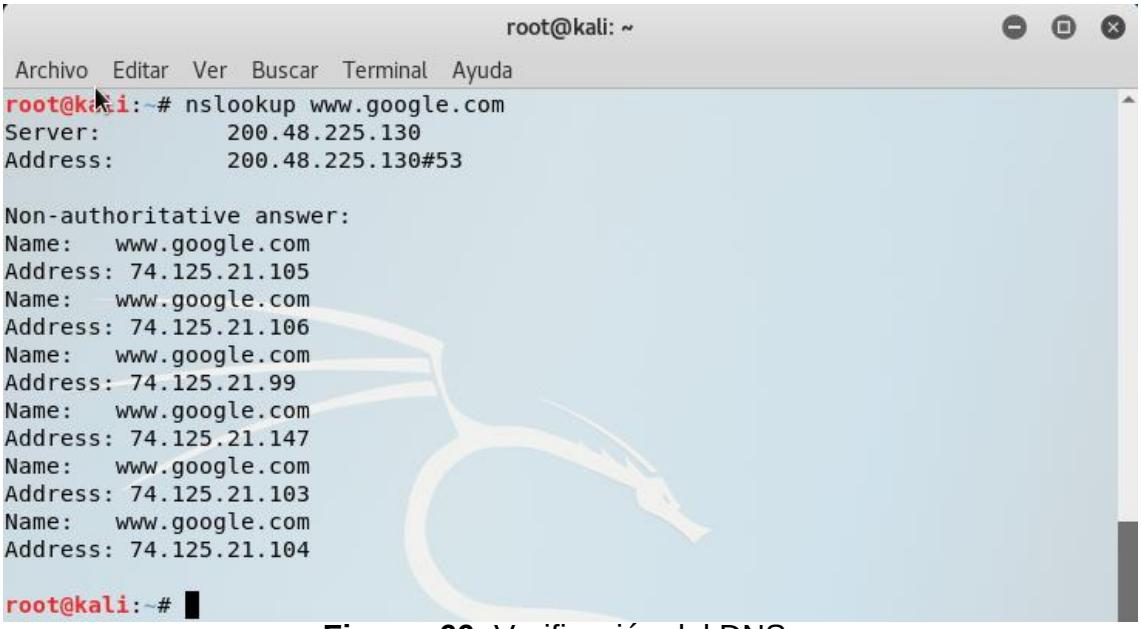


Figura 66: Verificación del DNS
Fuente: ANHMB

4. El Honeywall está registrando el tráfico.

Propósito: Garantizar el registro de tráfico en el Honeywall

Descripción: En el Honeywall puede no estar levantado Snort, para hacerlo en el menú seleccionar “Recargar Honeywall”

Pasos:

- ✓ Ingresar al Honeywall como root
- ✓ Seleccionar IP PROTO-> ICMP -> Result Format-> Wall Eye flow view
- ✓ Verificar las entradas con el protocolo ICMP correspondientes a los Ping realizados en pruebas anteriores.

Aggregated Flows: Aggregated by src_ip Between Sun Feb 4 03:06:40 2018 and Mon Feb 5 03:06:40 2018

(Previous Page) Start 1 - - - - - - - - - - - - End (Next Page) 1 / 1

Filter		Aggregate By	Aggregate Totals								Individual Flow Maximums			
Include	Exclude	Source IP	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes	SRC pkts	SRC bytes	DST pkts	DST bytes
+++	---	192.168.1.200	1,289	1,688	1,061	17	2,422,463	822,161,400	235,399	310,728,104	15,458	788,186	30,785	41,705,358
+++	---	192.168.1.150	13	0	12	5	187	14,781	24	6,718	122	8,418	7	2,631
+++	---	192.168.1.126	3	0	3	2	8	304	8	3,206	6	213	6	3,067
+++	---	192.168.1.125	38,682	108	920	1,033	422,290	25,961,779	412,447	29,208,502	36,321	2,326,424	36,337	2,328,536
+++	---	192.168.1.124	3,255		42,749	17	63,362	3,088,156	110,878	135,586,175	27,894	583,668	62,205	92,052,528
+++	---	192.168.1.22	17	3	6	4	53	6,203	31	2,951	11	1,197	10	987
+++	---	192.168.1.21	23	10	10	4	187	22,004	137	16,794	17	2,081	16	2,156
+++	---	192.168.1.20	18	3	8	6	96	11,832	40	7,541	22	2,382	10	4,435
+++	---	192.168.1.17	20	6	8	4	103	11,880	75	8,210	18	2,093	17	2,176
+++	---	192.168.1.16	26	11	10	4	195	23,795	162	20,129	17	2,113	17	2,176
+++	---	192.168.1.15	45	5	6	4	173	23,272	76	8,899	22	4,237	17	2,008
+++	---	192.168.1.14	19	4	7	4	66	7,558	41	3,858	11	1,207	10	987
+++	---	192.168.1.13	17	3	6	4	54	6,287	31	2,871	11	1,205	10	987
+++	---	192.168.1.11	342	3	278	10	88,415	84,144,921	64,582	3,619,571	64,158	83,104,968	39,536	975,553
+++	---	192.168.1.10	12	0	2	2	14	2,935	0	0	2	433	0	0
+++	---	192.168.1.1	1	0	1	1	1	128	0	0	1	128	0	0

Apply checkbox filters

Figura 67: Prueba de registro de tráfico

Fuente: ANHMB

5. Walleye está activado y permite ingresar con el usuario.

Propósito: La herramienta gráfica de análisis “Walleye” incluida en el Honeywall esté activa y correctamente configurada.

Descripción: Muchas veces el demonio http no se encuentra levantado o la IP para la administración no está configurada. Verificar que en el Honeywall este configurada “Would you like to configure a magnament interface” con “Yes”, y reiniciar el Honeywall verificando que http se levante.

Pasos:

- ✓ Conectar la máquina de pruebas a la interface de administración, configurar la IP correspondiente e ingresar a “https://192.168.1.3/’.
- ✓ Ingresar el usuario y contraseña.
- ✓ Verificar que el acceso este correcto.

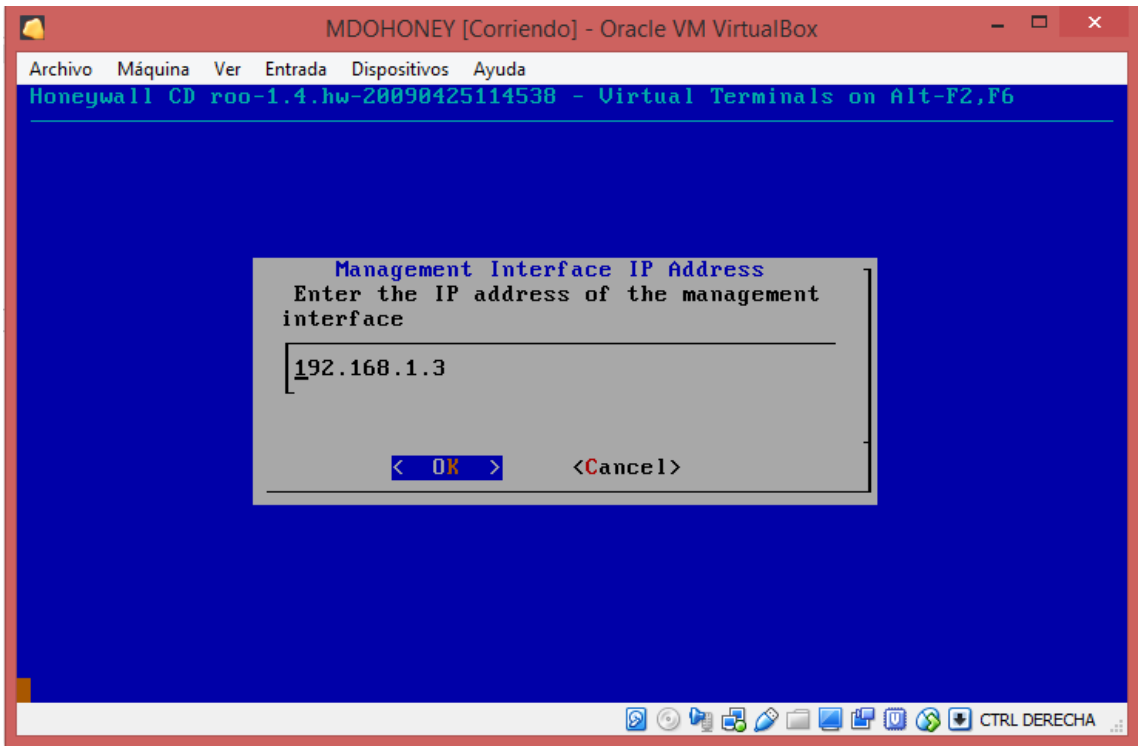


Figura 68: Dirección IP de interfaz de administración
Fuente: ANHMB

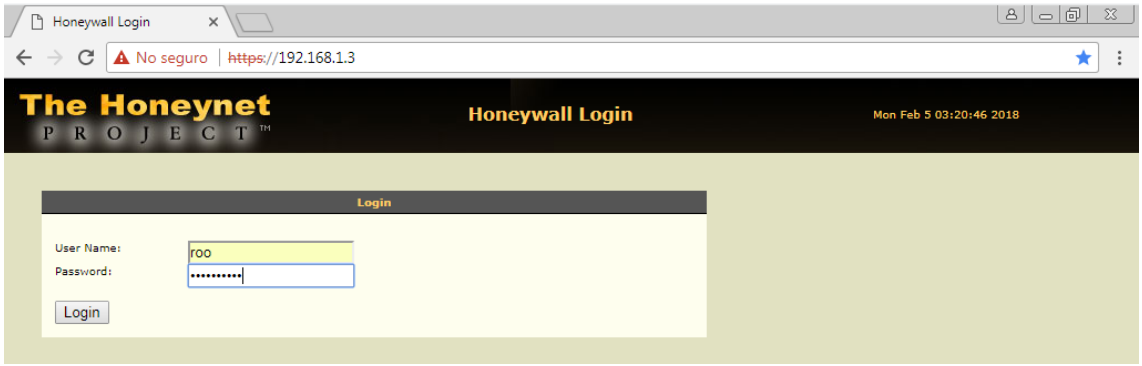


Figura 69: Ingreso a la Administración web
Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6. Walleye muestra el tráfico registrado por el Honeywall.

Propósito: Verificar que Walleye muestre el tráfico registrado por Snort en el Honeywall.

Descripción: Walleye es la principal herramienta de análisis, es necesario verificar que muestre los registros de Snort, en caso de que no lo haga se debe a una mala instalación, se procede a reinstalar el Honeywall.

Pasos:

- ✓ Ingresar en Walleye.
- ✓ En la pantalla principal deberíamos poder ver de manera gráfica el tráfico que está siendo capturado por el Honeywall.

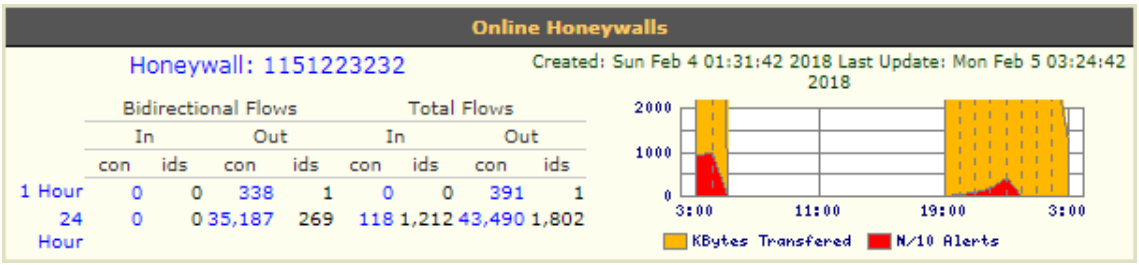


Figura 70: Tráfico capturado por Honeywall

Fuente: ANHMB

7. Sebek está funcionando en los Honeypots y enviando datos.

Propósito: Garantizar que el Cliente Sebek está enviando datos y el Servidor Sebek los recibe.

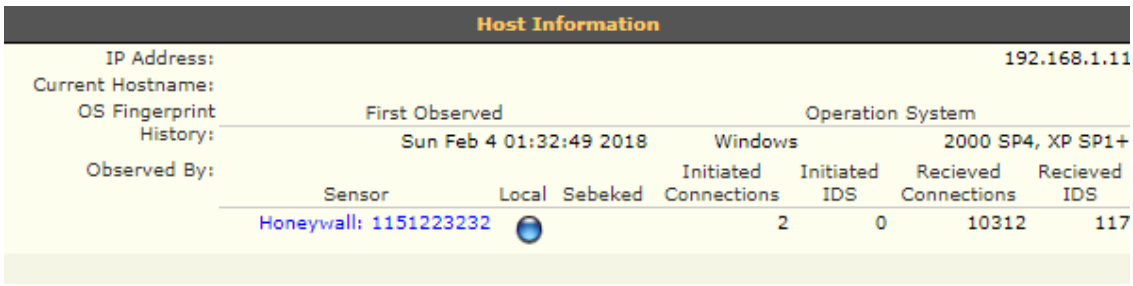
Descripción: Si no se recibe datos del Sebek puede ser por una mala configuración en los parámetros de red, el cliente Sebek para Windows sigue

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

funcionando aún después reiniciar el sistema, pero el Cliente Sebek de Linux requiere ser instalada cada vez que se inicia el Sistema Operativo

Pasos:

- ✓ Generar datos para el Sebek, para Windows ingresar comandos en la consola, en Linux conectarse por SSH a un Honeypot e ingresar comandos.
- ✓ Ingresar en Walleye y verificar los datos capturados por el Servidor Sebek, están marcados con la etiqueta “Sebeked”



Host Information

IP Address:							192.168.1.11
Current Hostname:							
OS Fingerprint History:	First Observed			Operation System			
	Sun Feb 4 01:32:49 2018			Windows			2000 SP4, XP SP1+
Observed By:	Sensor	Local	Sebeked	Initiated Connections	Initiated IDS	Recieved Connections	Recieved IDS
	Honeywall: 1151223232			2	0	10312	117

Figura 71: Recepción de datos a través de Sebek

Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6.3 TRAFICO GENERADO EN EL HONEYWALL

En esta comprobación del tráfico se muestran las tablas que contienen los datos analizados a través del Honeywall, de los cuales muestran el tráfico que se ha generado en la red datos de la Municipalidad Distrital de Huambos, durante los meses de, enero, febrero y marzo del 2016.

El tráfico recolectado que se ha reportado ha sido en los siguientes protocolos: SSH, ICMP, HTTP, DNS, NETBIOS, a fin de eliminar falsos positivos, tal como se muestra en la **Figura 69**

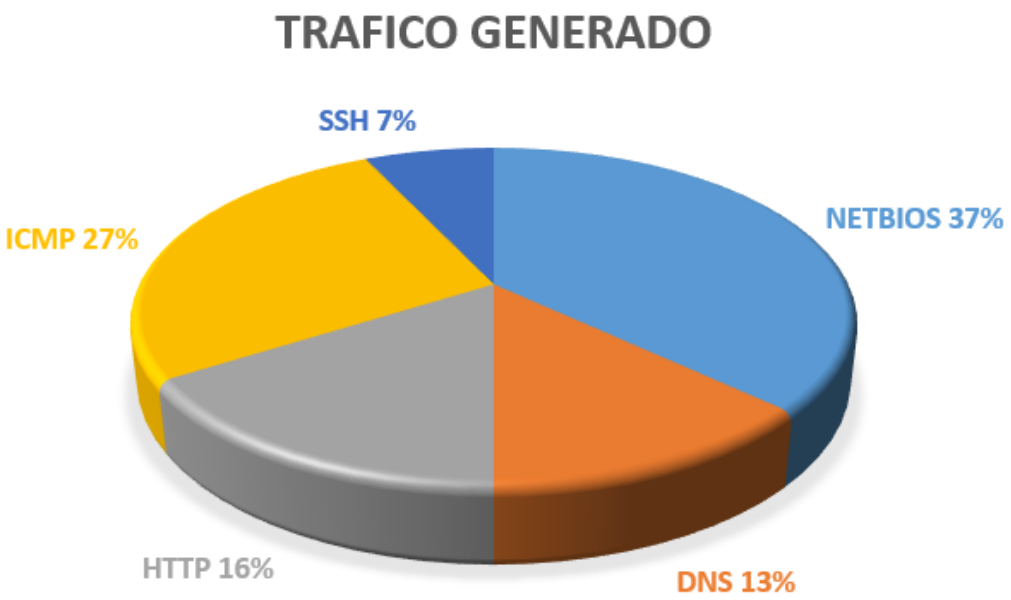


Figura 72: Tráfico Generado

Fuente: ANHMB

En la **tabla 9** se muestra un resumen detallado del tráfico generado por el protocolo SSH:

SSH	ENERO			FEBRERO			MARZO		
	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC
	132,162	1804	31	128,146	1632	24	128,162	1632	28

Tabla 10: Trafico SSH

Fuente: ANHMB

En la **tabla 10** se muestra un resumen detallado del tráfico generado por el protocolo ICMP:

ICMP	ENERO			FEBRERO			MARZO		
	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC
	1827452	765432	1203	293726	276351	3873	1626252	745130	1123

***Tabla 11*:** Trafico ICMP

Fuente: ANHMB

En la **tabla 11** se muestra un resumen detallado del tráfico generado por el protocolo HTTP:

HTTP	ENERO			FEBRERO			MARZO		
	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC
	228,116	15607	60	291,196	1996	79	218,116	15007	50

Tabla 12: Trafico HTTP

Fuente: ANHMB

En la **tabla 12** se muestra un resumen detallado del tráfico generado por el protocolo DNS:

DNS	ENERO			FEBRERO			MARZO		
	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC
	24,147	295.068	120	59,426	729.91	91	22,121	295.068	105

Tabla 13: Trafico DNS

Fuente: ANHMB

En la **tabla 13** se muestra un resumen detallado del tráfico generado por el protocolo NETBIOS:

	ENERO			FEBRERO			MARZO		
NETBIOS	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC	BYTES	PACKETS	CONEC
	9352748	567241	2401	8762567	462817	2137	8351743	465238	2205

Tabla 14: Trafico NETBIOS

Fuente: ANHMB

COMPROBACIÓN DE LA HIPÓTESIS

Para la comprobación de la hipótesis una vez que se ha analizado los ataques que han sido capturado a través de la Honeypot, se procede a especificar los intentos de ataques que han sido capturados a través del IDS y la vez el registro de incidencias en la red de datos de la MDH, donde se parcho las vulnerabilidades encontradas de los cuales se muestran en la **Figura 73, 74, 75 y Tabla 15** demostrando de esta manera que con la implementación de la tecnología Honeypot permitirá mejorar la seguridad informática a un 85% a través de la detección proactiva de ataques y simulación de objetivos vulnerables que despistaran al posible atacante informático.

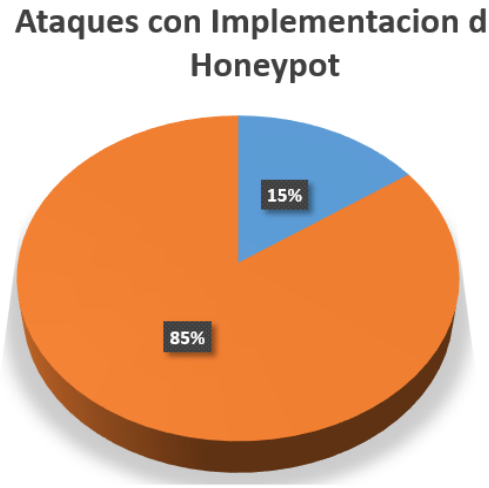


Figura 73: Mejora de la Red con la implementación del Honeypot

Fuente: ANHMB

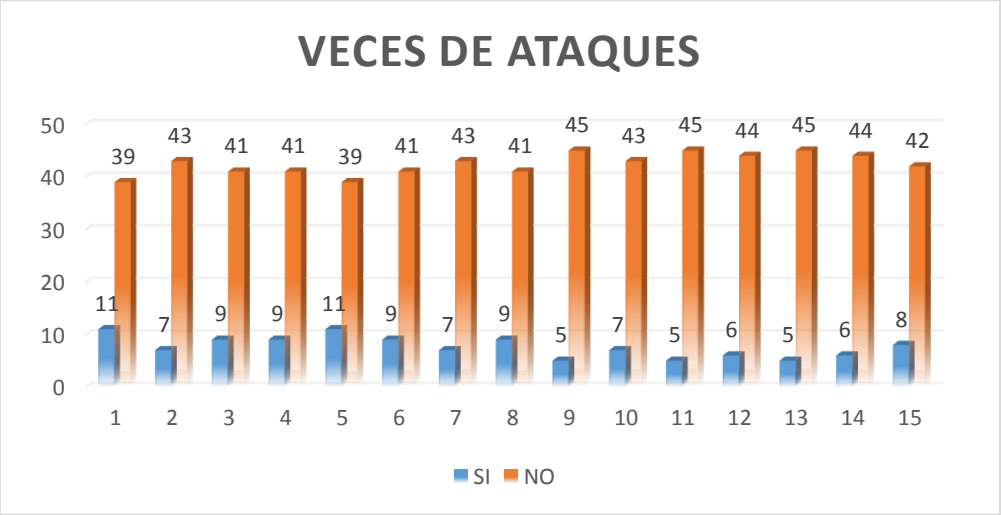


Figura 74: *Total de ataques registrados*

Fuente: ANHMB

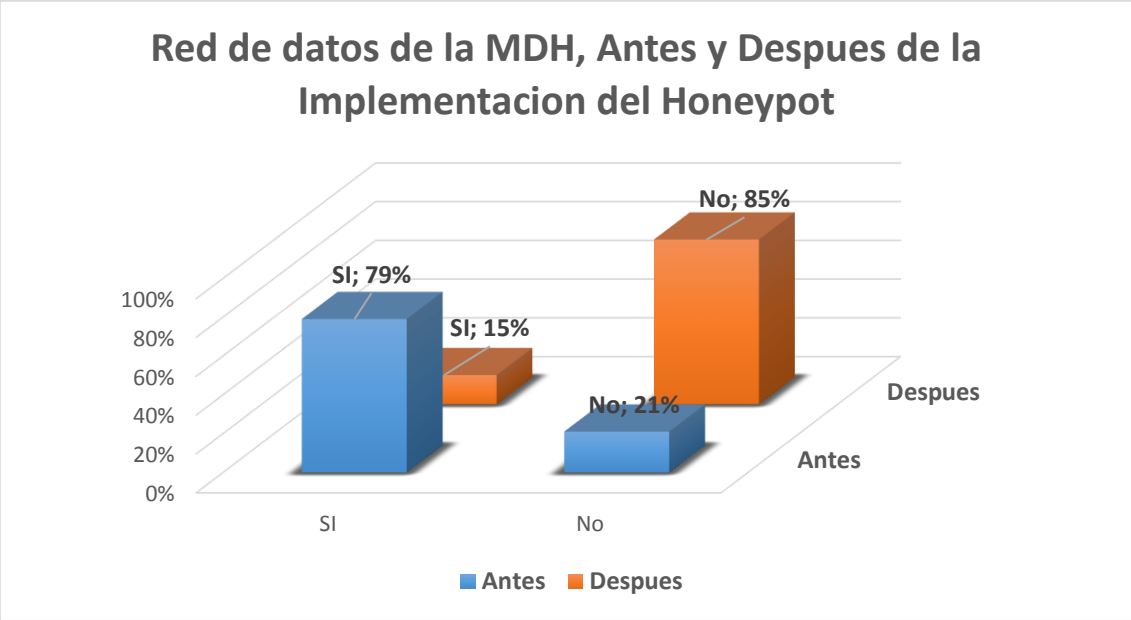


Figura 755: Red de datos de la MDH, Antes y después

Fuente: ANHMB

REGISTRO DE INCIDENCIAS EN LA RED DE DATOS DE LA MDH				
ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	2	8	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**.
script screenshot	10	1	9	
script run vnc	10	3	7	
script multicommand -cl "msg"	10	2	8	
srcrip reboot	10	3	7	
TOTAL	50	11	39	

Tabla 15: Registro de incidencias

Fuente: ANHMB

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO VII
GUÍA METODOLÓGICA

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

7.1 DESCRIPCIÓN DE LA GUÍA

La presente guía metodológica pretende ser un sustento técnico que ayudara en el diseño, instalación y configuración de una Honeynet Virtual, para lo cual se deberán realizar los siguientes pasos.

7.2 ANÁLISIS DE LA INFRAESTRUCTURA EXISTENTE

Como paso inicial es necesario el análisis de la infraestructura existente en la intranet donde se desee instalar y configurar una Honeynet virtual, paro lo cual se deberá tomar en cuenta:

- ✓ El tamaño de la red, a fin elegir el número de honeypots virtuales que se instalaran en la misma, de esta manera no se genera demasiado tráfico en redes que pueden ser susceptibles a congestionamiento, por ejemplo tormentas de broadcast.
- ✓ Los puntos de falla, estos se deberán analizar tomando en cuanta cuales pueden ser los posibles fallos de seguridad en la política informática de una institución, generalmente, estos se presentan en las redes inalámbricas, ya que las mismas poseen grandes fallos de seguridad que necesitan ser corregidos por el administrador. En el caso de no poseer red inalámbrica, el administrador deberá analizar si la red informática presenta puntos de red que puedan ser accedidos sin restricciones por el público general.
- ✓ Identificar la RED a la cual va a pertenecer la Honeynet, a fin de no tener problemas de conectividad.
- ✓ Analizar el diseño de la red existente, a fin de no crear un cuello de botella en la misma, recordando que, en la arquitectura de la Honeynet, esta

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

recolectara todos los paquetes que fluyan a través de la misma, sino se toma en cuenta esta sección, se producirán retardos en el tráfico de la red, debidos al funcionamiento erróneo de la Honeynet.

- ✓ Verificar los recursos tecnológicos de hardware a fin de decidir si la implementación de la Honeynet será de una manera física o de una manera virtual.

7.3 DISEÑO DE LA HONEYNET

Para el diseño de la Honeynet se deberá analizar qué tipo de generación será la base para nuestra implementación, se deberá tomar en cuenta lo siguiente:

7.3.1 Honeynet de Primera Generación:

- ✓ Los honeypots se encuentran en el mismo dominio de broadcast que los hosts.
- ✓ Sería necesaria la implementación de una tarjeta de red extra en el firewall a fin de conectarlo a la Honeynet.
- ✓ Si no se configura adecuadamente el IDS en una maquina robusta es probable que se produzca un cuello de botella en el mismo, lo cual ocasionaría un grave peligro a la disponibilidad de los datos empresariales.
- ✓ El router se instala con la intención de ocultar la presencia de los cortafuegos a ojos de los sistemas de la red de honeypots, de modo que cuando un intruso investigue el gateway de un sistema comprometido descubrirá un router y no unos cortafuegos.

- ✓ No es posible garantizar que todo el tráfico circule por el IDS, por el principio de una red Ethernet switcheada, de esta manera, se compromete la integridad de la Honeynet.
- ✓ El principal inconveniente que presentan las Honeynets de Primera.
- ✓ Generación tiene que ver con sus limitaciones en el control del atacante: si le permite un cierto umbral de conexiones, en el peor de los casos, sería posible que todas y cada una de estas conexiones sea un ataque exitoso y las medidas de contención habrían fracasado.

7.3.2 Honeynet de Segunda Generación

- ✓ La arquitectura, de una Honeynet de 2da generación es más sencilla que la que la de primera generación ya que tanto las tareas de control como las de captura y recolección de datos se realizan en un único sistema que el Honeynet Project denomina Honeywall.
- ✓ Esta centralización simplificará también los procesos de desarrollo y administración de la Honeynet.
- ✓ El Honeywall dispone de tres interfaces de red. La que aparece conectada al router se utiliza exclusivamente para la administración remota del sistema. Con respecto a las otras dos interfaces el sistema se va a comportar como un bridge: dichas interfaces van a carecer de direcciones IP y MAC asociadas y el sistema ni hará encaminamiento de tráfico ni decrementará el TTL de los paquetes que lo atraviesen.
- ✓ Al utilizar este tipo de topología, sólo se precisa de una máquina física, que funciona como anfitriona de la red virtual. Esto se traduce en una disminución significativa del coste del hardware y el espacio requerido por

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

la Honeynet, convirtiéndola así en la denominada Honeynet virtual o Auto contenida.

- ✓ Beneficia la administración, permitiendo centralizar y gestionar todos los sistemas de la Honeynet de modo centralizado desde el equipo anfitrión.
- ✓ El hecho de que todo se ejecute en un único equipo convierte una Honeynet en una solución “plug-and-play”.

7.4 IMPLEMENTACIÓN DE LA HONEYNET

Para la implementación de la Honeynet virtual, se deberán realizar los siguientes pasos:

- ✓ Instalación del software de virtualización VirtualBox
- ✓ Creación de una nueva máquina virtual con 3 tarjetas de red, de las cuales se encontrarán en modo host-only y 1 deberá ser configurada en modo puente.
- ✓ Instalación de Honeywall, si no se dispone de la imagen ISO del proyecto, se lo podrá descargar de https://projects.honeynet.org/honeywall.

Una vez que se ha creado la nueva máquina virtual, es necesaria la puesta en marcha de la instalación y la configuración de la Honeywall para lo cual se deben realizar los siguientes pasos:

- ✓ Formateo del disco duro e instalación automática de los componentes necesarios para la ejecución de la Honeywall.
- ✓ Ingreso a la configuración con el user **roo** y pass **honey.**
- ✓ Acceso al usuario de configuración a través del comando **su –** password **honey.**
- ✓ Leemos y verificamos si aceptamos el acuerdo de responsabilidad.

- ✓ Indicamos el método interview a fin de ingresar manualmente las configuraciones deseadas en el Honeywall.
- ✓ Ingresamos las direcciones Ips de los honeypots, de acuerdo a nuestro diseño.
- ✓ Ingresamos la dirección de red en formato CIDR.
- ✓ Ingresamos la dirección de broadcast de la red.
- ✓ El Honeywall nos indica que hemos terminado la primera parte de las configuraciones correspondiente a las direcciones Ips.
- ✓ Nos pregunta si deseamos configurar la interfaz de administración remota, le damos a yes.
- ✓ Ingresamos la dirección Ip por la que va a escuchar en modo administración remota.
- ✓ Ingresamos el gateway para la Ip de administración.
- ✓ Ingresamos el hostname con el que será identificado, para despistar lo recomendable sería ponerlo un nombre ficticio. Ejemplo serverMDH.
- ✓ Ingresamos el dominio al que pertenece el Honeywall, de no pertenecer a ningún dominio especificamos localdomain.
- ✓ Especificamos el servidor de DNS.
- ✓ Nos mostrara la confirmación si deseamos activar la interfaz de administración remota, le damos a sí.
- ✓ Nos pregunta si deseamos activar la interfaz desde en el próximo boot.
- ✓ Nos pregunta acerca de la configuración de SSH.
- ✓ Nos pregunta si deseamos que el usuario root pueda logearse remotamente.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

- ✓ De igual manera deberemos realizar el cambio de password para el usuario roo.
- ✓ Debemos escoger el puerto por el que va a escuchar la interfaz de administración.
- ✓ Ingresamos las direcciones Ips que están permitidas a administrar el
- ✓ Honeywall remotamente, sino no deseamos especificar direcciones ingresamos **"any".**
- ✓ Seleccionamos si deseamos habilitar la interfaz web de administración remota seleccionamos yes.
- ✓ Seleccionamos la opción para restringir las comunicaciones salientes.
- ✓ Ingresamos los puertos TCP salientes permitidos.
- ✓ Ingresamos los puertos UDP salientes permitidos.
- ✓ Nos muestra un mensaje indicándonos que hemos terminado con la segunda parte de la instalación de la Honeywall.
- ✓ Ingresamos el valor para la recolección de datos.
- ✓ Ingresamos el valor límite de conexiones TCP.
- ✓ Ingresamos el valor límite de conexiones ICMP.
- ✓ Ingresamos el límite de conexiones para los demás protocolos.
- ✓ Indicamos la dirección física para el archivo blacklist, el cual obtendrá las IPs que han sido banneadas manualmente.
- ✓ Indicamos la dirección física para el archivo whitelist, el cual obtendrá las IPs de confianza que han sido agregadas manualmente.
- ✓ Nos pregunta si deseamos activar el modo "Roach Motel" para lo cual seleccionamos no, ya que de hacerlo se restringirá el tráfico de los honeypots.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

- ✓ Nos muestra un mensaje indicándonos que hemos terminado con la tercera parte de la instalación de la Honeywall.
- ✓ Seleccionamos si a la opción que permite la utilización de los servidores DNS por parte de los honeypots.
- ✓ Especificamos si queremos utilizar la opción de envío de mails. Para ello deberemos tener configurado un servidor sendmail, sino el envío se realizara a localhost.
- ✓ Escogemos que la opción de alertas se active automáticamente cada vez que se reinicie el ordenador.
- ✓ Configuramos las opciones de Sebek, a fin de poder recibir datos desde los honeypots.
- ✓ Ingresamos la dirección que escuchara los paquetes Sebek desde los honeypots.
- ✓ Ingresamos el puerto UDP por el que el servidor va a escuchar los paquetes Sebek.
- ✓ Configuramos a Sebek a fin de que acepte y realice un log de todo el tráfico que es enviado a los honeypots.
- ✓ Finalmente nos muestra un cuadro en el que podemos ver que las configuraciones del Honeywall han sido culminadas.
- ✓ Una vez que ha terminado la instalación y configuración preliminar de la Honeywall, ya podemos abrir un navegador e ingresar https://[direccion_ip_de_administracion_remota].
- ✓ Ingresamos el user y pass y a continuación el Honeywall nos mostrara la pantalla de resumen con los principales resúmenes de la actividad que ha loggeado hasta el momento.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

7.5 VERIFICACIÓN DEL DISEÑO

Para la verificación del diseño, se deben realizar los siguientes pasos:

1. Configuración de Fecha y hora

Propósito: Correcta configuración de la fecha y hora del Honeywall y Honeypots.

Descripción: La instalación de los Sistemas Operativos por lo general nunca configura la hora y fecha actual, podemos tener una Honeynet con dispositivos con horas y fechas diferentes. Esto afecta en la recolección de datos, las estampas de tiempo en los logs no corresponderían impidiendo realizar un rastreo de un ataque.

Pasos:

- ✓ Chequear la fecha y hora en el Honeywall, usando el comando “date”.
- ✓ Verificar que corresponde la fecha y hora actual, caso contrario configurarla usando “date –s “fecha””.
- ✓ Chequear la fecha y hora en los Honeypots, usando el comando “date” para Linux y “time” Windows.
- ✓ Verificar que corresponde la fecha y hora actual, caso contrario configurarla usando “date” o “time”.

2. Los Honeypots deben poder establecer conexiones entrantes y salientes a la red interna usando el protocolo IP.

Propósito: Los Honeypots accedan en ambas direcciones a la red interna.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Descripción: Cuando una máquina no tiene acceso a la red lo primero que se verifica es su conexión, verificar el cableado, para las conexiones lógicas hay que revisar que correspondan las configuraciones de las interfaces de red virtuales (modo bride o modo host-only), revisar que la máquina física (Host) este correctamente conectada a la red, luego revisar si el firewall de Honeywall está funcionando, revisar que no esté bloqueando paquetes, revisar algún firewall instalado en los Honeypots (como el firewall de Windows.)

Pasos:

• Ping a cada Honeypot desde la máquina de pruebas, ejecutando ping <IP>

• Verificar que se obtiene respuesta con mínimo 4 ECHO replies desde la Honeypot.

• Ping la máquina de pruebas desde los Honeypots, ejecutando ping <IP>

• Verificar que se obtiene respuesta con mínimo 4 ECHO replies desde la máquina de pruebas.

3. Los Honeypots deben resolver nombres de dominio usando los DNS.

Propósito: Los Honeypots deben resolver los nombres de dominio.

Descripción: Es necesario para el correcto funcionamiento de los Honeypots, que puedan resolver nombres de dominio.

Pasos:

• Ejecutar “nslookup www.google.com” o “ping www.google.com” en los Honeypots.

• Verificar la correcta resolución de nombre para el dominio www.google.com

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4. El Honeywall está registrando el tráfico. Propósito: Garantizar el registro de tráfico en el Honeywall

Descripción: En el Honeywall puede no estar levantado Snort, para hacerlo en el menú seleccionar “Recargar Honeywall”

Pasos:

- ✓ Ingresar al Honeywall como root
- ✓ Seleccionar IP PROTO-> ICMP -> Result Format-> Wall Eye flow view
- ✓ Verificar las entradas con el protocolo ICMP correspondientes a los Ping realizados en pruebas anteriores.

5. Walleye está activado y permite ingresar con el usuario.

Propósito: La herramienta gráfica de análisis “Walleye” incluida en el Honeywall esté activa y correctamente configurada.

Descripción: Muchas veces el demonio http no se encuentra levantado o la IP para la administración no está configurada. Verificar que en el Honeywall este configurada “Would you like to configure a magnament interface” con “Yes”, y reiniciar el Honeywall verificando que http se levante.

Pasos:

- ✓ Conectar la máquina de pruebas a la interface de administración, configurar la IP correspondiente e ingresar a “https://IPADMISTRACION/’
- ✓ Ingresar el usuario y contraseña
- ✓ Verificar que el acceso este correcto

6. Walleye muestra el tráfico registrado por el Honeywall.

Propósito: Verificar que Walleye muestre el tráfico registrado por Snort en el

Honeywall.

Descripción: Walleye es la principal herramienta de análisis, es necesario verificar que muestre los registros de Snort, en caso de que no lo haga se debe a una mala instalación, se procede a reinstalar el Honeywall.

Pasos:

Ingresar en Walleye

En la pantalla principal deberíamos poder ver de manera gráfica el tráfico que está siendo capturado por el Honeywall

7. Honeywall envía mensajes de alerta.

Propósito: Garantizar que el Honeywall envía emails de alerta.

Descripción: El Honeywall no podrá enviar email si el puerto 25 no aceptando conexiones, o si no se ha configurado un email válido.

Pasos:

- ✓ En uno de los Honeypot generar paquetes ICMP hasta completar el límite permitido, (ping IP).
- ✓ Revisar la bandeja de entrada del correo configurado en el Honeywall por un email de alerta.

8. Sebek está funcionando en los Honeypots y enviando datos.

Propósito: Garantizar que el Cliente Sebek está enviando datos y el Servidor Sebek los recibe.

Descripción: Si no se recibe datos del Sebek puede ser por una mala configuración en los parámetros de red, el cliente Sebek para Windows sigue

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

funcionando aún después reiniciar el sistema, pero el Cliente Sebek de Linux requiere ser instalada cada vez que se inicia el Sistema Operativo

Pasos:

- ✓ Generar datos para el Sebek, para Windows ingresar comandos en la consola, en Linux conectarse por SSH a un Honeypot e ingresar comandos.
- ✓ Ingresar en Walleye y verificar los datos capturados por el Servidor Sebek, están marcados con la etiqueta “Sebeked”

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

VIII. CONCLUSIONES Y RECOMENDACIONES

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

8.1 CONCLUSIONES

Mediante la selección de ataques típicos en la red de datos de una Municipalidad, se encontró que el 70 % pertenece a la vulnerabilidad MS09-001 correspondiente al Servicio SMB Netbios, el cual se debe a la gran cantidad de hosts que corren bajo sistema operativo Windows XP SP2.

Para la simulación de los principales ataques de seguridad informática se utilizó la distribución de GNU/Linux Kali, la cual cuenta con herramientas que nos permiten atacar servidores y estaciones de la misma manera que lo haría un posible intruso.

De los ataques realizados antes de la implementación se pudo comprobar que se realizaron 750 ataques registrados de los cuales el 79 % ingreso exitosamente y el 21 % no ingreso, demostrando que la red de la MDH es muy Vulnerable a los ataques.

Al implementar el Honeypot se comprobó que es un importante recurso informático que permite simular objetivos vulnerables en una red de datos, para así despistar la atención del atacante y poder tomar las respectivas acciones por parte del administrador de red.

Al evaluar los resultados obtenidos se pudo concluir que el sistema ha funcionado correctamente y ha logrado detectar los diferentes ataques que se ha llevado acabo, generando las respectivas alertas; logrando así tener un monitoreo de todo el tráfico que circula por la red.

De los ataques evaluados con la implementación se pudo comprobar que se realizaron 750 ataques registrados de los cuales el 15 % ingreso exitosamente y el 85 % no ingreso, demostrando que la red de la MDH mejoró notablemente.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Al realizar la guía de prevención, diseño, implementación y verificación de la tecnología Honeynet se ha creado un documento técnico que podrá servir como base para futuras investigaciones en el campo de la seguridad informática, específicamente en el área de la simulación de objetivos vulnerables a través de la tecnología Honeypot.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

8.2 RECOMENDACIONES

Se recomienda al administrador de red de la MDH sensibilizar a los usuarios finales con capacitación de prevención de delitos informáticos, robo de información.

Se recomienda al administrador de red de la MDH que al implementar la Honeypot se debe tener en cuenta la protección de datos y responsabilidades por cualquier daño que es capaz de causar el atacante. Por tanto, es importante un monitoreo constante de la red y ubicar la Honeynet en una zona donde no comprometa a ningún sistema y evitar que alguna red sufra daños.

Se recomienda analizar exhaustivamente la infraestructura disponible antes de realizar el diseño de la Honeypot, a fin de evitar posibles cuellos de botella que podrían ocasionar el mal funcionamiento de la red.

Una vez que los resultados de vulnerabilidades han sido obtenidos, se recomienda la planificación y ejecución de una política de seguridad que permita gestionar y reparar dichas vulnerabilidades informáticas

Se recomienda actualizar constantemente la base de datos del IDS a fin de gestionar las nuevas vulnerabilidades que se sigan descubriendo, así como tratar en lo posible de eliminar los falsos positivos

Tener especial cuidado al momento de la instalación y ejecución de Sebek puesto que este será el motor para la recolección de los datos entregados hacia la Honeynet.

Se recomienda continuar con la investigación acerca de tecnologías involucradas en la seguridad informática como es el caso de los honeypots y

Honeynets, puesto que este nos brindara un mecanismo proactivo de alertas frente a posibles ataques informáticos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

REFERENCIAS

Katz, M. (2013). Redes y seguridad, Editorial: Alfa-omega, pp. 1-100.

Soriano, M. (2014). Seguridad en redes y seguridad de la información. Czech Republic: České vysoké učení technické v Praze .

Zongjian, W. (2013). “Intrusion Prevention System Design”. Springer London, Springer-Verlag London, pp. pp 375-382.

Olivier, T. & Viinikka, C. & Marc, D. (2011). “Automating the Analysis of Honeypot Data,” de Automating the Analysis of Honeypot Data. Cambridge, MA, USA, Springer Berlin Heidelberg, pp. pp 406-407.

Magalhaes, R. (2011). Understanding Virtual Honeynets. Ed12, pp 1.

Spitzner, L. (2003). Honeypots: Tracking Hackers. Editorial: Addison-Wesley, ISBN 0321108957.

The Honeynet Project. Know Your Enemy: Learning About Security Threats (2nd Edition). Editorial: Addison-Wesley, ISBN 0321166469.

Bylaws, O. (2010). “The Honeynet Project” (Enero 2010). Recuperado de: https://www.honeynet.org/project.

Graves, K. (2010). CEH: Certified Ethical Hacker Study Guide, USA: Sybex.

NIELS PROVOS. Virtual Honeypots. Chicago-EEUU, Kindle, 2010 420p

GARCÍA FERNÁNDEZ NÉSTOR. (1999). Administración de Redes de

Ordenadores. Madrid-España, Frikis, Pp 2-9

UNAM CERT. (2010). Universidad Autónoma de México. Recuperado el 5 de Septiembre de 2010, de PAPERS Proyecto Honeynet UNAM: http://www.honeynet.unam.mx/es/papers.pl

UTPL. (2010). Universidad Técnica Particular de Loja. Recuperado el 10 de Septiembre de 2010, de Proyecto Honeynet: http://www.utpl.edu.ec/honeynet/

Comunidad Underground de México. (08 de Junio de 2010). Recuperado el 12 de Agosto de 2010, de Paper Cyber Crimen y el Nacimiento de la Informática forense + HoneyPots : https://www.underground.org.mx/index.php?action=printpage;topic=25638.0

CEPEU. (2010). Recuperado el 20 de Septiembre de 2010, de Seguridad Informática: Pilares Básicos: http://www.cepeu.edu.py/LIBROS_ELECTRONICOS_3/lpcu082%20-%2001.pdf

Honeyd. (2010). Recuperado el 07 de Septiembre de 2010, de Virtual Honeypots: http://www.honeyd.org.

Honeypots. (2010). Recuperado el 5 de Septiembre de 2010, de Herramientas de seguridad de la Información: http://honeypots.wordpress.com/

IETF. (2004). Recuperado el 27 de Julio de 2010, de IDWG - Intrusion Detection Working Group: http://datatracker.ietf.org/wg/idwg/charter/.

Kuehl, K. (2002). The Honeynet project: Advancements in Honeypot tools. Recuperado el 23 de Julio de 2010, de Presentacion sobre The Honeynet project: Advancements in Honeypot tools: http://www.google.com.ec/url?sa=t&source=web&cd=1&ved=0CBQQFjAA&url=http%3A%2F%2Fwinfingerprint.sourceforge.net%2Fpresentations%2Fhoneynet _projectmexico2003. ppt&ei=KNpJTIT8MIP_8AbkqtzBDg&usg=AFQjCNE4MiwXqBPTUuTSzWr3SsM3Xfdg1A&sig2=JTZH4gUlidpX48C51qISfA

The Honeynet Proyect. (1999). Recuperado el 23 de Junio de 2010, de Sitio Web Home del Honeypot Proyect: http://www.honeynet.org/

The Honeynet Proyect. (2010). Recuperado el 23 de Julio de 2010, de Capitulos o Chapters de diversos paises: http://www.project.honeynet.org/og

Jose Fabián Roa Buendía. (2013). Seguridad informática. [aut. libro] Jose Fabián Roa Buendía. Seguridad informática. Madrid : McGraw-Hill, 2013, pág. 14.

Quezada Reyes, M.C Cintia y López Bar, M.C Jaquelina. 2004. Fundamentos de Seguridad Informática. Mexico DF : UNAM, 2004.

Skoudis, Edward. 2006. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. USA : s.n., 2006.

ANEXO A1

Configuración de los servicios en Honeywall

Virtualización en el software del VirtualBox.

El sistema Honeywall, está basado en distribuciones de CentOS Y Fedora. Y está diseñado para implementar una red trampa independiente. Las características que se necesitan para la instalación son las siguientes;

La memoria RAM: 2048 Mb

Disco duro: 50 Gb

Tarjetas de red: eth0, eth1, eth2

El tamaño en disco es de gran prioridad, debido a que alojara una gran cantidad de información para tener mayor almacenamiento usaremos 50GB.

En cuenta a las tarjetas de red que usaremos en los siguientes modos;

eth0: Interfaz externa, conectada a la red de producción.

eth1: Interfaz interna, conectada a los sistemas trampa. Esta es la interfaz sobre la que escucha Snort, incluyendo la recolección de todos los paquetes de Sebek.

eth2: Esta es utilizada para administración remota. En un desarrollo en modo puente, esta es la única interfaz que tiene una pila IP.

El cual se detalla en la **FIGURA I 01**

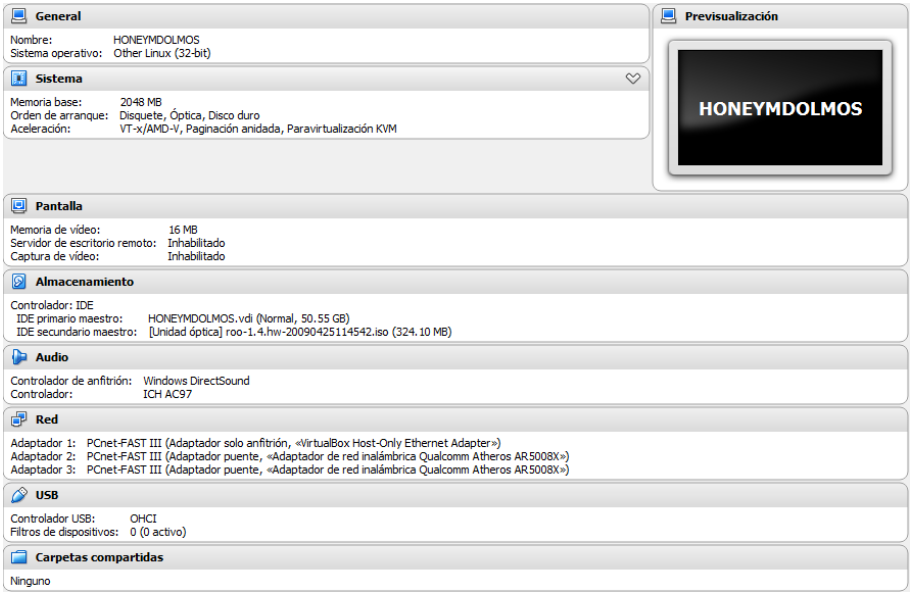


Figura A1 1: Creación de máquina virtual

Una vez creada la máquina virtual, procedemos a colocar la imagen del CD-ROM donde está el sistema Honeywall como medio de arranque. Al iniciar la instalacion en la máquina virtual aparece en la ventana “The Honeynet PROJECT”, para proceder con la instalación presionamos la tecla (ENTER) detalla en la **FIGURA I 02**

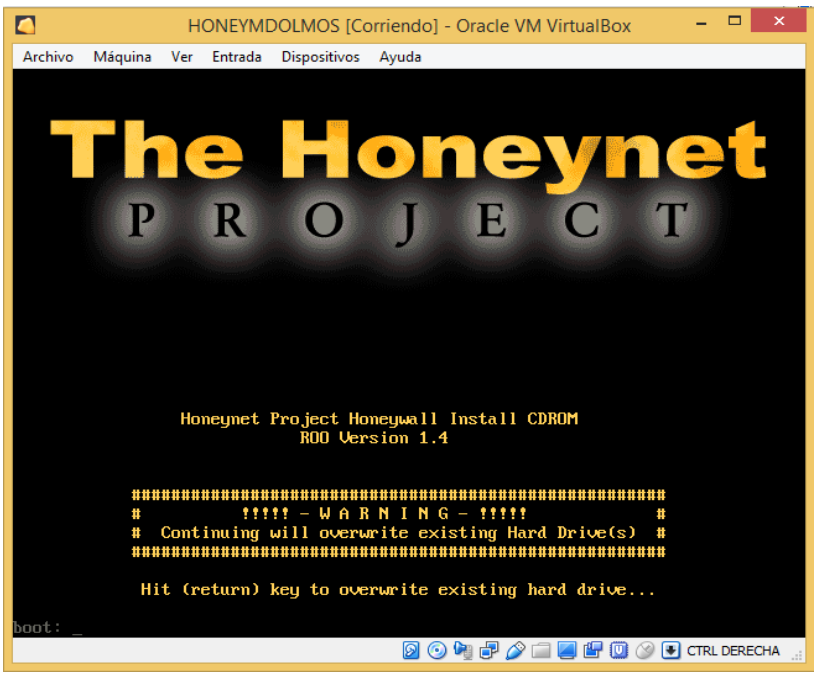


Figura A1 2: Inicio de la instalación del Honeywall

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

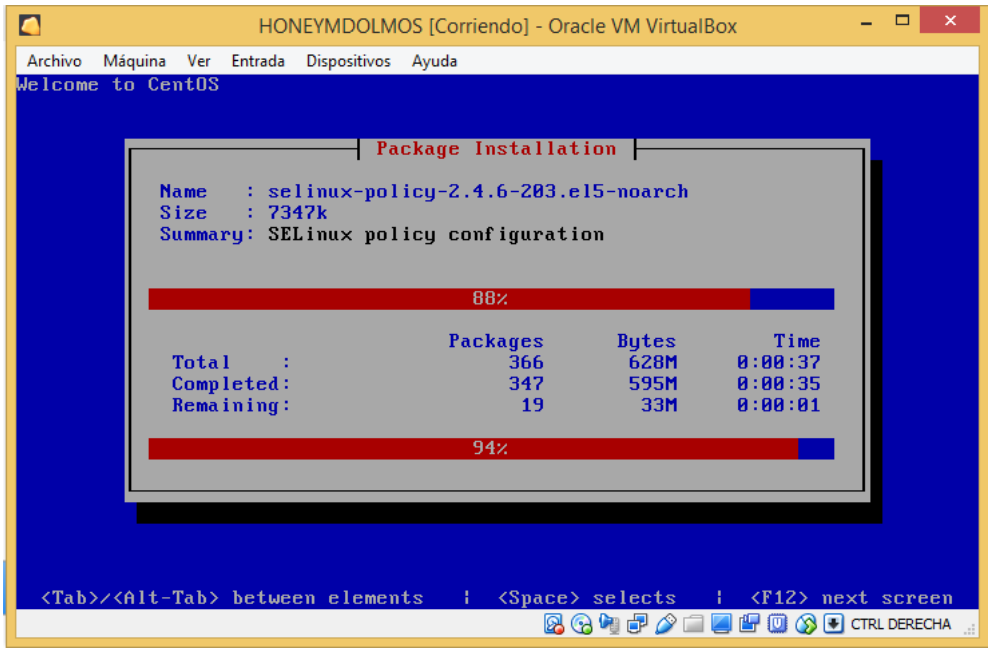


Figura A1 3: Fase de instalación del Honeywall

Después de que la instalación se ha completado con éxito, se reinicia automáticamente, al iniciar se presenta una consola de comando, donde se podrá iniciar sesión y comenzar el proceso de configuración del Honeywall.

Usuario por defecto (**roo y root**) y Contraseña (**honey**)

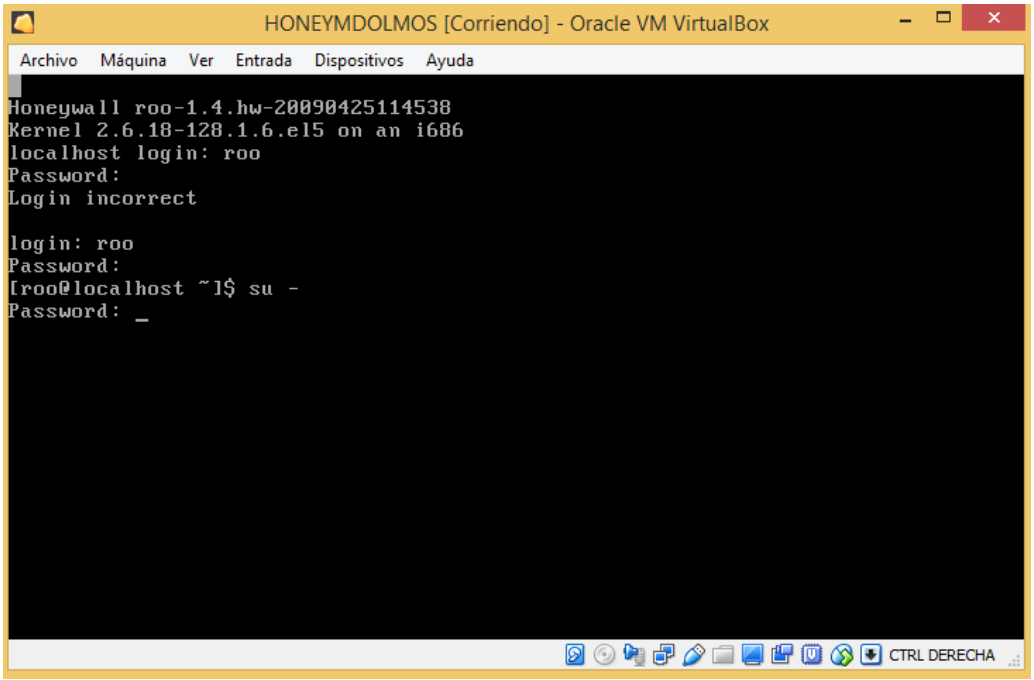


Figura A1 4: Inicio de sesión del Honeywall

Digitamos en la ventana del termina el comando “/dlg/dialogmenu.sh”

Una vez validado el usuario, nos carga el contra y licencia que debemos leer detenidamente, teniendo en cuenta los riegos que se presentan al instalar este tipo de herramientas que son debidamente controlados por el administrador.

Constan tres métodos de instalación, no está por demás saber el tipo de configuración de cada uno de ellos.

- ✓ **Floppy:** Utiliza un Disquete, como medio de configuración.
- ✓ **Defaults:** Esta configuración utiliza el valor por defecto de un Honeywall.
- ✓ **Interview:** Se utilizara para configurar nuestro primer Honeywall, aquí se utiliza el paso a paso. El cual se selecciona para empezar nuestra configuración.

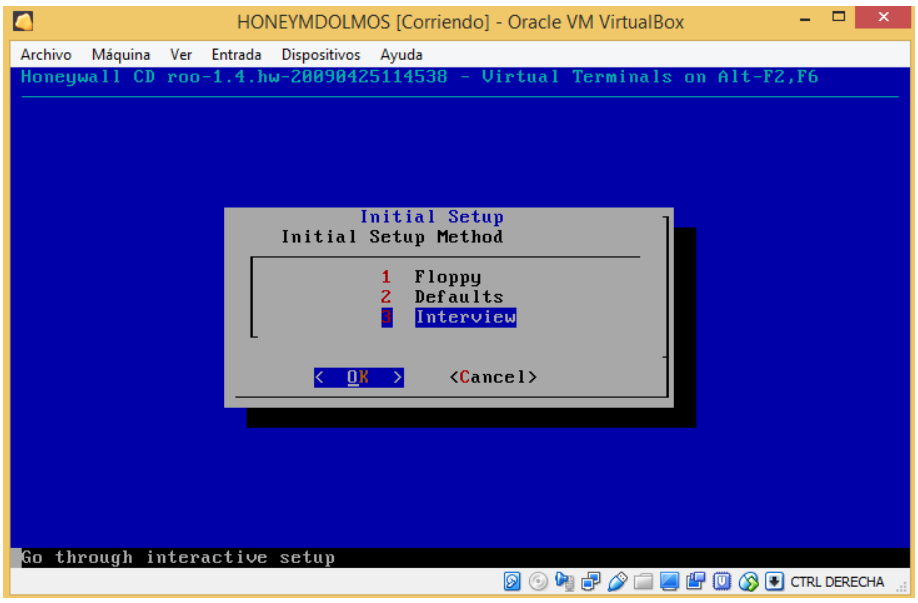


Figura A1 5: Selección del tipo de configuración

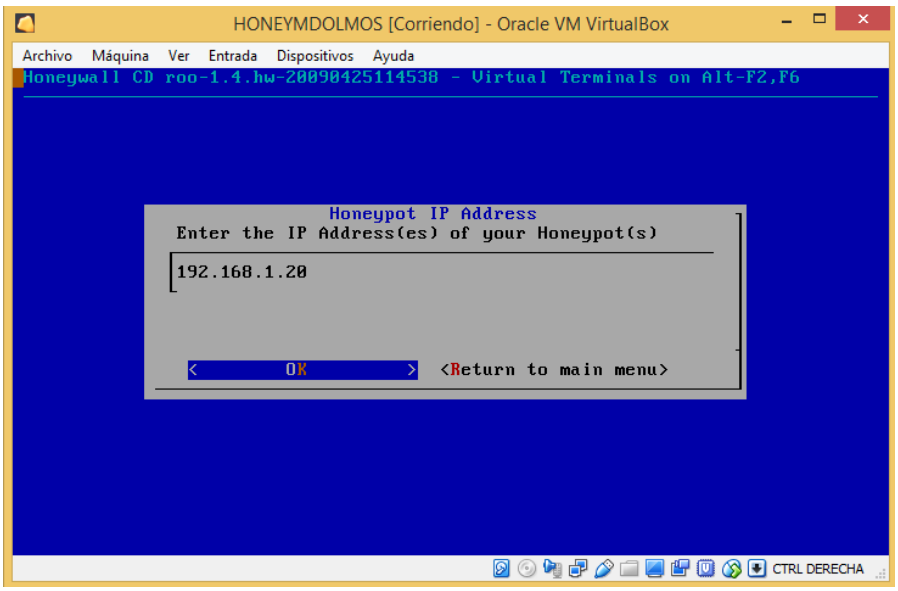


Figura A1 6: Ingreso de la dirección IP del Honeypot

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Al terminar con la configuración de las direcciones IP de las interfaces eth0, eth1 y eth2, se inicia la configuración de los servicios y puertos accesibles a nuestro Honeywall.

Configuración del puerto SSH

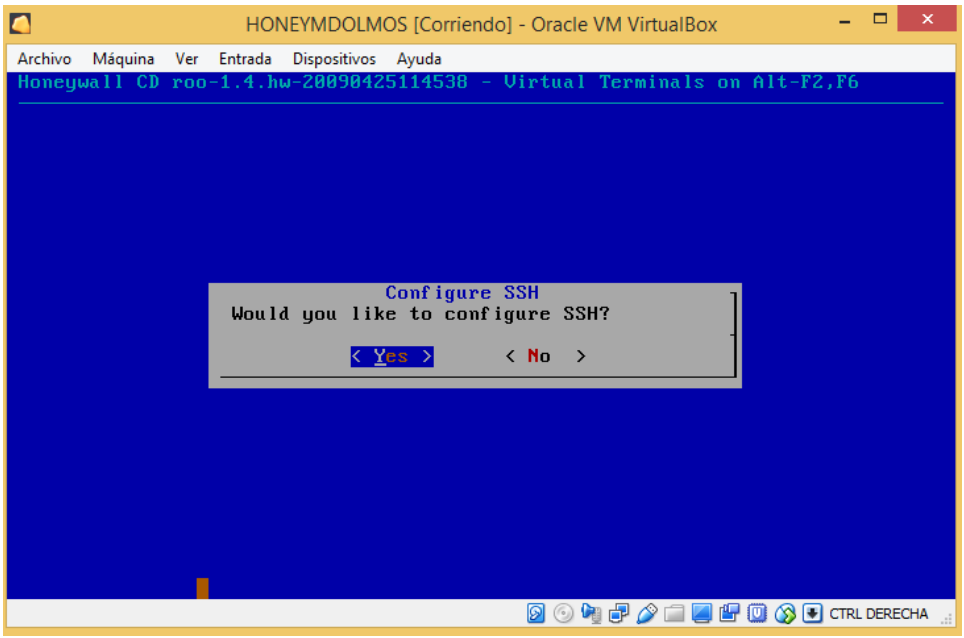


Figura A1 7: Iniciar la configuración de SSH

Adicionalmente se configuramos las contraseñas para acceder por línea de comandos, con el nivel de usuario roo y root, para revisar los nivele de seguridad establecidos en nuestra configuración.

El admin del Honeywall debe configurar los puertos 22 y 443 que permiten el acceso remoto SSH y conexión segura para HTTPS a través de la web. Así también como los puertos TCP y UDP de la RED. **VER FIGURA I 08**

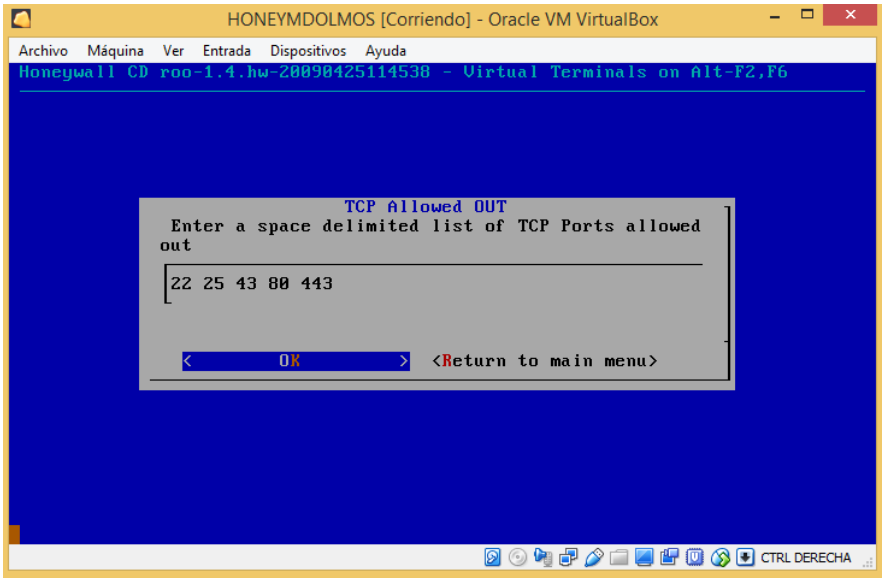


Figura A1 8: Ingreso de los puertos TCP que permiten la salida

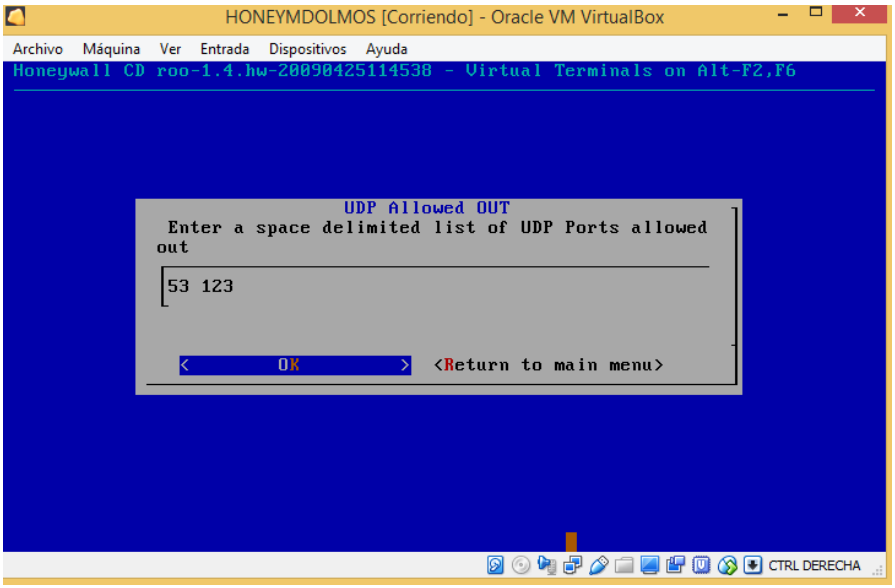


Figura A1 9: Ingreso de los puertos UDP que permitan la salida

Snort Inline

Permite el acceso a paquetes del iptables, creando una serie de direcciones para poder acceder o restringir.

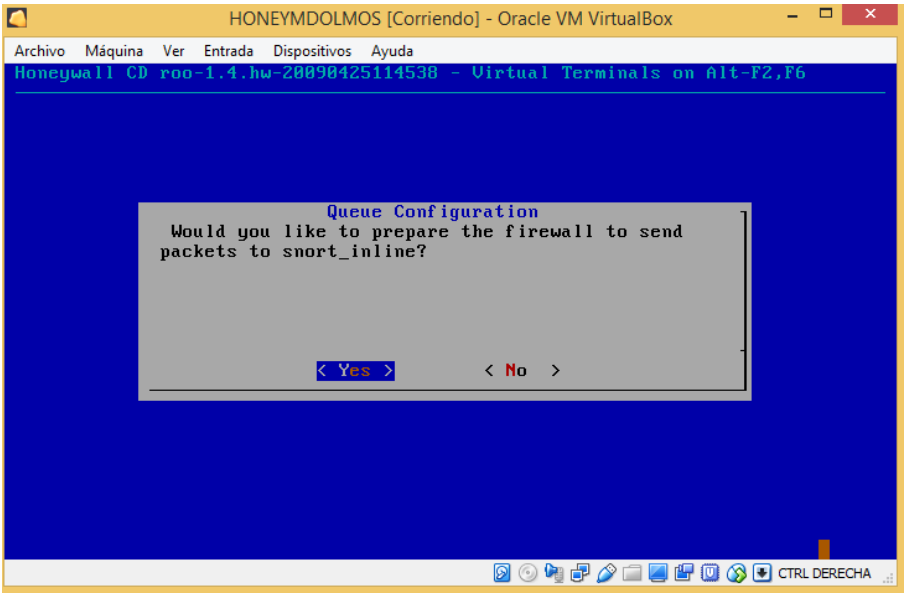


Figura A1 10: Activar el snor-inline para evitar el tráfico malicioso a la red.

ACCESO NO PERMITIDO

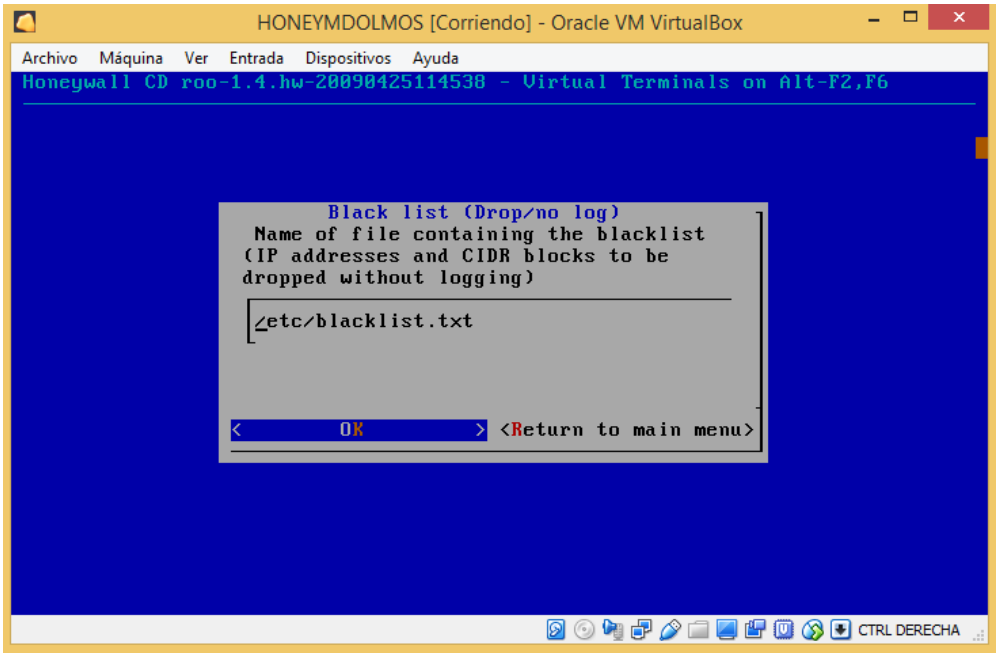


Figura A1 11: Nombre del archivo que contiene la ubicación de las direcciones IPs que generan SPAM (Blacklist).

ACCESO PERMITIDO

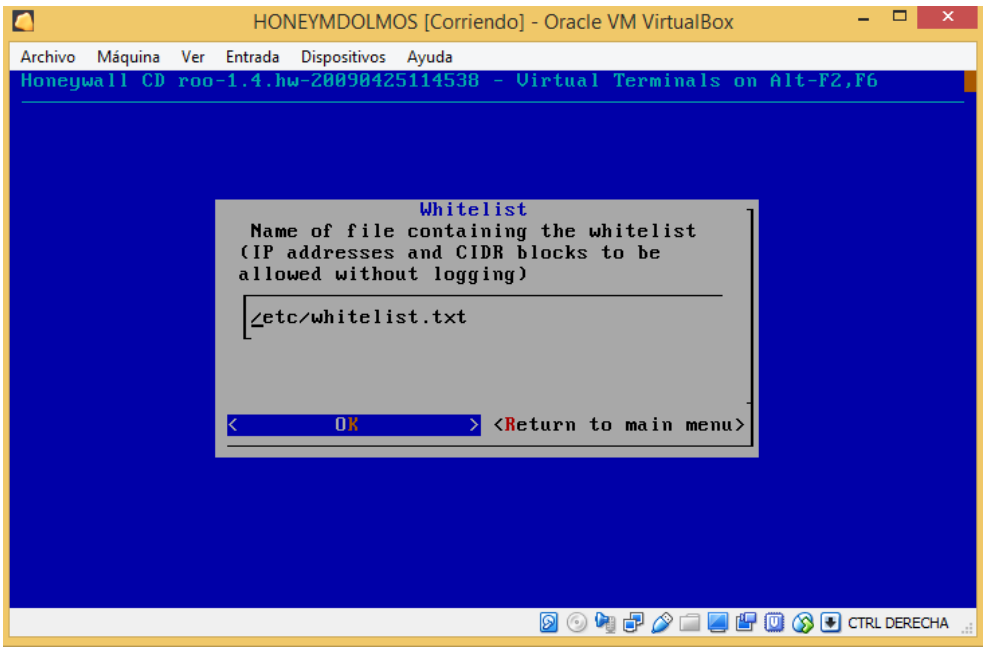


Figura A1 12: Nombre del archivo que contiene la ubicación las direcciones IPs que nunca generan SPAM (WhiteList)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Al finalizar con toda la configuración, tendremos que corroborar los documentos del Honeywall, para que toda configuración se almacena en una copia de seguridad no se pueda perder nada de información.

SEBEK

Es una herramienta patentada a "The Honeynet PROJECT", donde configuraremos el Servidor dentro del Honeywall, el cliente se configura el Honeypot o una terminal localizable en la red.

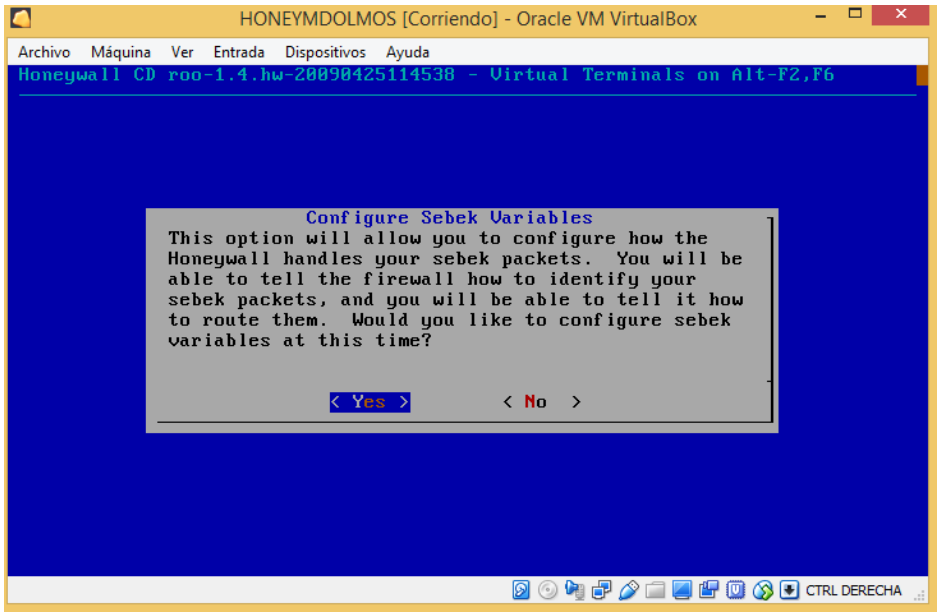


Figura A1 13: Configuración de las variables del Sebek

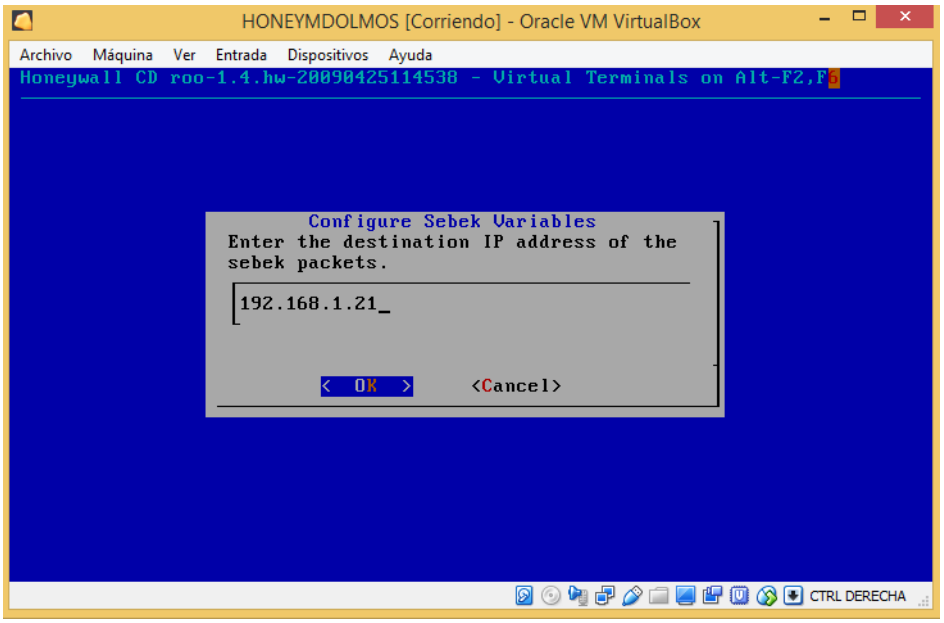


Figura A1 14: Ingreso de la dirección IP del Sebek

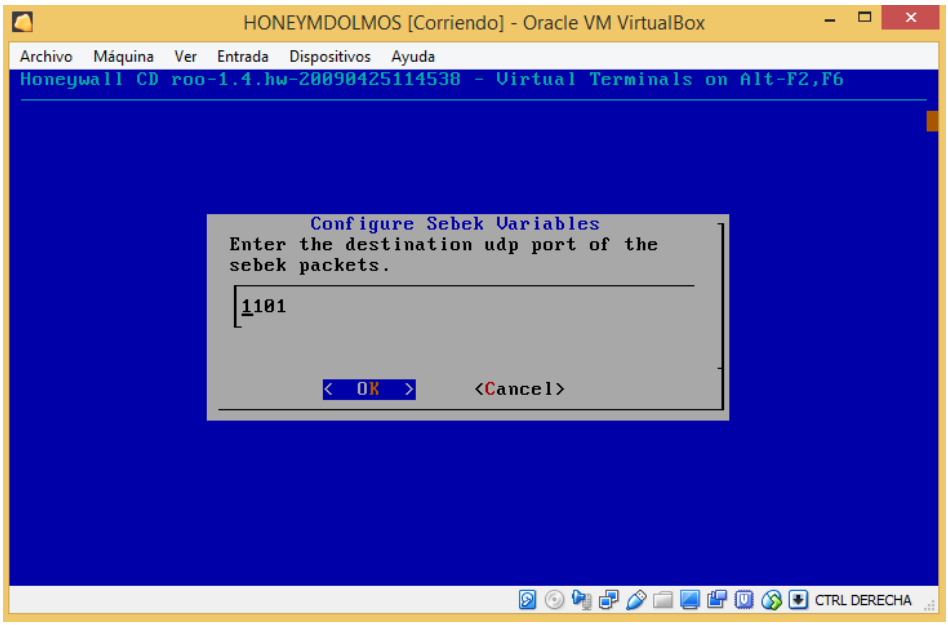


Figura A1 15: Ingreso del puerto del Sebek

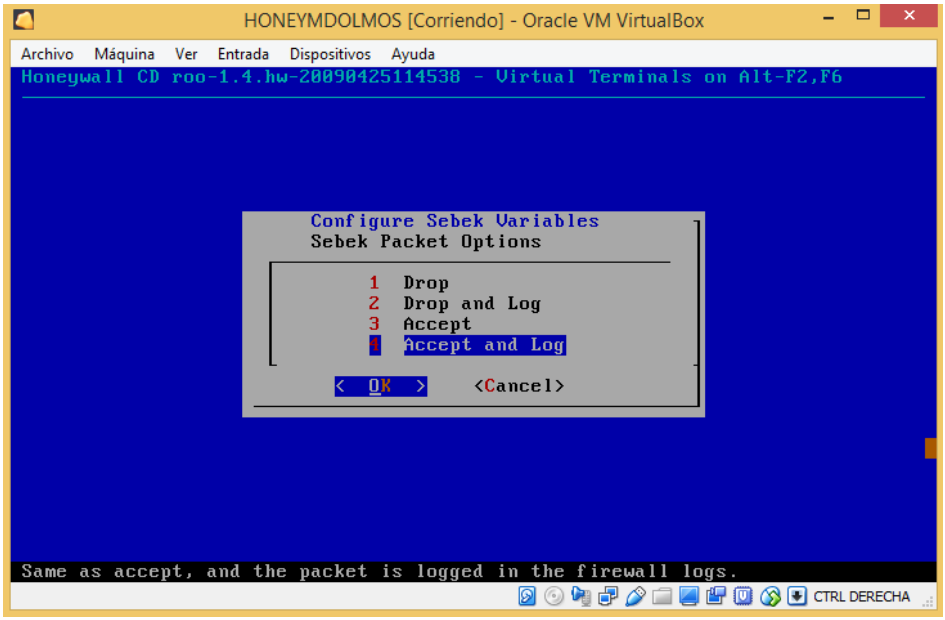


Figura A1 16: Finalizamos y aceptamos para su reinicio del Honeywall

Al reiniciar el servidor de la configuración dada del Honeywall podemos ver los log generados con el comando “/var/log”.

Anexo A2

En el Registro de incidencias de las pruebas de ataques realizados durante el diagnostico de situación actual de la red de datos de la Municipalidad Distrital de Huambos antes de la Implementación del Honeypot

Prueba 01

Computador 01

IP: 192.168.1.10

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-01:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	6	4
script screenshot	10	7	3
script run vnc	10	8	2
script multicommand -cl "msg"	10	9	1
srcrip reboot	10	9	1
TOTAL	50	39	11

Tabla A2 - 1: Computador 01
Fuente: Elaboración Propia

Prueba 02

Computador 02

IP: 192.168.1.11

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-02:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	7	3
script screenshot	10	9	1
script run vnc	10	8	2
script multicommand -cl "msg"	10	7	3
srcrip reboot	10	9	1
TOTAL	50	40	10

Tabla A2 - 2: Computador 02
Fuente: Elaboración Propia

Prueba 03

Computador 03

IP: 192.168.1.12

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente A2-03:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	9	1
script screenshot	10	7	3
script run vnc	10	6	4
script multicommand -cl "msg"	10	8	2
srcrip reboot	10	8	2
TOTAL	50	38	12

Tabla A2 - 3: Computador 03
Fuente: Elaboración Propia

Prueba 04

Computador 04

IP: 192.168.1.13

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-04:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	8	2
script screenshot	10	9	1
script run vnc	10	6	4
script multicommand -cl "msg"	10	3	3
srcrip reboot	10	8	2
TOTAL	50	38	12

Tabla A2 - 4: Computador 04
Fuente: Elaboración Propia

Prueba 05

Computador 05

IP: 192.168.1.14

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-05:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	8	2
script screenshot	10	9	1
script run vnc	10	7	3
script multicommand -cl "msg"	10	9	1
srcrip reboot	10	7	3
TOTAL	50	40	10

Tabla A2 - 5: Computador 05
Fuente: Elaboración Propia

Prueba 06

Computador 06

IP: 192.168.1.15

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-06:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	7	3
script screenshot	10	8	2
script run vnc	10	9	1
script multicommand -cl "msg"	10	8	2
srcrip reboot	10	9	1
TOTAL	50	41	9

Tabla A2 - 6: Computador 06
Fuente: Elaboración Propia

Prueba 07

Computador 07

IP: 192.168.1.16

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-07:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	8	2
script screenshot	10	7	3
script run vnc	10	9	1
script multicommand -cl "msg"	10	6	4
srcrip reboot	10	8	2
TOTAL	50	36	14

Tabla A2 - 7: Computador 07
Fuente: Elaboración Propia

Prueba 08

Computador 08

IP: 192.168.1.17

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-08:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	9	1
script screenshot	10	8	2
script run vnc	10	9	1
script multicommand -cl "msg"	10	8	2
srcrip reboot	10	7	3
TOTAL	50	41	9

Tabla A2 - 8: Computador 08
Fuente: Elaboración Propia

Prueba 09

Computador 09

IP: 192.168.1.18

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-09:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	7	3
script screenshot	10	9	1
script run vnc	10	8	2
script multicommand -cl "msg"	10	7	3
srcrip reboot	10	9	1
TOTAL	50	40	10

Tabla A2 - 9: Computador 09
Fuente: Elaboración Propia

Prueba 10

Computador 10

IP: 192.168.1.19

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-10:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	9	1
script screenshot	10	7	3
script run vnc	10	8	2
script multicommand -cl "msg"	10	6	4
srcrip reboot	10	9	1
TOTAL	50	39	11

Tabla A2 - 10: Computador 10
Fuente: Elaboración Propia

Prueba 11

Computador 11

IP: 192.168.1.20

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-11:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	8	2
script screenshot	10	9	1
script run vnc	10	7	3
script multicommand -cl "msg"	10	9	1
srcrip reboot	10	8	2
TOTAL	50	41	9

Tabla A2 - 11: Computador 11
Fuente: Elaboración Propia

Prueba 12

Computador 12

IP: 192.168.1.21

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-12:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	9	1
script screenshot	10	7	3
script run vnc	10	8	2
script multicommand -cl "msg"	10	9	1
srcrip reboot	10	7	3
TOTAL	50	40	10

Tabla A2 - 12: Computador 12
Fuente: Elaboración Propia

Prueba 13

Computador 13

IP: 192.168.1.22

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-13:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	7	3
script screenshot	10	9	1
script run vnc	10	9	1
script multicommand -cl "msg"	10	8	2
srcrip reboot	10	9	1
TOTAL	50	42	8

Tabla A2 - 13: Computador 13
Fuente: Elaboración Propia

Prueba 14

Computador 14

IP: 192.168.1.23

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-14:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	9	1
script screenshot	10	7	3
script run vnc	10	8	2
script multicommand -cl "msg"	10	7	3
srcrip reboot	10	9	1
TOTAL	50	40	10

Tabla A2 - 14: Computador 14
Fuente: Elaboración Propia

Prueba 15

Computador 15

IP: 192.168.1.24

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-15:

ATAQUES	VECES	INGRESO	
		SI	NO
scribt sysinfo	10	8	2
script screenshot	10	9	1
script run vnc	10	7	3
script multicommand -cl "msg"	10	9	1
srcrip reboot	10	8	2
TOTAL	50	41	9

Tabla A2 - 15: Computador 15
Fuente: Elaboración Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Anexo A3

En el registro de incidencias de las pruebas realizadas con la implementación del honeyot que nos permitirá la corrección vulnerabilidades previamente encontradas en la red de datos de la Municipalidad Distrital de Huambos.

Prueba 01

Computador 01

IP: 192.168.1.10

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-01:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	2	8	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**.
script screenshot	10	1	9	
script run vnc	10	3	7	
script multicommand -cl "msg"	10	2	8	
srcrip reboot	10	3	7	
TOTAL	50	11	39	

Tabla A3 - 1: Computador 01
Fuente: Elaboración Propia

Prueba 02

Computador 02

IP: 192.168.1.11

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-02:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	1	9	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**.
script screenshot	10	2	8	
script run vnc	10	1	9	
script multicommand -cl "msg"	10	2	8	
srcrip reboot	10	1	9	
TOTAL	50	7	43	

Tabla A3 - 2: Computador 02
Fuente: Elaboración Propia

Prueba 03

Computador 03

IP: 192.168.1.12

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-03:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	2	8	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**.
script screenshot	10	1	9	
script run vnc	10	3	7	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	2	8	
TOTAL	50	9	41	

Tabla A3 - 3: Computador 03
Fuente: Elaboración Propia

Prueba 04

Computador 04

IP: 192.168.1.13

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-04:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	1	9	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**.
script screenshot	10	3	7	
script run vnc	10	2	8	
script multicommand -cl "msg"	10	2	8	
srcrip reboot	10	1	9	
TOTAL	50	9	41	

Tabla A3 - 4: Computador 04
Fuente: Elaboración Propia

Prueba 05

Computador 05

IP: 192.168.1.14

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-05:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	3	7	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**.
script screenshot	10	1	9	
script run vnc	10	2	8	
script multicommand -cl "msg"	10	3	7	
srcrip reboot	10	2	8	
TOTAL	50	11	39	

Tabla A3 - 5: Computador 05
Fuente: Elaboración Propia

Prueba 06

Computador 06

IP: 192.168.1.15

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-06:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	2	8	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**.
script screenshot	10	1	9	
script run vnc	10	3	7	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	2	8	
TOTAL	50	9	41	

Tabla A3 - 6: Computador 06
Fuente: Elaboración Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 07

Computador 07

IP: 192.168.1.16

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A2-07:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	3	7	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	1	9	
script run vnc	10	2	8	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	0	10	
TOTAL	50	7	43	

Tabla A3 - 7: Computador 07
Fuente: Elaboración Propia

Prueba 08

Computador 08

IP: 192.168.1.17

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-08:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	1	9	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	1	9	
script run vnc	10	3	7	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	3	7	
TOTAL	50	9	41	

Tabla A3 - 8: Computador 08
Fuente: Elaboración Propia

Prueba 09

Computador 09

IP: 192.168.1.18

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-09:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	1	9	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	1	9	
script run vnc	10	2	8	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	0	10	
TOTAL	50	5	45	

Tabla A3 - 9: Computador 09
Fuente: Elaboración Propia

Prueba 10

Computador 10

IP: 192.168.1.19

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-10:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	2	8	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	0	10	
script run vnc	10	1	9	
script multicommand -cl "msg"	10	3	7	
srcrip reboot	10	1	9	
TOTAL	50	7	43	

Tabla A3 - 10: Computador 10
Fuente: Elaboración Propia

Prueba 11

Computador 11

IP: 192.168.1.20

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-11:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	1	9	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	2	8	
script run vnc	10	1	9	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	0	10	
TOTAL	50	5	45	

Tabla A3 - 11: Computador 11
Fuente: Elaboración Propia

Prueba 12

Computador 12

IP: 192.168.1.21

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-12:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	2	8	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	1	9	
script run vnc	10	1	9	
script multicommand -cl "msg"	10	2	8	
srcrip reboot	10	0	10	
TOTAL	50	6	44	

Tabla A3 - 12: Computador 12
Fuente: Elaboración Propia

Prueba 13

Computador 13

IP: 192.168.1.22

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-13:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	1	9	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	2	8	
script run vnc	10	1	9	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	0	10	
TOTAL	50	5	45	

Tabla A3 - 13: Computador 13
Fuente: Elaboración Propia

Prueba 14

Computador 14

IP: 192.168.1.23

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-14:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	1	9	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	2	8	
script run vnc	10	1	9	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	1	9	
TOTAL	50	6	44	

Tabla A3 - 14: Computador 14
Fuente: Elaboración Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba 15

Computador 15

IP: 192.168.1.24

Se realizaron 50 ataques de los cuales observamos en el registro de incidencias del cual se detalla en la siguiente Tabla A3-15:

ATAQUES	VECES	INGRESO		PARCHES DE SEGURIDAD
		SI	NO	
scribt sysinfo	10	2	8	✓ Vulnerabilidad MS09-001, descargar: **KB958687**. ✓ Vulnerabilidad MS08-067, descargar: **KB958644**. ✓ Vulnerabilidad MS17-010, descargar: **KB4012598**
script screenshot	10	1	9	
script run vnc	10	3	7	
script multicommand -cl "msg"	10	1	9	
srcrip reboot	10	1	9	
TOTAL	50	8	42	

Tabla A3 - 15: Computador 15
Fuente: Elaboración Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ANEXO A4

GUIA DE CORRECCIONES DE LAS VULNERABILIDADES

Para esta guía de corrección de vulnerabilidades encontradas como se demostró en el capítulo 04, la herramienta NESSUS demostró que se encuentran 3 de las cuales se clasifican en; MS09-001 Microsoft Windows SMB Vulnerabilidad, MS09-067 Microsoft Windows Server Service Crafted RPC y MS17-010 Security Update for Microsoft Windows SMB Server. Para corregir esta vulnerabilidad de Microsoft Windows XP SP 2, se procederá a parchar las vulnerabilidades en la red de datos de la Municipalidad Distrital de Huambos, descargando de la página oficial de Microsoft. Se deben realizar los siguientes pasos:

1. MS09-001 Microsoft Windows SMB Vulnerabilidad

Propósito:

Corregir la vulnerabilidad MS09-001 correspondiente al puerto 445.

Descripción:

En la presente investigación de tesis, se demostró que mediante la herramienta NESSUS corresponde el 70% de a la Vulnerabilidad MS09-001 y permite ingresar al puerto 445 SMB, para corregir esta vulnerabilidad se tiene que instalar el parche **KB958687**. Esto se debe a que gran parte de las computadoras de la MDH corre bajo el Sistema Operativo Microsoft Windows XP SP2.

Pasos:

- ✓ Ingresar a la página web y escribir en el navegador https://www.microsoft.com/es-ES/download/details.aspx?id=963.

- ✓ Descargar el parche **KB958687**, guardar en una carpeta.
- ✓ Ejecutar el instalador WindowsServer2003-KB958687-x86-ENU.exe
- ✓ Luego de Finalizar la instalación, Reiniciar el computador.

2. MS08-067 Microsoft Windows Server Service Crafted RPC

Propósito:

Corregir la vulnerabilidad MS08-067 correspondiente al puerto 445.

Descripción:

En la presente investigación de tesis, se demostró que mediante la herramienta NESSUS corresponde el 20% de a la Vulnerabilidad MS09-067 y permite ingresar al puerto 445 SMB, para corregir esta vulnerabilidad se tiene que instalar el parche **KB958644**. Esto se debe a que gran parte de las computadoras de la MDH corre bajo el Sistema Operativo Microsoft Windows XP SP2.

Pasos:

- ✓ Ingresar a la página web y escribir en el navegador https://www.microsoft.com/es-es/download/details.aspx?id=3205
- ✓ Descargar el parche **KB958644**, guardar en una carpeta.
- ✓ Ejecutar el instalador WindowsXP-KB958644-x86-ESN.exe
- ✓ Luego de Finalizar la instalación, Reiniciar el computador.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3. MS17-010 Security Update for Microsoft Windows SMB Server

Propósito:

Corregir la vulnerabilidad MS17-010 correspondiente al puerto 445.

Descripción:

En la presente investigación de tesis, se demostró que mediante la herramienta NESSUS corresponde el 10% de a la Vulnerabilidad MS17-010 y permite ingresar al puerto 445 SMB, para corregir esta vulnerabilidad se tiene que instalar el parche **KB4012598**. Esto se debe a que gran parte de las computadoras de la MDH corre bajo el Sistema Operativo Microsoft Windows XP SP2.

Pasos:

- ✓ Ingresar a la página web y escribir en el navegador https://www.microsoft.com/es-es/download/details.aspx?id=55245
- ✓ Descargar el parche **KB4012598**, guardar en una carpeta.
- ✓ Ejecutar el instalador WindowsXP-KB4012598-x86-Custom-ESN.exe
- ✓ Luego de Finalizar la instalación, Reiniciar el computador.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe