UNIVERSIDAD AMAZÓNICA DE PANDO

DIRECCIÓN DE POSTGRADO E INVESTIGACIÓN

TESIS PARA OPTAR EL GRADO ACADEMICO DE

MAGISTER EN INGENIERÍA INFORMÁTICA

"Diseño e implementación de una Honeynet Virtual para la detección de posibles ataques informáticos en la red de datos de la Empresa Minera SOMINEX SRL."

POSTULANTE:

LIZETH PATRICIA GUTIERREZ GONZALES

TUTOR:

JUAN RAMIRO VILLA

POTOSI - BOLIVIA

2012

AGRADECIMIENTOS

A Dios por brindarme la fortaleza y sabiduría siendo mi guía en todo momento, permitiéndome culminar una nueva etapa en mi vida.

A mi familia por apoyarme en mi vida profesional y personal, haciendo de mi lo que soy, ya que todo lo que tengo y todo lo que he obtenido es gracias a su amor, esfuerzo y apoyo incondicional.

ÍNDICE GENERAL

INTRODUCCION……..……. 1

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA, OBJETIVOS Y ESTRATEGIA METODOLÓGICA…….. 5

1.1 Introducción……..……..……..……. 5

1.2 Antecedentes...……..……..……..……. 5

1.3 Planteamiento del problema……... 7

1.3.1 Problema general..…….…….. 7

1.3.2 Problemas específicos…….. 7

1.3.3 Objeto de estudio……. 8

1.3.4 Campo de acción……. 8

1.4 Objetivos…… 8

1.4.1 Objetivos general…...…….. 8

1.4.2 Objetivos específicos…….. 9

1.5 Justificación e importancia de la investigación…….. 9

1.6 Estrategia metodológica……. 11

1.6.1 Hipótesis…….. 11

1.6.2 Identificación de variables……... 11

1.6.3 Operacionalización de variables…….. 12

1.6.4 Diseño metodológico……... 13

1.6.5 Enfoque metodológico……. 14

1.6.5.1 Tipo de investigación…… 15

1.6.5.2 Diseño de la investigación…… 16

1.6.5.3 Fuentes de información……. 16

1.6.5.4 Población de estudio…… 17

1.6.5.5 Técnicas e instrumentos de recolección de datos……. 17

1.6.5.6 Diseño del instrumento de recolección de datos…….. 18

1.6.5.7 Análisis e interpretación de datos…… 18
CAPITULO II: SUSTENTO TEORICO……. 20
2.1 Introducción…… 20
2.2 Seguridad informática……... 20
2.3 ¿Por qué es tan importante la seguridad?..... 22
2.4 Amenazas.…… 22
2.5 Vulnerabilidades…….…… 25
2.6 Tipos de ataques……. 25
2.7 Tipos de intrusos…….…….……. 27
2.8 Motivación de los intrusos……..……...…… 29
2.9 Elementos a proteger…….……..…….. 31
2.10 Formas de protección……...…...……. 32
2.11 Honeypots……. 32
2.11.1 Definición…...…….…….. 32
2.11.2 Tipos de Honeypots…...……...…….. 33
2.11.2.1 Honeypot de producción……. 33
2.11.2.2 Honeypot de investigación……..…….. 34
2.11.2.3 Honeypot de baja interacción……. 35
2.11.2.4 Honeypot de alta interacción……...……...… 35
2.11.2.5 Honeypots físicos……..…….. 37
2.11.2.6 Honeypots virtuales……..…….. 37
2.12 Proyecto Honeynet……... 37
2.13 Honeynets……. 38
2.13.1 Definición…...…….…….. 38
2.13.2 Uso de las Honeynets…… 38
2.13.3 Arquitectura de las Honeynets……... 39
2.13.3.1 Control de datos…….. 40
2.13.3.2 Captura de datos……. 41

2.13.3.3 Recolección y análisis de datos……. 42
2.13.4 Tipos de Honeynets…….……. 42
2.13.4.1 Honeynets de generación I……..…… 42
2.13.4.2 Honeynets de generación II…..……..……..... 42
2.13.4.3 Honeynets de generación III.....……..……..... 48
2.13.4.4 Honeynets virtuales..……... 49
CAPITULO III: SUSTENTO EMPIRICO……...……...…..……... 53
3.1 Análisis de la situación actual...……. 53
3.1.1 Modelo actual de la red……... 53
3.1.2 Identificación de las vulnerabilidades..... 55
3.1.2.1 Identificación de vulnerabilidades basadas en la red…….…….. 56
3.1.2.2 Identificación de vulnerabilidades basadas en el host……..…….. 57
3.1.3 Determinación de problemas y necesidades…… 61
3.1.3.1 Problemas……. 61
3.1.3.2 Necesidades…….. 62
3.1.4 Estudio de factibilidad……. 64
3.1.4.1 Factibilidad técnica...……..…….. 64
3.1.4.2 Factibilidad operacional……...…… 67
3.1.4.3 Factibilidad económica…… 67
3.2 Propuesta de solución……. 69
3.2.1 Modelo de red propuesto.…… 71
3.2.2 Herramientas a ser utilizadas……..……. 75
3.2.2.1 Software para virtualización…… 75
3.2.2.2 Honeywall CD-ROM …..…… 76
3.2.2.3 Sebek……. 77
3.2.2.4 Nepenthes……. 78
3.2.3 Establecimiento de políticas de seguridad……... 78

CAPITULO IV: RESULTADOS……...……...……...…..……... 82
4.1 Configuración de la Honeynet Virtual……... 82
4.1.1 Instalación y configuración de las maquinas virtuales…….….. 82
4.1.2 Instalación y configuración del Honeywall…….… 83
4.1.3 Instalación y configuración de los Honeypots……..…….…….. 84
4.1.3.1 Configuración del Honeypot I…….. 84
4.1.3.2 Configuración del Honeypot II …… 88
4.2 Resultados obtenidos durante la configuración de la Honeynet Virtual..…….. 88
4.2.1 Procedimientos que usan los atacantes para comprometer un sistema……... 91
CONCLUSIONES Y RECOMENDACIONES...……... 97
REFERENCIAS BIBLIOGRÁFICAS…… 100
BIBLIOGRAFÍA……. 101
ANEXOS……. 104
ANEXO 1: Cuestionario aplicado a los empleados de la Empresa SOMINEX SRL……..... 104
ANEXO 2: Valoración e interpretación de los resultados obtenidos…….. 107
ANEXO 3: Instalación de la imagen Honeywall en Vmware Workstation……. 116
ANEXO 4: Configuración del Honeywall Roo V1.4 ……. 121

ÍNDICE DE FIGURAS

Figura 2.1 Clasificación de las amenazas……. 23

Figura 2.2 Arquitectura Honeynet…….…... 40

Figura 2.3 Honeynet Generación I……... 43

Figura 2.4 Honeynet Generación II…….. 46

Figura 2.5 Honeynet Virtual Autocontenida…… 50

Figura 2.6 Honeynet Virtual Híbrida……...…… 51

Figura 3.1. Modelo de red actual de la Empresa Minera SOMINEX SRL…….. 54

Figura 3.2. Directiva para contrarrestar contraseña……. 58

Figura 3.3. Directiva en el establecimiento del Umbral de Bloqueo……... 58

Figura 3.4. Directiva de Anuncio de Inicio de sesión personalizado……... 59

Figura 3.5. Directiva Auditoría y registros…….. 59

Figura 3.6. Configuración para evitar el escalamiento de Privilegios……. 60

Figura 3.7 Honeynet Virtual Autocontenida…… 71

Figura 3.8 Modelo de red propuesto para la Empresa Minera SOMINEX SRL…… 72

Figura 3.9 Honeynet Virtual Autocontenida en la red de la Empresa Minera SOMINEX SRL…… 74

Figura 4.1 Configuración de la Honeywall, en la aplicación VMware…… 83

Figura 4.2 Configuración del Honeypot I Windows XP…….. 84

Figura 4.3 Configuración de los servicios en el Honeypot I Windows XP……..... 85

Figura 4.4 Instalación de Sebek Client en el Honeypot I Windows XP……..... 86

Figura 4.5 Configuración de Sebek Client en el Honeypot I Windows XP……. 86

Figura 4.6 Configuración de magic value en el Honeypot I Windows XP…….. 87

Figura 4.7 Resumen de la configuración del Sebek Clien en el Honeypot I Windows XP. 87

Figura 4.8 Configuración de red en el Honeypot II Debian……... 88

Figura 4.9 Ping Honeypot I al Honeypot II…… 89

Figura 4.10 Ping Honeypot II al Honeypot I…… 89

Figura 4.11 Ping Honeypot I a la maquina externa…….. 90

Figura 4.12 Conexiones registradas en el Honeywall…….. 90

Figura 4.13 Procedimientos utilizados por un atacante…….. 92

Figura 5.1 Inicio de la configuración de la maquina virtual…… 116

Figura 5.2 Asignación del nombre a la maquina virtual……... 116

Figura 5.3 Asignación del memoria a la maquina virtual……. 117

Figura 5.4 Configuración de número de procesadores de la maquina virtual…….. 117

Figura 5.5 Configuración de las interfaces de red de la maquina virtual……. 118

Figura 5.6 Configuración del tipo de disco a ser utilizado en la maquina virtual…… 118

Figura 5.7 Configuración de la capacidad del disco a ser utilizado en la maquina virtual….. 119

Figura 5.8 Resumen general de la configuración a ser utilizada en la maquina virtual…….. 119

Figura 5.9 Inicio del proceso de instalación de la Honeywall en la maquina virtual…….. 120

Figura 6.1 Pantalla de advertencia para configurar el Honeywall…… 121

Figura 6.2 Inicio de la configuración del Honeywall…… 121

Figura 6.3 Inicio de la primera sección de configuración……. 121

Figura 6.4 Selección del tipo de configuración…… 122

Figura 6.5 Ingreso de la direcciones Ips de los Honeypots……... 122

Figura 6.6 Ingreso de la red utilizada para la Honeynet…… 122

Figura 6.7 Interface eth0 y eth1 encontrada…….. 122

Figura 6.8 Ingreso de las direcciones broadcast de la red LAN……... 123

Figura 6.9 Finalización de la primera sección de la configuración…….. 123

Figura 6.10 Inicio de la configuración de interface de administración…… 123

Figura 6.11 Ingreso del NIC de la interface de administración……... 123

Figura 6.12 Interface de administración activa…… 123

Figura 6.13 Ingreso de la dirección IPs de administración…….. 124

Figura 6.14 Ingreso de la máscara para la interfaz de administración……. 124

Figura 6.15 Ingreso de la default gateway para la interface de administración……... 124

Figura 6.16 Configuración de interfaz……. 124

Figura 6.17 Configuración de interfaz……. 125

Figura 6.18 Ingreso de las direcciones IPs de los servidores DNS…….. 125

Figura 6.19 Activación de la interface de administración…… 125

Figura 6.20 Iniciar la interface de administración en el siguiente boteo…….. 125

Figura 6.21 Iniciar la configuración de SSH…… 125

Figura 6.22 Permitir el loguearse remotamente por SSHD…….. 126

Figura 6.23 Cambio de la contraseña del root…….. 126

Figura 6.24 Ingreso de la nueva contraseña del root…… 126

Figura 6.25 Cambio de la contraseña exitoso…….. 126

Figura 6.26 Cambio de la contraseña del roo…….. 127

Figura 6.27 Ingreso de la nueva contraseña del roo……. 127

Figura 6.28 Cambio de la contraseña exitosa……... 127

Figura 6.29 Ingreso del puerto TCP permitido para acceder a la administración web del 127

Honeywall…….

Figura 6.30 Ingreso de la IP para acceder a la web de administración de la Honeywall……. 127

Figura 6.31 Activar la interfaz Walleye……... 128

Figura 6.32 Activa r las restricciones del firewall para prevenir troyanos y malware……. 128

Figura 6.33 Ingreso de los puertos TCP que permiten la salida……... 128

Figura 6.34 Ingreso de los puertos UDP que permitan la salida…….. 128

Figura 6.35 Finalización de la segunda sección de configuración del Honeywall…….. 129

Figura 6.36 Establecer el límite de conexiones salientes. (second, minute, hour, day)…….. 129

Figura 6.37 Establecer el límite de conexiones TCP……... 129

Figura 6.38 Establecer el límite de conexiones UDP……... 129

Figura 6.39 Establecer el límite de conexiones ICMP……...…….. 130

Figura 6.40 Establecer el límite de conexiones de los demás protocolos…… 130

Figura 6.41 Activar el snort-inline para evitar el tráfico malicioso a la red…… 130

Figura 6.42 Ingrese el nombre del archivo que contiene la lista de direcciones IPs que generan SPAM (Blacklist)…… 130

Figura 6.43 Ingrese el nombre del archivo que contiene las direcciones IPs que nunca generan SPAM (WhiteList)…….. 131

Figura 6.44 Habilitar el filtrado de la lista Blanca y Negra……. 131

Figura 6.45 No habilitar “Strict” Capture Filtering……. 131

Figura 6.46 Ingrese el nombre del archivo que contiene las direcciones IP que por medio del Fencelist el firewall bloqueará todo el tráfico hacia ellas…….. 131

Figura 6.47 No habilitar Fence List Filtering……... 132

Figura 6.48 No habilitar “Roach Motel” para así desactivar el bloqueo de todo el tráfico 132

saliente de los Honeypots…….…….

Figura 6.49 Inicio de la tercera sección de configuración del Honeywall……... 132

Figura 6.50 Configuración de los DNS para los Honeypots…… 132

Figura 6.51 Configuración de los DNS para los Honeypots…… 133

Figura 6.52 Ingresar la lista de IPs de los Honeypots……..… 133

Figura 6.53 Configuración de DNS server que serán usados para no limitar el acceso…….. 133

Figura 6.54 Inicio de la cuarta sección de configuración del Honeywall…… 133

Figura 6.55 Inicio de la configuración de alertas de mail…… 134

Figura 6.56 Ingreso del correo electrónico usado para recibir las alertas…… 134

Figura 6.57 Iniciar la configuración del mail de alertas en el boteo…… 134

Figura 6.58 Inicio de la configuración de variables del Sebek…… 134

Figura 6.59 Ingreso de la dirección IP destino de los paquetes del Sebek……..…… 135

Figura 6.60 Configuración de las variables de Sebek…….. 135

Figura 6.61 Aceptar todas las configuraciones…… 135

Figura 6.62 Finalización de configuración del Honeywall…….. 135

ÍNDICE DE TABLAS

Tabla 1.1 Definición conceptual de variables……..... 12

Tabla 1.2 Definición operacional de variables……..... 13

Tabla 2.1 Tipos de riesgos en un ambiente computacional, causas y consecuencias…..... 24

Tabla 2.2 Diferencias de los Honeypots……..……. 36

Tabla 3.1. Resultado de Escaneo de Servicios y Puertos abiertos……..... 56

Tabla 3.2 Especificación de hardware requerido para el Honeywall…….…….. 65

Tabla 3.3 Especificación de hardware requerido para los Honeypots…….…… 65

Tabla 3.4 Especificación de hardware disponible ……...…… 66

Tabla 3.5 Especificación software requerido…….…..... 66

Tabla 3.6 Especificación de software requerido……...……...… 68

Tabla 3.7 Resumen de costos en hardware y software…….…… 68

Tabla 3.8 Sistemas operativos configurados en la Honeynet Virtual Autocontenida.……. 72

Tabla 3.9 Configuración de red de la Empresa Minera SOMINEX SRL…… 74

Tabla 3.10 Componentes del CD-ROM roo V1.4…….…….. 77

RESUMEN

El presente trabajo trata de los sistemas de seguridad y las herramientas adicionales para resguardar la información, siendo la Honeynet una herramienta complementaria a las tradicionales en el mercado. La problemática del mismo surge a partir de la necesidad de profundizar sobre temas de seguridad en redes y llevarlos a la práctica mediante la implementación de esta herramienta en la Empresa Minera SOMINEX SRL., la misma que no cuenta con mecanismos de seguridad implementados, lo que representa un gran problema debido a que pone en riesgo toda la información referente a las operaciones principales de la Empresa.

El principal objetivo de este trabajo, es determinar el nivel de seguridad en la red de datos de la Empresa Minera SOMINEX SRL. e implementar una herramienta de seguridad informática, la cual permitirá analizar, controlar y monitorear la red ante posibles ataques tanto internos como externos.

Las metodologías que se llegaron a emplear para el desarrollo de esta tesis, fueron el Método Empírico y el Método Teórico, llegando a contemplar varios procedimientos, es así que con la propuesta de solución planteada se pudo realizar un mejor aseguramiento de la información y lo más importante representa una solución de bajo costo complementaria a todas las herramientas de seguridad comerciales en el mercado.

Palabras clave: Seguridad, Redes de Datos, Honeynet Virtual

INTRODUCCIÓN

Es un hecho que las intrusiones y los ataques informáticos a través de Internet se han incrementado notablemente, este incremento en el número de incidentes ha venido acompañado por una clara evolución de las herramientas y técnicas utilizadas por los atacantes. Parte de los responsables de estas acciones son usuarios avanzados que desarrollan sus propias aplicaciones y son capaces de crear y utilizar sofisticadas herramientas para introducirse en otros sistemas.

Existe una idea generalizada, que hace pensar que solo serán objeto de ataque aquellos equipos que contengan información trascendente, sin embargo, esto es un grave error. Estos ataques selectivos dirigidos por expertos suponen un porcentaje muy pequeño de los que a diario se produce a través de la red, en la práctica la totalidad de los incidentes que acontecen en Internet no van dirigidos contra equipos ni compañías específicas, sino que tienen como objeto la victima fácil. El blanco seleccionado puede ser cualquier equipo conectado a la red que posea una debilidad específica que el atacante busca y es capaz de aprovechar para conseguir el acceso a la máquina.

De alguna manera, hoy ya no se necesita poseer conocimientos desbordantes sobre el funcionamiento de un sistema para poder atacarlo. De hecho, la mayoría de los intrusos se limita a utilizar herramientas creadas por otros, herramientas que se pueden encontrar fácilmente en Internet, que son cada vez más sencillas de manejar y que no exigen que el atacante conozca su modo interno de funcionamiento.

Tradicionalmente los enfoques de seguridad como los firewalls, Sistemas de Detección de Intrusos (IDS), Redes Privadas Virtuales (VPNs), Listas de Control de Acceso (ACL), entre los más conocidos, se han basado en acciones defensivas, que consistía principalmente en defender la infraestructura de la información, detectar fallos y reaccionar a estos. Los problemas con estos mecanismos de seguridad se producen cuando no están correctamente configurados, y pueden dar una falsa sensación de seguridad. Para plantear las reglas correctas

en firewalls, IDSs y ACLs, es imprescindible que el administrador de la red tenga una visión detallada y realista de los tipos de ataques a los que su red es susceptible.

Con el cambio que está surgiendo en Internet debido al gran avance tecnológico y a la evolución de las técnicas de los atacantes, se requiere un nuevo modelo que permita ampliar el concepto de seguridad. Dentro de este nuevo modelo aparece el concepto de proactividad, en el cual no se dejan de lado herramientas antes utilizadas, sino que junto a éstas aparecen nuevas técnicas que permiten detectar e incluso prevenir nuevos ataques.

Una de estas técnicas son los Honeypots o "potes de miel", con lo cuales se crea un ambiente de red controlado, pero a la vez lo suficientemente atractivo para los atacantes, permitiendo detectar comportamientos maliciosos, para estudiarlos, entenderlos y actuar en consecuencia, de una manera proactiva, sin perjudicar el ambiente de producción de la organización. Estos ambientes pueden construirse en base a sistemas total o parcialmente compuestos por elementos virtuales denominados Honeynet Virtual. La idea de virtualización ha sido aplicada, desde hace bastante tiempo, a diferentes aspectos y ámbitos de la informática, desde sistemas computacionales completos hasta capacidades o componentes individuales.

La problemática de este trabajo nace a partir de la necesidad de profundizar temas de seguridad en redes y llevarlos a la práctica mediante la implementación de una herramienta de seguridad como es la Honeynet Virtual en la Empresa Minera SOMINEX SRL., ya que la misma no cuenta con mecanismos de seguridad implementados, situación que representa un gran problema porque pone en riesgo toda la información referente a las operaciones principales de la empresa.

El desarrollo de este trabajo se integrará con el conjunto de soluciones que la empresa tiene como por objetivo implementar para su desarrollo, siendo este en una primera instancia la determinación del nivel de seguridad, para luego proveer de una herramienta de seguridad cuya finalidad sea el de mantener la información protegida, contra los distintos tipos de ataques y vulnerabilidades constitutivas del entorno.

También es necesario indicar los objetivos específicos que constituyen una parte importante en la investigación, dentro los cuales se definen a los siguientes: Identificación y documentación de las características y requerimientos de los usuarios, de acuerdo a sus conocimientos e intereses; Investigación de las vulnerabilidades existentes y las más utilizadas por un atacante; Diseño e implementación de una arquitectura de red para la implementación de una Honeynet Virtual; Por último el establecimiento de políticas de seguridad basados en estándares internacionales.

La hipótesis de esta investigación está centrada en la implementación de la herramienta de seguridad, Honeynet Virtual la misma permitirá monitorear la red de datos de la Empresa Minera SOMINEX SRL. De la misma manera es importante indicar el alcance de la investigación la cual está enmarcada solamente en la institución que es caso de estudio, centrando la investigación en la regional correspondiente a la ciudad de Potosí.

En función al desarrollo del trabajo y por consiguiente el logro del objetivo mismo, es necesario aplicar algunos métodos de investigación, es así que las metodologías que se emplearon en el desarrollo de esta tesis fueron el Método Empírico y el Método Teórico.

A nivel empírico se emplearon los procedimientos observación, experimentación, estadístico y las técnicas encuesta y entrevista, las mismas permitieron obtener información de primera mano, contribuyendo con la determinación de la situación actual en cuanto a la seguridad en la red de datos de la institución, asimismo coadyuvaron de manera positiva con el logro de los objetivos planteados.

Dentro de los métodos teóricos se emplearon los siguientes procedimientos: histórico- lógico, análisis –síntesis, sistémico, inductivo-deductivo y el hipotético-deductivo, todos de gran utilidad al momento de realizar el estudio de las diferentes fuentes impresas de información, así como en el procesamiento de los fundamentos científicos y de las apreciaciones de varios autores que fueron consultados durante el proceso de investigación que involucro la elaboración del presente trabajo.

En tal sentido, la presente investigación conlleva una estructura de cuatro capítulos a continuación se hace una breve descripción de cada uno de ellos.

El primer capítulo describe el problema principal que originó la realización de este trabajo, de la misma manera contiene el objetivo principal, los objetivos específicos, la hipótesis y la estrategia metodológica utilizada.

El segundo capítulo contiene el marco teórico de la investigación, describe el problema sobre los diferentes tipos de ataques a los que están expuestas las redes de datos, así como definiciones, tipos y usos de los Honeypots, centrándose posteriormente en las Honeynets y Honeynets Virtuales, tomando en cuenta su arquitectura y las diferentes generaciones, conceptos que permitieron asumir una o varias posiciones teóricas encaminadas a la solución del problema.

En el tercer capítulo se detallan la selección de las arquitecturas a implementar llevando a cabo un análisis de las mismas. Además se realizo un diagnóstico de la vulnerabilidades a los cuales está expuesta la red de datos de la organización, en este capítulo también se detalla el diseño general de la arquitectura escogida para la red de datos de la Empresa Minera SOMINEX SRL., realizando una descripción detallada de los pasos seguidos para la implementación de la Honeynet Virtual, con lo que se dio respuesta al problema planteado.

Finalmente, en el capitulo cuatro se describen los resultados obtenidos tras la propuesta de solución planteada, así como las imágenes de la implementación y configuración de la herramienta de seguridad Honeynet Virtual, con los cuales se llegara a determinar las conclusiones de este trabajo y recomendaciones para futuros trabajos de investigación.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA, OBJETIVOS Y ESTRATEGIA METODOLÓGICA

1.1. Introducción

Los entornos informáticos y la información procesada por los mismos suman valor a las entidades y organizaciones, de esta manera, se considera que el principal activo de una empresa es la información que esta posee. Debido a la sistematización del mundo, la información es cada vez más pretendida, y más propensa a sufrir ataques causados por ajenos, que aprovechan las vulnerabilidades que poseen las redes informáticas, con la finalidad de apoderarse de la información. Por tanto, la seguridad de la información puede expresarse como la suma de todas las medidas y mecanismos de seguridad a tomar, para prevenir pérdidas de cualquier clase.

Este capítulo presenta en su contenido información sobre el principal problema al que se enfrenta la red de datos de la Empresa Minera SOMINEX SRL., para luego conocer el objeto de estudio y el campo de acción definidos, en torno a los cuales se llevará a cabo la investigación, posteriormente se conocerá el objetivo general y los objetivos específicos planteados, que deberán cumplirse una vez que la investigación culmine. Finalmente se presenta la estrategia metodológica, que se empleo, en la cual se contempla la formulación de la hipótesis, la operacionalización de variables y el diseño metodológico utilizado.

1.2. Antecedentes

La frecuencia de aparición de ataques indiscriminados se ha disparado en los últimos años, y este hecho, unido al creciente número de vulnerabilidades descubiertas en todo tipo de sistemas operativos y aplicaciones, así como la inexistencia de una legislación penal adecuada en Bolivia, convierte a cualquier sistema conectado a Internet en una víctima potencial. Este panorama plantea la necesidad de disponer de instrumentos que permitan

descubrir y analizar tanto agujeros de seguridad que pueda presentar un sistema como las técnicas y herramientas utilizadas por la comunidad de atacantes que habita la red.

La Sociedad Minera de Exportaciones SRL., con sus siglas SOMINEX SRL. es una empresa privada que cuenta con instalaciones en la ciudad de Potosí y La Paz, esta empresa está dedicada a la comercialización de concentrados de mineral, ofreciendo servicios de calidad con seguridad industrial y responsabilidad ambiental, dentro de los principales mercados con los cuales trabaja se puede mencionar a los países Suiza, China y Perú. El prestigio de la organización y su antigüedad en el ramo, ha brindado como resultado, el poder trabajar con varios proveedores y clientes de esta ciudad así como de otras del país además de empresas, multinacionales y extranjeras, lo cual genera un importante rendimiento económico en sus dos regionales: Potosí y La Paz.

La expansión de la organización y la dinámica del negocio, dio lugar a la implementación de servicios informáticos. Por esta razón, casi todo el personal posee equipos computacionales para desarrollar su trabajo diario, además estos equipos están interconectados mediante una red. El personal cuenta con los servicios de Internet, correo electrónico corporativo, sistema interno transaccional, directorio y archivos compartidos.

El servicio de Internet, permite acceder a páginas web y servicios de mensajería instantánea a todos los empleados; el correo electrónico corporativo, permite enviar y recibir mensajes de manera eficiente; los documentos son compartidos mediante directorios y toda la información de la organización, es registrada en un sistema informático transaccional. Como se había mencionado toda la información referente a compras y ventas de concentrado de mineral, así como la información sobre los proveedores y clientes con los que se trabaja, está contenida en una base de datos, la cual proporciona datos necesarios para el sistema interno, siendo esta información un activo de gran valor para la organización.

El hecho de que la organización haya recurrido al uso de tecnologías de información mediante la implementación de una red así como el uso de sistemas de información transaccional donde almacenan información critica para la empresa, y principalmente el hecho de estar conectada

a los servicios de Internet, de alguna manera la vuelve vulnerable a recibir cualquier tipo de ataque. En entrevistas que fueron llevadas a cabo con el personal de la empresa se pudo constatar que el grado de seguridad que tiene esta infraestructura de red es mínimo, es decir no cuenta con mecanismos de seguridad implementados, por lo que representa un gran problema ya que pone en riesgo toda la información referente a las operaciones principales de la empresa. Por lo expuesto anteriormente, es imprescindible implementar un mecanismo de seguridad que permita mejorar considerablemente el nivel de seguridad con el que cuenta la empresa.

1.3. Planteamiento del problema

1.3.1. Problema general

La problemática de este trabajo nace a partir de la necesidad de profundizar temas de seguridad en redes y llevarlos a la práctica mediante la implementación de una herramienta de seguridad como es la Honeynet Virtual en la Empresa Minera SOMINEX SRL., la misma no cuenta con mecanismos de seguridad implementados, situación que representa un gran problema debido a la existencia de personas, grupos de personas, organizaciones tanto internas como externas a la institución, que trabajan diariamente en búsqueda de vulnerabilidades en sistemas operativos, aplicaciones informáticas, servidores, redes de computadores, lo que deriva en que la información referente a las operaciones principales de la empresa este en constante peligro, ya que puede ser objeto de sufrir algún tipo de ataque.

Por todo lo expuesto, se formula el siguiente problema de investigación:

¿Cuál es el nivel de seguridad implementado en la red de datos de la Empresa Minera SOMINEX SRL. y qué medidas o políticas de seguridad se deberían implementar para mejorar la seguridad?

1.3.2. Problemas específicos

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de

seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo. Por lo tanto se define a continuación los siguientes problemas específicos:

- No se tiene identificado ni documentado los requerimientos de los usuarios, en términos de conocimientos e intereses respecto al tema de seguridad.
- Falta de conocimiento por parte del personal de la empresa, respecto a la existencia de vulnerabilidades así como las técnicas de ataque más utilizadas por un intruso.
- Falta de sistemas o herramientas de seguridad que formen en conjunto un eficiente sistema de seguridad.
- Falta de protección a los recursos y la información con que se cuenta en la red, a través de herramientas y de procedimientos basados en una política de seguridad que permitan un control adecuado de los mismos.

1.3.3. Objeto de estudio

La protección de la información, constituye un pilar fundamental en las organizaciones, debido a la gran importancia y valor que representa la información privada y confidencial, por lo que se define como objeto de estudio a la Seguridad en las Redes de Datos.

1.3.4. Campo de acción

El campo de acción definido es la herramienta de seguridad conocida como Honeynet Virtual, cuyo objetivo es reunir información sobre la actividad del intruso, logrando así detectar las vulnerabilidades que posee nuestra red antes de que estas sean explotadas, además de conocer los riesgos a los cuales nuestros sistemas de información están expuestos.

1.4. Objetivos

1.4.1. Objetivo General

Una vez delimitadas las áreas en las que se desarrolla el presente trabajo el objetivo general es: Determinar el nivel de seguridad en la red de datos de la Empresa Minera SOMINEX SRL. e implementar una herramienta de seguridad informática, la cual permitirá monitorear la red ante posibles ataques tanto internos como externos.

1.4.2. Objetivos Específicos

Para llegar al objetivo general se definieron los objetivos específicos que constituyen una parte importante en la investigación, los mismos se detallan a continuación:

- Identificar y documentar las características y requerimientos de los usuarios, en términos de conocimientos e intereses.
- Investigar las vulnerabilidades existentes y las más utilizadas por un atacante.
- Implementar un prototipo funcional de Honeynet Virtual que analice el comportamiento de los intrusos, sus motivos y las herramientas que utilizan.
- Determinar y/o establecer políticas de seguridad para las vulnerabilidades y ataques que se presenten en la red.

1.5. Justificación e importancia de la investigación

La justificación e importancia de la investigación permite determinar la significación y el gran aporte que tiene este trabajo para la institución, la misma se ve reflejada tomando en cuenta los siguientes criterios:

Conveniencia: La necesidad de controlar el enorme flujo de datos e información que circulan en nuestros días por las grandes redes de comunicación, justifica la conveniencia a la hora de la aplicación de esta herramienta de seguridad sobre los datos, ya que la protección de la información, constituye un pilar fundamental en las organizaciones, debido a la gran importancia y valor que representa la información privada y confidencial antes de que éstos sean modificados, publicados o difundidos. De esta forma se pretende evitar que el uso inadecuado de toda esta información, revierta en un daño o perjuicio sobre individuos o entidades, de los cuáles se tienen datos que son accesibles por cualquier usuario desde cualquier parte del mundo. El presente trabajo, proporciona soluciones para proteger la información, entre ellas la creación y/o mejoramiento de políticas de seguridad, así como la implementación de

herramientas de seguridad como medidas preventivas y correctivas de manera que se permita gestionar una red de datos más segura.

Aporte social: No se pretende, en ningún caso, vetar el derecho a la información que todos tenemos y que está fuera de toda duda, sino equilibrar éste con otro derecho básico que contempla la preservación de la intimidad del individuo. El aporte social a la hora de implementar la herramienta de seguridad Honeynet Virtual, consistirá en aportar una máxima calidad de información de la forma más segura a todas las personas que formen parte activa de la Empresa Minera SOMINEX SRL.

Significación práctica: Mediante el desarrollo de este trabajo, se pretende proveer a la empresa de una herramienta de seguridad que permita contrarrestar los problemas de seguridad informática debido a las vulnerabilidades y brechas de seguridad existentes. Por ello, para la prevención o mitigación de cualquier tipo de amenaza es necesario conocer y comprender las vulnerabilidades constitutivas del entorno. Una de las metodologías para esto es crear un ambiente de red controlado pero a la vez lo suficientemente atractivo para los atacantes, que permita detectar comportamientos maliciosos, para estudiarlos, entenderlos y actuar en consecuencia, ya sea de una manera proactiva o reactiva, sin perjudicar el ambiente de producción de la organización, siendo este el principio fundamental de una Honeynet.

Aporte teórico: La implementación de una Honeynet Virtual, ayudará a revisar, desarrollar y apoyar las distintas metodologías de seguridad informática existentes, planteando y sugiriendo ideas, así como recomendaciones para futuros estudios, por ello se entiende el valor que tiene la contribución de este tipo de arquitectura cuyo propósito es crear una red altamente controlada, donde sea posible capturar toda la actividad que en ella existe, permitiendo detectar en tiempo real actividades que puedan resultar dañinas, así como el conocimiento sobre el comportamiento y técnicas reales utilizadas por los atacantes en un entorno “real”.

Utilidad Metodológica: La presente investigación servirá de aporte para el estudio de problemas similares al identificado, el diseño e implementación de esta red nos permitirá identificar las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de la red de la Empresa Minera SOMINEX SRL., de esa manera se entenderá la importancia de definir políticas, procedimientos y estándares, de acuerdo a los requerimientos de la institución.

1.6. Estrategia metodológica

1.6.1. Hipótesis

Es de conocimiento que la hipótesis se refiere a la suposición de un aspecto para obtener una consecuencia, explorando datos vagos, inadecuados e indemostrables en forma objetiva, en este sentido la formulación de la hipótesis se detalla de la siguiente manera:

La implementación de la herramienta de seguridad informática Honeynet Virtual permitirá proteger y monitorear la red de datos de la Empresa Minera SOMINEX SRL.

1.6.2. Identificación de variables

Las variables constituyen una parte importante dentro de la investigación, cuya propiedad principal consiste en ser capaz de asumir diferentes valores, características, fenómeno, o situación susceptible de ser objeto de estudio, se definen las siguientes variables:

Variable Independiente: La implementación de la herramienta de seguridad informática Honeynet Virtual.
Variable Dependiente 1: Proteger la red de datos.
Variable Dependiente 2: Monitorear la red de datos.
Unidad de Observación: Red de datos de la Empresa Minera SOMINEX SRL.
Enlace lógico: Permitirá.

1.6.3. Operacionalización de variables

Una vez que las variables han sido identificadas, las variables citadas son las consideradas para llevar a cabo la operacionalización, las variables dependientes: *Proteger y monitorear la red de datos* no son consideradas dentro de la definición operacional debido a que es el resultado que se espera de aplicar la herramienta de seguridad Honeynet Virtual.

A continuación se presentan los cuadros de las variables que serán consideradas:

a) Definición Conceptual

Hipótesis	Variables	Definición conceptual
La implementación de la herramienta de seguridad informática Honeynet Virtual permitirá proteger y monitorear la red de datos de la Empresa Minera SOMINEX SRL.	Implementación de la herramienta de seguridad informática Honeynet Virtual	Red de señuelos contenida completamente en un único computador mediante la utilización de software de virtualización.
	Proteger la red de datos	Medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
	Monitorear la red de datos	Define un proceso continuo de recolección y análisis de datos con el fin de anticipar problemas en la red.

Tabla 1.1 Definición Conceptual de Variables
Fuente: Elaboración propia

b) Definición Operacional

VARIABLE	DEFINICION CONCEPTUAL	DIMENSIONES	INDICADORES	ITEMS	APLICADO
Herramienta de seguridad informática Honeynet Virtual	Red de señuelos contenida completamente en un único computador mediante la utilización de software de virtualización	Red	-Políticas -Estrategias -Controles	1,2 3,4 5	Usuarios
		Computador	-Costos - Infraestructura	6 7	
		Software	-Arquitectura -Seguridad	8 9	

Tabla 1.2 Definición Operacional de Variables.
Fuente: Elaboración propia

1.6.4. Diseño metodológico

En esta sección se presenta el diseño metodológico que es necesario para el desarrollo de la investigación, el cual está compuesto por los métodos, procedimientos, técnicas e instrumentos que fueron usados en el desarrollo del estudio con la finalidad de dar respuesta a la problemática planteada.

Cualquier proceso de investigación puede valerse de diversas técnicas y métodos según los requerimientos de la misma. Haciendo un paréntesis es necesario aclarar que las técnicas complementan a los métodos tanto teóricos como empíricos para el desarrollo de la investigación.

A pesar de las diferencias existentes, en muchas ocasiones, el proceso de investigación puede valerse de una combinación de técnicas, es decir se puede utilizar la entrevista y la encuesta, o simplemente la utilización de un solo tipo de técnica, de acuerdo a los objetivos que se pretenden alcanzar con la investigación es que se define una combinación de ambos métodos es decir teóricos y empíricos.

1.6.5. Enfoque metodológico

En función al desarrollo del trabajo y por consiguiente el logro del objetivo mismo, fue necesario aplicar algunos métodos de investigación, es así que las metodologías que se emplearon en el desarrollo de esta tesis fueron el Método Empírico que permitió efectuar el análisis preliminar de la información y el Método Teórico que permitió revelar las relaciones esenciales del objeto de investigación.

Dentro del método empírico, se utilizaron los siguientes procedimientos:

- Observación, para realizar el estudio y análisis del objeto de estudio, con la finalidad de conocer de manera progresiva el problema identificado, y a la vez obtener el conocimiento acerca del tema de seguridad en redes en la actualidad.
- Experimentación, para recoger información sobre los ataques y vulnerabilidades que afectan la red de datos de la Empresa Minera SOMINEX SRL.
- Encuesta a través de cuestionarios que fueron aplicados al personal de la Empresa Minera SOMINEX SRL., instrumento que permitió obtener información de primera mano sobre las necesidades y requerimientos que presenta la misma.
- Entrevista, con el objetivo de recoger información puntual y relevante fundamentada esencialmente en cuestionarios.
- Estadístico, cuya finalidad constituye la interpretación de los resultados a través de cuadros estadísticos.

Por otra parte dentro del método teórico, se contemplo los siguientes procedimientos:

- Histórico – Lógico, que permitió comprender el objeto de la investigación, sus antecedentes y desarrollo, como también permitió realizar una valoración crítica de la situación actual de la Empresa Minera SOMINEX SRL.

- Análisis-Síntesis, para valorar las diferentes fuentes de información primarias y secundarias a lo largo del presente trabajo.
- Sistémico, que proporcionará la orientación general para el estudio y solución integral del problema.
- Inductivo-Deductivo, plasmado en la generalización y particularización, de los eventos que se originan en base a la observación del objeto de estudio, gracias a este procedimiento se pudo determinar la elección del tema de investigación, la definición del objetivo general y específicos, también permitió desarrollar el marco teórico y proponer una solución a la problemática planteada.
- Hipotético-Deductivo, basada en la proposición de una hipótesis como consecuencia de la observación al objeto de estudio y la deducción de proposiciones más elementales así como la verificación de la hipótesis planteada.

1.6.5.1. Tipo de investigación

Para poder emplear los métodos, procedimientos y técnicas adecuadas para el desarrollo de la investigación es necesario, definir el tipo de investigación. En general se distinguen tres tipos: exploratoria, descriptiva y correlacional.

De manera general, la investigación o los estudios exploratorios tienen como propósito explorar algún problema de investigación que ha sido poco estudiado. En cuanto a los estudios descriptivos, estos exponen las características de los fenómenos a estudiar, tales características pueden ser medidas para finalmente poder describirlas. Finalmente se encuentra la investigación o estudios correlacionales los cuales miden dos o más variables para ver si pueden ser o no relacionadas.

Es así que el tipo de estudio definido para la investigación en una primera instancia se inicio como exploratoria después se pasó a un tipo de investigación descriptiva. A partir de la selección del tipo de investigación a realizarse se determina el diseño de investigación.

1.6.5.2. Diseño de la investigación

La elección del diseño de investigación radica fundamentalmente en la elección de dos tipos de diseños, el experimental y no experimental. Para propósitos de esta investigación se eligió el primero, es decir el diseño experimental, ya que este tipo de investigación integra un conjunto de actividades metódicas y técnicas que se realizan para recabar la información sobre el tema a investigar y el problema a resolver.

Decidido el tipo y diseño de investigación a realizarse, se eligen las herramientas necesarias para llevar a cabo la investigación.

1.6.5.3. Fuentes de información

Las fuentes de información son todas aquellas personas, empresas, instituciones, documentación, libros, revistas y todo aquello que pueda brindar información relacionada con la investigación. Con el objetivo de obtener información para esta investigación, fue necesario obtener todos los datos por medio de las siguientes fuentes.

- Fuentes primarias: Para esta investigación la información se obtuvo a través de un cuestionario dirigido al personal de la Empresa Minera SOMINEX SRL., y entrevistas a usuarios selectos que velan por la seguridad de la información de la institución.

- Fuentes secundarias: Fue necesario recopilar información de carácter bibliográfico tales como: libros, informes de seguridad, y de toda aquella información escrita relacionada directamente con la manera de cómo realizan el monitoreo de incidentes o ataques informáticos, como de proyectos que están actualmente vigentes y que han servido de ejemplo para guiar la implementación de la herramienta de seguridad, e Internet.

1.6.5.4. Población de estudio

Se puede decir que la población es el conjunto de todas las unidades, personas o cosas que concuerden con una serie de descripciones. La población compone el objetivo de la investigación, ya que es el centro de la misma y de ella se extraerá la información requerida para el estudio en cuestión, la población puede estar conformada por un conjunto infinito o finito de individuos u objetos.

El tipo de universo que se determino es de carácter finito, ya que se conoce la cantidad de personal que trabaja en la Empresa Minera SOMINEX SRL. El Universo de la investigación estuvo constituido por 10 personas que conforman la parte administrativa y técnica de la institución, por tal razón no se requirió determinar la muestra, sino que se opto por realizar un registro y fue factible estudiar la opinión de todos.

1.6.5.5. Técnicas e instrumentos de recolección de datos

La técnica que se utilizo para recolectar la información fue la entrevista, la cual es una técnica de fuente primaria, que ha sido y sigue siendo un recurso altamente utilizado. Las entrevistas, permiten aproximarse a, el o los hechos que van a ser estudiados, esta aproximación depende del propósito que se persiga. Para el desarrollo de esta tesis fueron realizadas las entrevistas a los diez trabajadores que componen la parte administrativa y técnica de la institución.

Como instrumento se utilizó un cuestionario de preguntas múltiples, es importante considerar que el cuestionario es la fuente de información primaria y por lo tanto su aplicación está enmarcada en la permanente actualización bibliográfica, además recalcar que se realizo tomando en cuenta los indicadores determinados en la operacionalización de variables.

También se realizó la observación directa aplicada a la población sirviendo la información recolectada como base para conocer la situación al momento de iniciar el estudio en la institución.

1.6.5.6. Diseño del instrumento de recolección de datos.

La herramienta que se utilizo para la recopilación de información fue el cuestionario que se paso al personal de la Empresa Minera SOMINEX SRL., con el fin de obtener información de primera mano, que permita la consecución de los objetivos propuestos.

El cuestionario fue organizado de acuerdo a la siguiente estructura: la primera parte contiene el nombre del proyecto, la segunda el objetivo de la investigación, la tercera las indicaciones y la cuarta contiene el cuerpo del cuestionario que contiene seis preguntas de esta forma se recopilo la información primaria (ver anexo 1).

Luego de concluida la investigación, se procedió a la valoración de los resultados obtenidos lo que permitió tener un panorama de todas las interrogantes y sus respectivos porcentajes, para luego proporcionar una interpretación de cada una de las preguntas que aparecen en el cuestionario (ver anexo 2).

1.6.5.7. Análisis e interpretación de datos

La investigación realizada por medio de la elaboración de estos cuestionarios es de mucha importancia ya que permitió obtener información de primera mano, las necesidades que la Empresa Minera SOMINEX SRL., tiene acerca de la seguridad informática, siendo necesario el diseño de una herramienta de seguridad de apoyo, y permitiendo dar posibles soluciones a los problemas.

La seguridad informática es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de herramientas y de procedimientos basados en políticas de seguridad tales que permitan el control adecuado de toda esta información. Como conclusiones a la elaboración de este cuestionario se pudo llegar a lo siguiente:

- El 90 % de los empleados encuestados, aseguran no conocer sobre los mecanismos apropiados que permitan gestionar la información de manera adecuada.

- Se determinó que el 70 % de los encuestados no tienen conocimiento sobre los riesgos a los que están expuestos los sistemas informáticos de la Empresa Minera SOMINEX SRL, cuando se conectan a los servicios de Internet.

- De acuerdo a los resultados obtenidos se pudo evidenciar que la mayoría de las personas encuestadas específicamente un 90%, no utiliza alguna estrategia o medida para la detección de intrusos.
- La mayoría de las personas encuestadas no utiliza alguna estrategia para la prevención de ataques a su información, por otra parte un 20% del personal encuestado no tiene conocimiento respecto a estrategias utilizadas en la prevención de ataques.

- El 80 % de los empleados encuestados de la Empresa Minera SOMINEX SRL., aseguran no tener conocimiento sobre la realización de controles y/o monitoreos a la red de datos para prevenir los ataques informáticos.

- El 100 % de los empleados de la Empresa Minera SOMINEX SRL., afirman que están interesadas en informarse acerca de los mecanismos de seguridad adecuados, y en la implementación de un sistema de seguridad con herramientas gratuitas.

- Se determinó que el 100% de los encuestados afirmó desconocer el sistema Honeynet Virtual como herramienta de seguridad.

- Se determinó que el 100 % de los encuestados están dispuestos en conocer e implementar un sistema de seguridad con herramientas gratuitas como lo es la Honeynet Virtual.

- Se concluyó que la institución, está 100 % interesada en una propuesta de solución utilizando la herramienta de seguridad Honeynet Virtual.

CAPITULO II

SUSTENTO TEORICO

2.1. Introducción

Este capítulo introduce y extiende la comprensión de la seguridad informática, análisis de amenazas y riesgos, para luego conocer los tipos de ataques y enemigos cibernéticos y lo que los motiva a realizar actividades de intrusión que afectan la información que circula por una red de datos. También se presento conceptos sobre la herramienta de seguridad diseñada para ser atacada y comprometida por un intruso e introduce como primer paso la definición de los Honeypots, tipos de Honeypots, así como la definición de Honeynets y el uso que se les da a este tipo de herramientas, para luego definir a las Honeynets virtuales con lo cual se analizo las ventajas y desventajas acerca de esta herramienta.

2.2. Seguridad informática

La seguridad informática, consiste en asegurar que los recursos del sistema de información[1] de una organización sean utilizados de la manera en que se decidió. Así entonces la seguridad es una característica de cualquier sistema ya sea informático o no, que nos indica que ese sistema está libre de peligro, daño o riesgo.

Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100 por ciento seguro. Para que un sistema se pueda definir como seguro debemos de dotar de tres características que se plasman a continuación:

[1] Sistema de Información: Es un conjunto de elementos interrelacionados que recoge datos, los procesa y convierte en información, que almacena y posteriormente distribuye a sus usuarios, con el fin de apoyar a las actividades de una empresa o negocio.

a. Integridad

La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada y copiada, durante el proceso de transmisión o en su propio equipo de origen [1], a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

b. Confidencialidad

La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos, ya que la transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada [1]. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo: conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se filtran a una empresa competidora, facilitarían a esta ultima desarrollar un producto de características semejantes).

c. Disponibilidad

La disponibilidad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas [2]. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

2.3. ¿Por qué es tan importante la seguridad?

Por la existencia de personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas. El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

2.4. Amenazas

Es necesario definir amenaza, en el entorno informático, como cualquier tipo de evento o acción que pueda producir un daño material o inmaterial sobre los elementos de un sistema. Al igual que sucede con cualquier otra forma de procesamiento de datos, las redes de datos también se ven expuestos a amenazas. Existen diferentes clasificaciones de ellas, las cuales dependen del punto desde donde se las observe, sean estas internas o externas, intencionales o accidentales, provocadas por el hombre o por la naturaleza.



Figura 2.1 Clasificación de las amenazas
Fuente: Tesis Licenciatura en Sistemas, Titulo "Seguridad Informática sus implicancias en implementación", Autor Borghello Cristian

Una amenaza es externa cuando el factor que la provoca es ajeno a la empresa que sufre las consecuencias de su materialización. Por otra parte, una amenaza es interna cuando el elemento que la provoca yace dentro de la misma empresa.

Una amenaza es intencional cuando existe premeditación por parte de la persona o agente que provoca la materialización de la amenaza; por otra parte una amenaza es no intencional cuando la ocurrencia del evento se debe a una casualidad o un hecho fortuito. Dentro de las amenazas provocadas por la naturaleza se incluyen los terremotos, inundaciones, tormentas eléctricas, entre otras. Por otra parte dentro de las amenazas provocadas por el hombre se tienen sabotaje, robo, secuestro, suplantación, entre otras.

A continuación se presentan una tabla, que refleja las posibles consecuencias que se pueden tener en un ambiente computacional según sea la intencionalidad de la amenaza, pudiendo ser estas intencionales o no intencionales, y de acuerdo con las consecuencias típicas de una materialización daño, alteración y revelación.

	CONSECUENCIAS		
	DAÑO	**ALTERACION**	**REVELACIÓN**
ACCIONES INTENCIONALES	Fuego, robo de equipos, discos y disquetes; destrucción física de los datos y programas almacenados en discos y dispositivos de almacenamiento; interrupción en la prestación de las facilidades que provee la computadora; motín, sabotaje, entre otras.	Agregado, cambio o borrado de alguna porción de los archivos que contienen los datos o programas con propósitos personales, por diversión o por venganza.	Venta de información con propósitos personales, por diversión o por venganza.
ACCIONES NO INTENCIONALES	Catástrofes naturales: tales como incendio, inundación, terremoto; daño accidental de discos, disquetes y otro dispositivo de almacenamiento, pérdida de las facilidades provistas por la computadora.	Agregado, cambio o borrado accidental de alguna porción de los archivos que contienen los datos o programas; alteración de los datos ocasionada por el mal funcionamiento de algún componente de hardware o software	Mostrar alguna información a colegas; despliegue accidental de contraseñas o salidas que producen los sistemas de información.

Tabla 2.1 Tipos de riesgos en un ambiente computacional, causas y consecuencias.
Fuente: Tesis Licenciatura en Sistemas, Titulo "Seguridad Informática sus implicancias en implementación", Autor Borghello Cristian

2.5. Vulnerabilidades

Por vulnerabilidad se entiende a la exposición latente a un riesgo o amenaza. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; peor aún, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Específicamente, en los ataques de negación de servicio, el equipo de cómputo ya no es un blanco, es el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el sitio web de la compañía. Con ello, es evidente que los riesgos están en la red, no en la PC.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

2.6. Tipos de ataques

Los ataques se presentan en todas las formas, tamaños y en diferentes métodos, algunos son más complejos y otros más básicos, se pueden clasificar de la siguiente manera:

Ataques de intromisión: Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en una computadora hasta encontrar algo que sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los

ataques registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

Ataque de espionaje en líneas: Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien espíe el flujo de información.

Ataque de intercepción: Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en una red.

Ataque de modificación: Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos, utilizando la vulnerabilidad de los sistemas operativos y sistemas de seguridad es decir atributos, claves de accesos, etc.

Ataque de denegación de servicio: Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos anteriormente son inutilizados. Si se habla de comunicaciones, se puede inutilizar dispositivos de comunicación puede ser tan sencillo como cortar un simple cable, saturar e inundar con tráfico excesivo las redes para que estas colisionen.

Ataque de suplantación: Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha puesto de moda este tipo de ataques; los "nuevos ladrones" han hecho portales similares a los bancarios, donde las

personas han descargado sus datos de tarjetas de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son vaciadas.

Es importante mencionar, que así como se llevan estos tipos de ataques en medios electrónicos, muchas veces se llevan a cabo en archivos físicos como expedientes, archiveros con información en papel, y en otro tipo de medios con los que las personas están familiarizadas a trabajar todos los días como los teléfonos convencionales, celulares, cajeros automáticos, etc.; inclusive los ataques a computadoras, muchas veces, comienzan precisamente con información obtenida de una fuente física papeles, basura, intervención de correo, cartas, estados de cuenta que llegan a los domicilios; o simplemente de alguien que vigila lo que hacemos.

Se realiza una mención de estos últimos puntos, porque muchas veces se piensa que la intrusión, pérdida, alteración, inserción, bloqueo de información en sistemas, bloqueo de sistemas operativos y de dispositivos, suceden por casualidad o simplemente porque existen los Hackers.

2.7. Tipos de intrusos

Dependiendo de su forma de actuar, su nivel de conocimiento y los objetivos que persigue un intruso se puede clasificar en alguno de los tipos que se muestran a continuación.

Hackers: Los Hackers, provienen de los tiempos de los técnicos de telefonía que arreglaban máquinas con un golpe, a estos técnicos se les llamaba hackers ya que la palabra hack significa golpear en ingles. A su vez, los hackers difieren mucho del estereotipo de joven ojeroso con lentes gruesos, ya que la mayoría son personas comunes y corrientes con cierto grado de curiosidad por la tecnología. Un hacker, no es hacker hasta que es reconocido por sus pares. Para obtener este reconocimiento y respeto de parte de sus pares un hacker debe realizar 5 acciones:

- Escribir programas útiles y donar los códigos fuentes a la comunidad.
- Ayudar, probar y depurar herramientas de software libre.

- Filtrar y recoger información útil y ponerlos a disposición de la comunidad.
- Mantener el funcionamiento de la infraestructura de la comunidad, tales como foros de discusión, listas de correo, etc.
- Hacer algo por la cultura hacker, donde siempre se recomienda la modestia.

Un hacker es una persona que vive para aprender, que le encantan los retos y lucha por la libre difusión de la información y la globalización de las comunicaciones. Un hacker no es un pirata informático ya que los piratas informáticos comercian la información que obtienen, mientras que los hackers obtienen la información sólo para uso personal.

Crackers: Los Crackers, son personas cuyo objetivo va más allá de la simple investigación. Es una persona con fines malignos, haciendo daño solo por diversión o para demostrar sus habilidades.

Phreakers: Phreakers viene de la fusión de palabras freak, phone y free. Es la actividad en la que estos individuos engañan a las compañías telefónicas para realizar llamadas gratis. Los Phreakers son crackers pero de las redes de comunicación, con amplios conocimientos en telefonía.

Carding: El carding consiste en el uso ilegitimo de las tarjetas de crédito de otras personas para realizar fraudes. En un principio, los números y claves de tarjetas de crédito se podían obtener mediante un analizador de las señales electromagnéticas producida por los cajeros automáticos, con lo cual aumentó este tipo de personas.

Gurús: Los maestros y encargados de adiestrar a los futuros hackers, se encargan de enseñar las técnicas básicas, aunque no están activos son reconocidos por la importancia de sus actos en el pasado.

Lamers o Script Kiddies: Son los aficionados, que prueban todos los programas que llegan a sus manos, se aprovechan de los conocimientos de otros para presumir. La mayoría de las veces son los responsables de lanzar virus o bombas lógicas por las redes.

Wannaber: Son aquellas personas que desean ser hackers pero la comunidad considera que su coeficiente no está a la altura, pese a su actitud positiva es muy difícil que logre avanzar en sus planes.

Piratas Informáticos: Son aquellas personas que realizan copias ilegales de dispositivos audiovisuales o software tales como dvd, cd, etc. para venderlos ilegalmente.

Samurai: Son la amenaza pura, saben lo que buscan, dónde y cómo encontrarlo, trabajan a encargo y por dinero, no pertenecen a la comunidad y se basan en que cualquiera puede ser atacado o saboteado.

Insiders: Individuos pertenecientes al personal de una organización que realizan ataques a los sistemas. Esto es muy alarmante ya que estas personas pueden conocer perfectamente los sistemas incluyendo los puntos débiles de este, pudiendo vulnerarlos más efectivamente que un atacante externo. Los tipos de insiders pueden definirse de acuerdo a la intención que puedan tener, algunos pueden ser:

• Ex-Empleado: Las personas pertenecientes a este grupo suelen estar interesados en violar la seguridad de la empresa, ya sea por haber sido despedidos o para sacar información para la competencia.

• Curiosos: Son los atacantes más habituales del sistema. En la mayoría de los casos son estudiantes con la intención de ingresar a los servidores o empleados que tratan de conseguir información prohibida para ellos.

• Intrusos Remunerados: Son los atacantes más peligrosos, ya que cuentan grandes conocimientos y experiencia, pero no son muy habituales. Generalmente son contratados por la competencia para robar información privilegiada, o simplemente arruinar la imagen de la empresa.

2.8. Motivación de los intrusos

La motivación es uno de los elementos principales para comprender que es lo que mueve a estos individuos a realizar sus actos. De acuerdo a la organización federal de investigación de los Estados Unidos la cual encaja cuatro elementos importantes mediante las siglas en inglés MICE que viene de los acrónimos, dinero (Money), ideología (Ideology), compromiso (Compromise) y ego (Ego). Sin embargo esta definición de motivaciones se extiende a las siguientes seis:

a. Dinero.

El dinero es uno de los aspectos que los atacantes toman como una principal motivación partiendo del punto de vista que deben de explotar sus conocimientos para beneficio propio. Un ejemplo de lo mencionado es cuando se aprovechan de los recursos de llamadas internacionales telefónicas a través de Internet, aquellos que ofrecen servicios de robo de archivos o números de tarjetas de crédito beneficiándose por una suma de dinero, son lo que considera como un atacante.

b. Entretenimiento

El entretenimiento es probablemente una de las motivaciones que tiene menores repercusiones ya que el objeto final de estas es más que un juego de forma destructiva.

c. Ego

El ego es una de las motivaciones más grandes que existen conjuntamente a la económica. Pero definitivamente esta palabra debería de estar íntimamente ligada a la reputación que tratan estos individuos de obtener por medio de actividades delincuenciales de forma digital. La satisfacción personal de sobrepasar obstáculos, aplicando técnicas aprendidas y/o utilizando herramientas artesanales en ambos casos propios, tratando de penetrar o alterar sistemas e información que están protegidos siendo unos de los blancos más usuales que estos tipos de individuos tratan de perseguir.

d. Causa

La causa o ideología es una motivación usualmente formada por diferentes factores como es el de la orientación geopolítica, las influencias culturales, religiosas, sociales, de pensamiento e históricas. La causa o la ideología dio paso a una actividad llamada "hack-tivismo" el cual encierra las anteriores mencionadas como motivación para el daño o robo de información de forma electrónica, un ejemplo de esto es aquellos motivados a que toda la información debería de ser gratuita, los piratas informáticos irrumpen en grandes corporaciones para extraer información y publicarla a través de todo lado.

e. Aceptación a un grupo social.

La aceptación del grupo social es una motivación que abarca la necesidad de pertenencia y reconocimiento. Cada persona necesita pertenecer a un grupo en cuyo interior se sienta aprobado y respetado. Esta calificación solo puede ser lograda en estos grupos realizando y sorteando actividades vandálicas como retos, hechos y meritos.

f. Estatus

El estatus resulta ser una de las partes más importantes como individuos, la necesidad de sobresalir o de una simple jerarquización en donde el que posee un peldaño más arriba se traduce en poder. La comunidad de hacker y crackers están también basadas en este punto siendo esta una de las motivaciones reales para crear algún daño, demostrando que la persona posee más conocimientos o que posee una mayor habilidad en quebrantar sistemas.

2.9. Elementos a proteger

Los tres elementos principales a proteger en una red o sistema informático son el software, el hardware y los datos. Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

Contra cualquiera de los tres elementos descritos anteriormente, se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas.

Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se trataría de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; se considera un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado.

2.10. Formas de protección

Las formas de protección se dividen en tres grandes grupos: de prevención, de detección y de recuperación. Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad. Los mecanismos de detección son utilizados para detectar violaciones de la seguridad o intentos de violación.

Finalmente, los mecanismos de recuperación son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto. Dentro de este último grupo de mecanismos de seguridad, encontramos un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

2.11. Honeypots

2.11.1. Definición

La tecnología que nos permite conocer con detalle los ataques y vulnerabilidades de las redes son los Honeypots, antes de analizar el concepto de una Honeynet es preciso explicar sobre

los Honeypots y sus diferentes tipos. Es por tal virtud que se ampliaran algunos conceptos generales que luego son de utilidad en el desarrollo del presente trabajo. Existen muchas definiciones para el término Honeypots, dependiendo de sus autores y usos. "Un honeypot, o sistema señuelo, es una herramienta de seguridad diseñada para ser sondeada, atacada y comprometida, tiene la capacidad de detectar y registrar estas acciones" [3]. De una manera más clara también se define como "recurso de un sistema de información, cuyo valor reside en el uso no autorizado o ilícito del mismo" [4], es decir un Honeypot es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas.

Directamente no es la solución a ningún problema; su función principal es recoger información importante sobre el atacante que permita prevenir estas incursiones dentro del ámbito de la red real en casos futuros.

2.11.2. Tipos de Honeypots

La clasificación de los Honeypots depende mucho del autor consultado. Según el autor Lance Spitzner [5], los Honeypots pueden ser clasificados de acuerdo al uso, es decir de acuerdo a las formas en que agregan valor de seguridad y reducen el riesgo en una organización.

2.11.2.1. Honeypot de producción

Llamados así por su ubicación junto a la red de producción en una organización, que proporciona servicios similares a la verdadera red. Su principal objetivo es mitigar el riesgo de un ataque a la red productiva dentro de una organización, aportando un valor específico para asegurar sistemas y redes con la prevención, el engaño y la disuasión de los atacantes, desviándolos de su objetivo real hacia el señuelo, permitiendo la detección.

Cuando el Honeypot detecta un ataque, se analizan las herramientas y tácticas utilizadas y se procede a reforzar los sistemas de seguridad para que el ataque no afecte a los sistemas de producción. Cuando el atacante compromete a un Honeypot, este se analiza en detalle para

caracterizarlo, se buscan estos patrones en sistemas de producción y se determina si alguno también fue comprometido.

Asi, los Honeypots representan una herramienta altamente flexible y enfocada a recopilar únicamente tráfico producido por accesos no autorizados y que, administrada por una política de seguridad de la organización, permite prevenir, detectar y responder a los ataques.

Simplemente se instalan en el mismo ambiente de los sistemas en producción, esperando atraer a los enemigos para que las investiguen, ataquen o comprometan.

2.11.2.2. Honeypot de investigación

Este tipo de Honeypot a diferencia del anterior, no añade un valor directo a la red dentro de una organización, no tiene como fin la protección porque no mitiga los ataques, tiene como propósito investigar las tácticas, herramientas y motivos de los atacantes y compartir las lecciones aprendidas, sirve como herramienta didáctica para aprender a proteger los sistemas contra nuevas amenazas. Es principalmente usado para investigación en instituciones como Universidades, organizaciones gubernamentales, militares.

Uno de los principales problemas en la seguridad de la información, es el poco conocimiento acerca de los atacantes y sus herramientas. Los Honeypots aplicados a la investigación se enfocan en detectar ataques y en generar y compartir el conocimiento requerido para que las diferentes organizaciones refuercen su infraestructura.

En otras palabras el Honeypot de Producción cumple el rol de capturar y defender y el Honeypot de Investigación sólo de capturar información para ser analizada.

La siguiente clasificación divide ambos tipos de Honeypots, tanto el de investigación como el de producción y los clasifica basándose en el grado de compromiso o riesgo que introducen en nuestra red, se mencionan dos tipos:

- Honeypots de baja interacción.
- Honeypots de alta interacción.

2.11.2.3. Honeypots de baja interacción

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

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

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

2.11.2.4. Honeypots de alta interacción

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

Retomando el ejemplo del servicio FTP, en este caso no se emularía dicho servicio, ahora se instalaría un sistema operativo Windows o Unix, al cual se le instalará el servidor FTP verdadero, al ponerlo en línea en algunos casos estará en la misma red de otros sistemas en producción, y brindará al atacante un nivel real de interactividad con el servicio.

La ventaja que se obtiene al montar esta solución es la gran cantidad de información que se puede recoger del atacante, según la complejidad del Honeypot, se puede conocer exactamente todos los pasos del intruso, sus técnicas y sus herramientas. Como el riesgo aumenta, se hace necesario implementar controles que eviten que el Honeypot se convierta en una plataforma de ataque.
Una tabla que resume las diferencias entre estos dos tipos de Honeypots se detalla a continuación:

DIFERENCIAS ENTRE LOS HONEYPOTS DE ALTA Y BAJA INTERACCIÓN	
ALTA INTERACCIÓN	**BAJA INTERACCIÓN**
Servicios, sistemas operativos o aplicaciones reales	Emulación de la pila TCP/IP, vulnerabilidades, etc.
Alto riesgo	Bajo riesgo
Difíciles en implementación y mantenimiento	Fáciles en implementación y mantenimiento
Mayor cantidad de información capturada.	Menor cantidad de información capturada.

Tabla 2.2 Diferencias de los Honeypots
Fuente Honeypots: Tracking Hackers, Autor Spitzner

Otra clasificación para los Honeypots se basa en su implementación. Se distinguen dos tipos: Honeypots físicos y Honeypots virtuales.

2.11.2.5. Honeypots físicos

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

2.11.2.6. Honeypots virtuales

Los Honeypots virtuales nacen de la necesidad de tener un gran espacio de direcciones IP, es casi imposible implementar un Honeypot por cada IP por razones en espacio físico y económico.
En una máquina física (Host), se puede levantar varios Honeypots como máquinas virtuales, los Honeypots no constituyen una máquina real, pero pueden proporcionar todo el nivel de interacción como un Honeypot Físico de Alta Interacción, la única diferencia es que está corriendo bajo algún software de virtualización y comparten los recursos físicos de la máquina real, inclusive la conexión a internet, permitiendo tener conectadas a toda una red de Honeypots con sus respectivas IPs dentro de una máquina física, facilitando la movilidad y reduciendo enormemente la cantidad de hardware usado.

2.12. Proyecto Honeynet

El Proyecto Honeynet es una organización de investigación voluntaria sin fines de lucro formada por profesionales de la seguridad dedicados a la investigación de amenazas cibernéticas y al aprendizaje de las herramientas, tácticas y motivos de la comunidad de atacantes conocidos como blackhat con la finalidad de compartir las lecciones aprendidas. Sus principales objetivos son incrementar el conocimiento e informar sobre las amenazas existentes.

El Proyecto nació de una lista de correos llamada Wargames en abril de 1999 y en junio de 2000 se convirtió en el Proyecto Honeynet. Cuenta con una junta directiva de no más de dos

miembros de la misma organización. En el año 2002 nace un foro de las organizaciones pertenecientes al proyecto llamado The Honeynet Research Alliance que comparte y despliega tecnologías relacionadas con las Honeynet. En los siguientes apartados se realiza una descripción detallada de esta herramienta, empezando por la definición, uso, características, arquitectura, tipos de Honeynets para concluir con la definición de las Honeynets Virtuales ventajas y desventajas.

2.13. Honeynets

2.13.1. Definición

Las Honeynets son un tipo de Honeypots de alta interacción, específicamente, con diferentes sistemas operativos y servicios de red, permitiendo al atacante interactuar con un entorno verdadero. Para lograr este entorno real e interactivo se deben usar sistemas reales y elementos típicos de una red. Una Honeynet no es un producto o software que se puede instalar en un computador; es toda una arquitectura.

En resumen, podemos decir que una Honeynet es una red de Honeypots de alta interacción que simula una red de producción y configurada de tal forma que toda la actividad sea controlada, registrada y regulada.

2.13.2. Uso de las Honeynets

Tradicionalmente, la información sobre seguridad ha sido puramente defensiva. Cortafuegos, Sistemas de Detección de Intrusiones, cifrado; todos estos mecanismos se usan defensivamente para proteger los recursos de alguien. La estrategia es defender la organización de alguien tan bien como sea posible, detectar posibles fallos en la defensa y entonces reaccionar a esos fallos. El problema de esta situación es puramente defensivo, el enemigo está al ataque. Las Honeynets intentan cambiar esto. El principal propósito de una Honeynet es recoger información sobre las amenazas existentes, nuevas herramientas pueden

ser descubiertas, pueden determinarse patrones de ataque, y los motivos del agresor estudiados.

Las Honeynets proveen la estrategia de detectar los fallos y mejorar en la defensa cuando se usan en conjunto con otros mecanismos de seguridad. Al recoger información de las intrusiones y estudiarlas podemos conocer nuevas amenazas y herramientas aún no documentadas, determinando así patrones de ataque y los diferentes motivos de los intrusos [6].

Las Honeynets son una herramienta, y puede ser usada para otros fines, como comprobar y desarrollar la capacidad de respuesta ante cualquier incidente. En las universidades pueden ser usadas para estudiar tipos y patrones de ataque o simplemente para investigar amenazas como función principal [7].

2.13.3. Arquitectura de las Honeynets

Como se había mencionado las Honeynets no son un producto, son toda una arquitectura, una red con un ambiente totalmente controlado, dentro de ella se tiene a los sistemas que son los objetivos. La Honeynet es como una pecera con servidores, routers, computadores personales, y todos los elementos de una red común dentro de ella como elementos, mientras se puede ver cómo los atacantes interactúan con ellos [8].

Para mantener el ambiente controlado la clave en la arquitectura de la Honeynet es su puerta de salida (Gateway) llamado Honeywall. Este dispositivo separa la Honeynet del resto del mundo. Por el Honeywall atraviesa todo el tráfico desde y hacia la Honeynet. El Honeywall es un dispositivo que originalmente era de Capa 3 pero actualmente puede ser un bridge invisible de Capa 2. Tiene tres interfaces de red (eth0, eth1, eth2) como se muestra en la Figura 2.2; las dos primeras (eth0, eth1), como puertas de entrada y salida, forman el bridge de Capa 2 separando la Honeynet con el mundo, y una tercera interface de red opcional que sirve para administración.

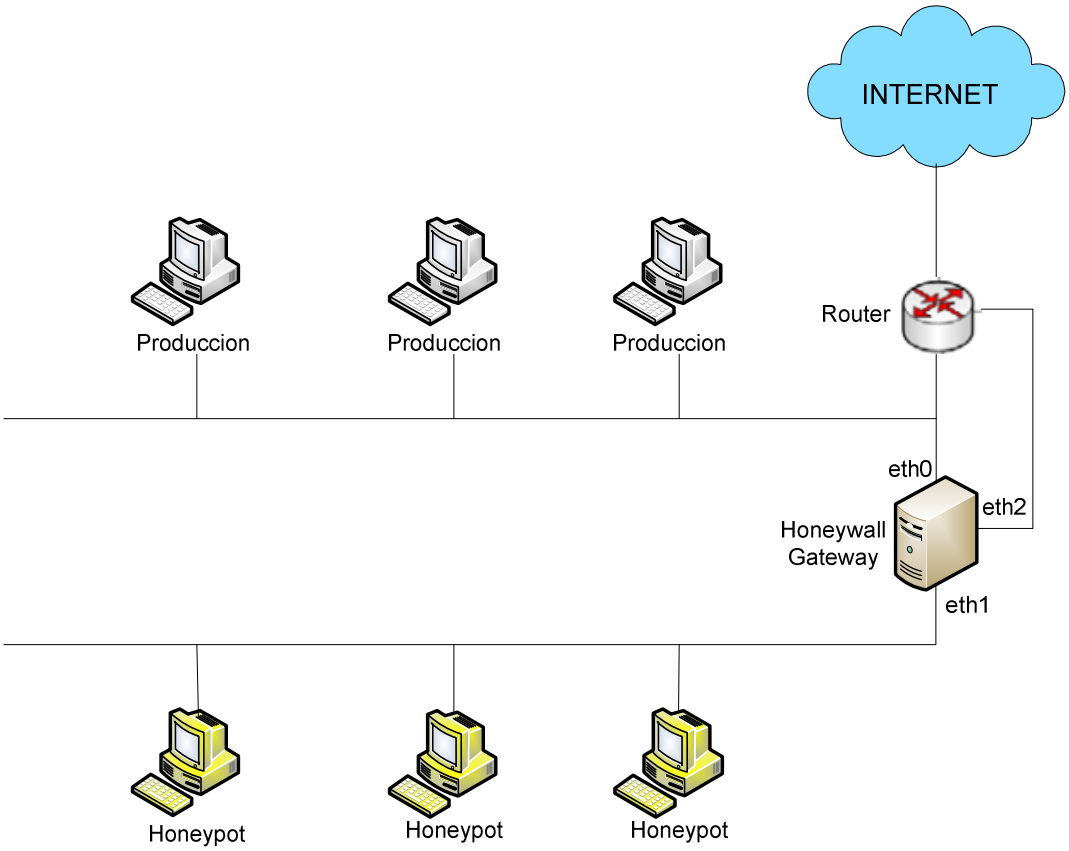


Figura 2.2 Arquitectura Honeynet

Fuente Honeynet Project, Know Your Enemy: Honeynets

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

2.13.3.1. Control de datos

El control de datos en una Honeynet es una actividad de contención, que se encarga de mitigar, reducir o de bloquear todo riesgo que se produzca desde los Honeypots hacia el mundo. Es importante que la Honeynet no sea usada por los atacantes como un arma o

herramienta de ataque hacia otros sistemas productivos. Es necesario recordar que en la Honeynet se está usando sistemas no emulados, lo cual eleva el riesgo de ser usado como herramienta de ataque.

Se debe definir qué nivel de riesgo se va manejar en la Honeynet, entre mayor sea el riesgo, mayor será la cantidad de datos obtenidos del atacante porque se estará aumentando la libertad con la que él puede interactuar con los sistemas. El control de datos es el requerimiento más importante en una Honeynet y es imprescindible, por ningún motivo se deja abierto el acceso directo sin restricciones desde y hacia los Honeypots en una Honeynet. La implementación del control de datos debe ser la suma de diferentes mecanismos sobrepuestos como capas para evitar un punto único de fallo.

2.13.3.2. Captura de datos

La captura de datos consiste en el monitoreo y registro de toda la actividad de los atacantes, con la finalidad de aprender las herramientas, tácticas y motivos de los atacantes. Al igual que el control de datos, la captura debe ser implementada en capas, proporcionando varios niveles y tipos de captura. Distintos mecanismos de captura deben agruparse, proporcionando una mayor gama de tipo de datos capturados y previniendo también los puntos únicos de fallo. Estos mecanismos pueden ir desde un simple sniffer que registre todos los datos que pasan por la red, hasta un complejo sistema que permita registrar datos sobre canales encriptados como IPSec[2], SSH[3], SSL[4].

Dentro de la captura de datos se debe analizar el lugar para almacenar la información recolectada, la cual no debe grabarse en forma local sino debe ser registrada y almacenada en un sistema seguro separado de los Honeypots.

[2] IPSec: (Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos

[3] SSH: (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

[4] SSL:(Secure Socket Layer, en español: capa de conexión segura) proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

2.13.3.3. Recolección y análisis de datos

La recolección de datos está planteada para el caso en que se tengan varias Honeynets en un entorno distribuido. Puede ser a nivel nacional o en varios sectores centralizando los datos recogidos. El análisis es el punto en el que los datos recogidos por la Honeynet son capturados y guardados de forma centralizada para que posteriormente sean analizados y estudiados en busca de patrones de ataque, nuevos ataques y lo que se haya definido como objeto de investigación.

2.13.4. Tipos de Honeynets

Siguiendo los requisitos de una Honeynet se han implementado y desarrollado tres generaciones, las cuales se diferencian en los métodos y técnicas que se usan para implementar dichos requisitos.

2.13.4.1. Honeynets de generación I

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

Como muestra la Figura 2.3, se tiene un firewall de capa 3, el cual separa la red en tres diferentes redes: Honeynet, red de producción y la Internet. Detrás del firewall se encuentra un router, los Honeypots, un detector de intrusiones de red o NIDS y un servidor centralizado de logs y alarmas.

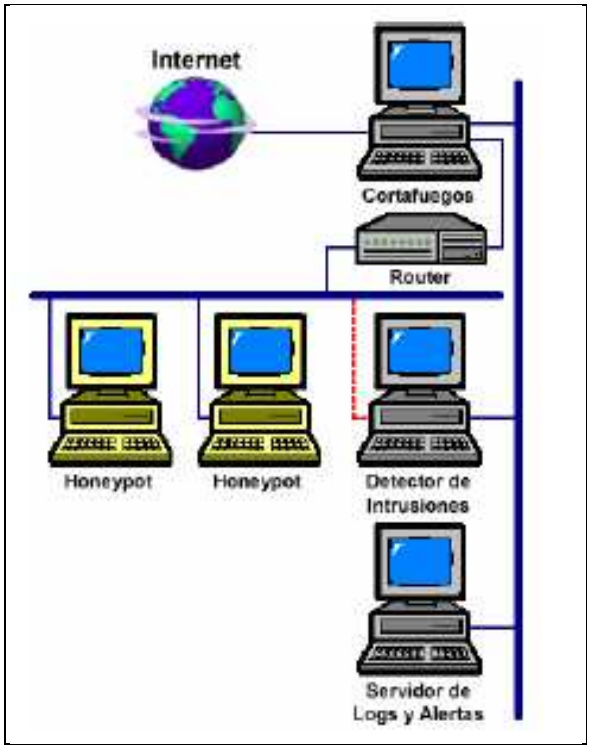


Figura 2.3 Honeynet Generación I

Fuente Gallego Eduardo, Honeynets: Aprendiendo del Atacante

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

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

- ***Control de datos (Generación I)***

El objetivo del control de datos es mitigar o debilitar el riesgo de ataques desde un Honeypot comprometido hacia una red productiva o cualquier red en el mundo. Este riesgo se lo puede

mitigar aplicando reglas sobre las conexiones salientes. En el caso de la Generación I los dispositivos que actúan son el firewall/gateway y el router.

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

Dependiendo de la calidad de información que se desee recoger esta tasa debe aumentar o disminuir y proporcionalmente aumentará y disminuirá el riesgo sobre el sistema. Para la captura de ataques automáticos como gusanos, no es necesario tener conexiones salientes, pero cuando se trata de intromisiones por parte de agentes humanos es necesario dar la libertad al atacante de descargarse sus herramientas o poder comunicarse a través de un sistema. Toda esa información es registrada y estudiada posteriormente. Al limitar el número, se reduce la posibilidad de que un Honeypot sea usado para escaneo o como herramienta para un ataque DoS (Denegación de Servicio).

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

- ***Captura de datos (Generación I)***

Los dispositivos que forman parte de la captura de datos son: el firewall, el IDS y los honeypots. El firewall/gateway captura y registra todo los paquetes que lo atraviesen en cualquier sentido, pues toda actividad en la Honeynet es sospechosa. El Firewall está diseñado

no sólo para registrar actividades, también nos alertará de ciertos eventos configurados, como el intento de conexión por Telnet, está alerta puede ser enviada por email al administrador de la red.

El IDS captura y almacena todos los paquetes circulantes en la red. Reside en un puerto de monitoreo, así que puede registrar toda la actividad de la red. Para esta tarea se usa Snort que trabaja como un NIDS (Sistema de Detección de Intrusiones de Red) en modo de full logging es decir recoge todos los paquetes IP y tcpdump que recoge todo el tráfico de red en formato binario.

Se usan estas dos herramientas para evitar un punto único de fallo, y para asegurar la integridad de los datos enviados a un servidor remoto de logs. Otra de las tareas de este sistema IDS es alertarnos de la actividad sospechosa, comparando los paquetes con una base de datos de marcas de ataques. En los Honeypots es necesario recolectar actividades dentro de los sistemas. Los atacantes más experimentados acostumbran a bloquear y borrar logs del sistema, por esto es necesario crear un repositorio externo de dichos logs salvándolos de ser borrados o alterados por el atacante. Se usa una técnica para que los sistemas repliquen sus logs al servidor remoto.

2.13.4.2. Honeynets de generación II

Este segundo modelo dentro de las generaciones de las Honeynets fue lanzado y ha sido usado desde principios del 2002 por el Honeynet Project. En relación a su antecesora, esta arquitectura introduce una serie de modificaciones, las cuales se enfocan en aumentar la interacción con el atacante para aumentar la cantidad y calidad de datos recolectados. Para esta tarea fue necesario ocultar mejor los sistemas haciéndolos prácticamente indetectables.

Como se muestra en la Figura 2.4, esta arquitectura es mucho más sencilla que la presentada en la Generación I, las tareas de control y captura de datos ahora están centralizadas en un solo dispositivo llamado Honeywall lo que permite que esta arquitectura sea fácil de desarrollar y mantener.

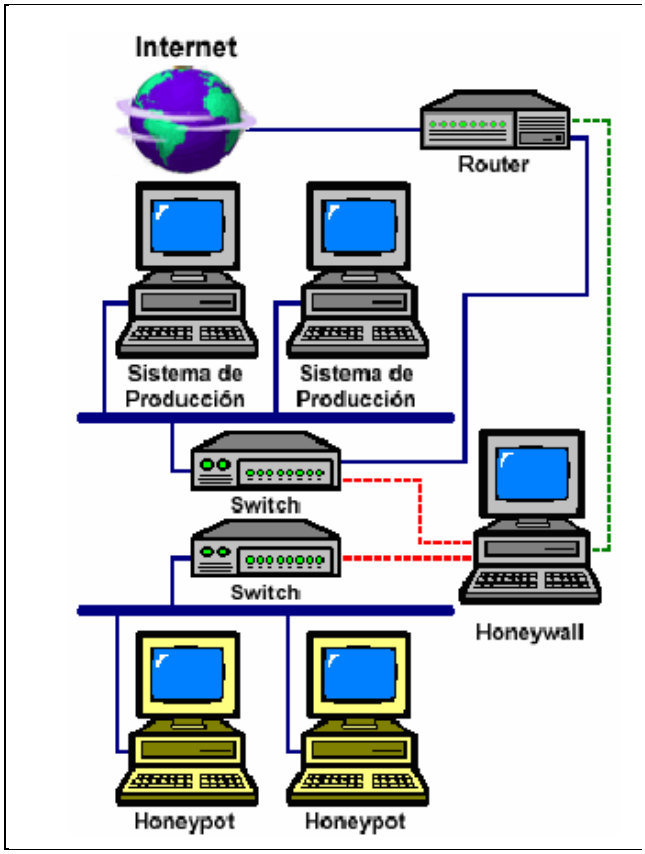


Figura 2.4 Honeynet Generación II
Fuente Gallego E, Honeynets: Aprendiendo del Atacante

El Honeynet Gateway denominado Honeywall es un dispositivo con tres interfaces de red: eth0, eth1, eth2. La interface externa eth0 del Honeywall se conecta con el sistema de producción, la interface interna eth1 se conecta con la Honeynet, ambas están a modo de puente (bridge) transparente lo cual significa que no poseen una dirección IP.

La tercera interfaz eth2 sí tiene una dirección de IP y es conectada a una red segura con fines de administración y recolección de datos. El comportamiento del Honeywall como dispositivo de Capa 2 es decir en modo bridge, lo vuelve transparente, dificultando enormemente su detección por parte de los atacantes y permite la integración de la Honeynet a la red de producción. Esta integración permite el estudio de ataques internos y externos en los sistemas de producción, en el caso de la Generación I esta tarea se dificulta porque se tienen dos redes la Honeynet, y la red de producción totalmente aisladas.

- ***Control de datos (Generación II)***

Para mejorar la arquitectura de la Generacion I, la cual usaba un firewall que trabajaba en capa 3, que lo hacía fácilmente detectable, se resolvió crear un gateway de capa 2 transparente, el cual es mucho más difícil detectar. En este único dispositivo va funcionar el control de datos de la Honeynet, será un firewall que controle y cuente todas las conexiones que entran y salen pero ahora en modo bridge.

Se agrega una nueva capa al control de datos, un NIPS (sistema de prevención de intrusos). El NIPS trabaja de la misma forma que un IDS (sistema de detección de intrusos), tiene la capacidad de analizar en tiempo real un paquete, usa una base de datos de firmas con ataques conocidos, si el paquete coincide con un ataque este puede ser bloqueado o modificado para hacerlo inofensivo, para mejorar la interacción con el atacante y hacer más invisible el sistema se puede modificar los paquetes, permitiendo al intruso ejecutar sus ataques pero sin llegar a afectar a los sistemas comprometidos.

Los NIPS bloquean o modifican ataques que sean conocidos y configurados en su base de datos, pero para ataques nuevos no representan una barrera. En este caso entra la primera capa del control de datos que viene de la Generacion I y el honeywall bloqueará paquetes utilizando el conteo de conexiones inhabilitando cualquier ataque que supere el umbral configurado.

- ***Captura de datos (Generación II)***

La captura se ejecuta en tres capas, exactamente igual como lo hacía la Generación I, la capa del firewall, la capa de red y la capa de los sistemas. La diferencia está en que la recopilación de los datos se realiza en forma centralizada desde el Honeywall y la captura para la capa de los sistemas se realiza mediante el uso de una herramienta llamada Sebek.
La herramienta Sebek incorporada en el Honeywall permite capturar la información aun cuando se utilice un medio cifrado ya que funciona a nivel de kernel del Sistema Operativo. Además, cuenta con programas que permiten limitar la cantidad de conexiones por unidad de

tiempo, junto con monitorear y cambiar las reglas del firewall. También se puede limitar el ancho de banda utilizado pero esta opción no es muy común.

En la Generación II se agrega unas características adicionales la de recolección de datos y las alertas. El sistema de alertas envía un correo electrónico al administrador de la Honeynet cada vez que un evento muestre alguna intrusión en la misma.

2.13.4.3. Honeypots de generación III

La tercera generación de las Honeynet se da a conocer a inicio de 2005. Con respecto a su arquitectura es muy similar a su antecesora, manteniendo los mismos dispositivos y características. En esta nueva generación se mejoran las versiones de las herramientas usadas, además se caracterizan por integrar análisis de datos en el mismo dispositivo Honeywall, lo que hace más sencillo su utilización y mantención, anteponiendo como su principal objetivo el de mejorar el análisis de los datos recogidos.

Durante la etapa de vida de la Generación II se tomó como experiencia la gran cantidad de datos recogidos por la Honeynet y su dificultad al ser analizados, ya que cada herramienta en cada capa de recolección de datos manejaba su propio formato, y no se los podían vincular. Si existe un ataque se debe rastrear su tiempo de vida en todos los niveles de captura, para luego realizar el análisis de los datos por separado, lo que consume mucho tiempo, debido a que se tienen diferentes archivos como: logs de sistemas, y registros en base de datos que deben ser vinculados unos con otros.

La Generación II en captura de datos presentaba limitantes al no definir un formato de recolección, cada fuente de datos tiene un formato independiente, todo esto simplemente retrasaba la tarea de investigación, por estas razones nace un nuevo requisito, el análisis de datos

.

El análisis de datos en la Generación III, unifica todos los datos registrados por cada herramienta de la captura de datos relacionándolos con los datos proporcionados por el

control de datos, de esta forma se puede saber precisamente qué conexión generó una alerta y será posible rastrear todos los paquetes que están relacionados a esa conexión. Todos estos datos ahora están relacionados pero proceden de fuentes y herramientas distintas. Para poder unificar formatos, alguna de las herramientas usadas en la captura de datos han sido modificadas y actualizadas, como es el caso del Sebek, el cual para ésta generación corre desde su versión 3.0.

2.13.4.4. Honeynets virtuales

Una Honeynet Virtual se basa en el mismo concepto de la Honeynet pero implementándose dentro de un mismo computador, todos sus dispositivos son virtualizados mediante un software que permita esta tecnología. Dentro de una máquina física se levantan los Honeypots como máquinas virtuales formando la Honeynet Virtual. Dependiendo de la configuración de cada uno, y de la arquitectura de red, se puede hablar de Honeynets virtuales de I, II, III generación.

La idea de virtualizar el sistema es reducir costos por requerimiento de dispositivos, entre más grande es la Honeynet, más dispositivos y espacio físico se necesita. En una Honeynet Virtual todo se encuentra en una sola máquina física. En el caso de aumentar más dispositivos virtuales simplemente se mejora el hardware de la máquina anfitriona. Entre las limitaciones tenemos: el hardware necesario de la máquina que alberga a la Honeynet, el software que es usado para virtualizar, si el atacante toma en su poder la máquina anfitriona tendría control sobre toda la Honeynet y sería un peligro para los sistemas reales.

Las Honeynet Virtuales se dividen en dos grandes tipos: Autocontenidas e Híbridas .

- ***Honeynet Virtual Autocontenida***

Una Honeynet Virtual Autocontenida es una red entera Honeynet condensada en un sólo computador. La red entera está virtualmente contenida en un único y físico sistema. Una red

Honeynet típicamente consiste de un cortafuegos para control de datos y captura de datos, y los Honeypots dentro de la Honeynet, ver Figura 2.5.

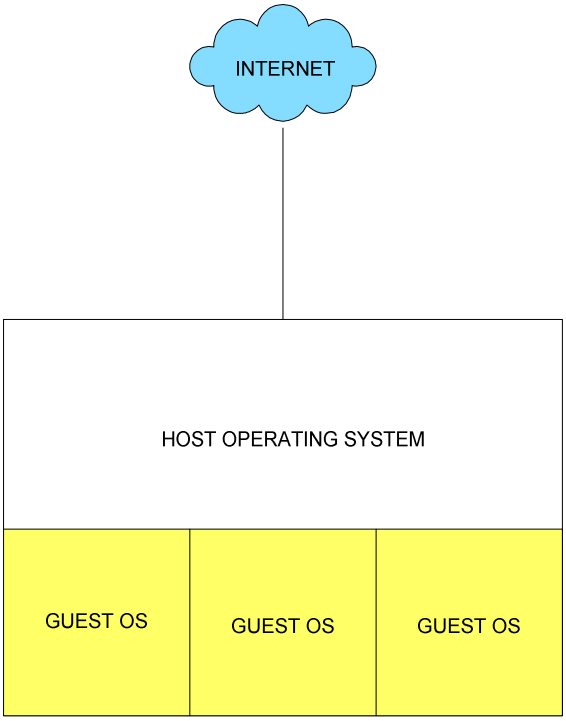


Figura2.5 Honeynet Virtual Autocontenida
Fuente Honeynet Project, Conoce a tu enemigo: Definiendo Honeynets Virtuales

Las ventajas que presentan este tipo de Honeynets Virtuales son:

- Movilidad: pueden ser instaladas en un portátil y llevadas a cualquier parte.
- Rápida puesta en funcionamiento: una vez instalada, sólo hay que conectarla a la red y configurarla en pocos minutos.
- Plug and Play: fácilmente pueden ser conectadas dentro de una red o de otra, ya que la implantación es fácil por ser un solo dispositivo.
- Económica: ahorra dinero porque no necesita de varios equipos, y ahorra espacio al usar un dispositivo.

Las desventajas que presentan este tipo de Honeynets Virtuales son:

- Punto único de fallo: si falla el hardware toda la Honeynet queda sin funcionar.

- ❖ Máquina potente: es necesario un computador potente para simular una red grande con muchos dispositivos.
- ❖ Seguridad: como se comparten dispositivos físicos como discos duros y unidades, es posible que el atacante pueda acceder a otras partes del sistema. La seguridad depende del software de virtualización.
- ❖ Limitación por software. como todo tiene que ejecutarse en una sola máquina, hay software que no se podrá utilizar por problemas de incompatibilidad. Por ejemplo un sistema operativo de cisco en una máquina con un procesador de Intel.

- ***Honeynet Virtual Hibrida***

Una Honeynet Híbrida es una combinación de la clásica Honeynet y del software virtual. Captura de Datos, como por ejemplo cortafuegos, y control de datos, como por ejemplo sensores IDS y almacenamiento de logs, están en un sistema separado y aislado. Este aislamiento reduce el riesgo de compromiso. Sin embargo, todas las Honeynets son virtualmente ejecutadas en una única máquina ver Figura 2.6.

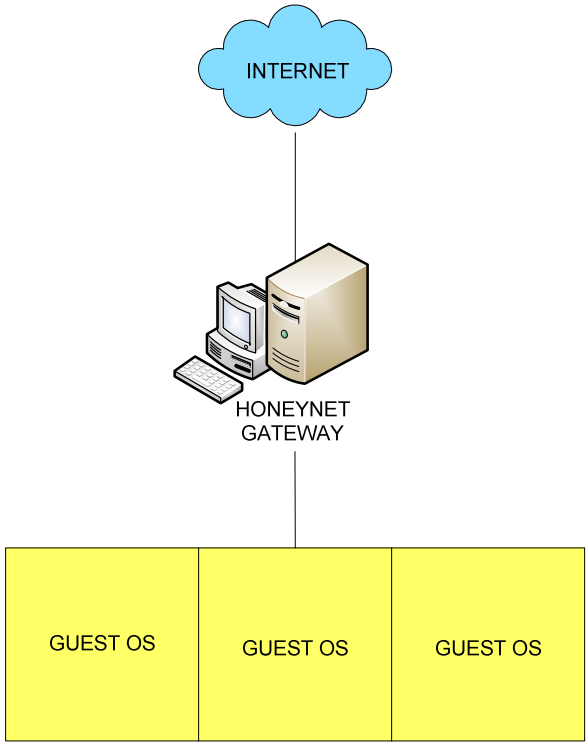


Figura 2.6 Honeynet Virtual Híbrida

Fuente Honeynet Project, Conoce a tu enemigo: Definiendo Honeynets Virtuales

Las ventajas que presentan este tipo de Honeynets Virtuales son:

- Seguridad: eliminan el punto único de fallo y aíslan los datos y el control en otro dispositivo.
- Flexible: se tiene un dispositivo que contienen diferentes tipos de Honeypot que son máquinas virtuales, las cuales pueden ser de diferentes tipos con diferentes servicios, fáciles de copiar, borrar, duplicar, lo que facilita enormemente en la tarea de administración. Si se daña un Honeypot sólo hay que levantar un duplicado ya pre instalado.

Las desventajas que presentan este tipo de Honeynets Virtuales son:

- Se dificulta la movilidad: debido a que tenemos dos dispositivos.
- Costosas: se incrementa el costo por hardware y en espacio. Para cualquier tipo de Honeypot o Honeynet Virtual hay que considerar que pueden ser usadas técnicas de fingerprinting (obtención del tipo y versión del sistema operativo mediante el envío de paquetes IP específicamente construidos) sobre los Honeypots revelándole al atacante la virtualización de los sistemas.

CAPITULO III

SUSTENTO EMPIRICO

3.1. Análisis de la situación actual

La Empresa Minera SOMINEX SRL., al ser una institución privada que maneja un flujo continuo de datos referentes a todas sus actividades principales, necesita garantizar la consistencia de la red, permanencia de los recursos informáticos y la seguridad de los datos que transitan a través de su red de datos, con el fin de evitar las pérdidas o alteraciones indebidas de la información.

3.1.1. Modelo actual de la red

El modelo de la red actual, se basa en una topología estrella además de tratarse de una arquitectura Cliente/Servidor, donde existe un servidor que contiene el principal sistema con el se trabaja, siendo ahí donde se almacena toda la información critica para la empresa y los clientes son equipos computacionales de escritorio o portátiles.

La figura 3.1, muestra de forma esquemática el modelo de la red que funciona actualmente en la organización de caso de estudio.

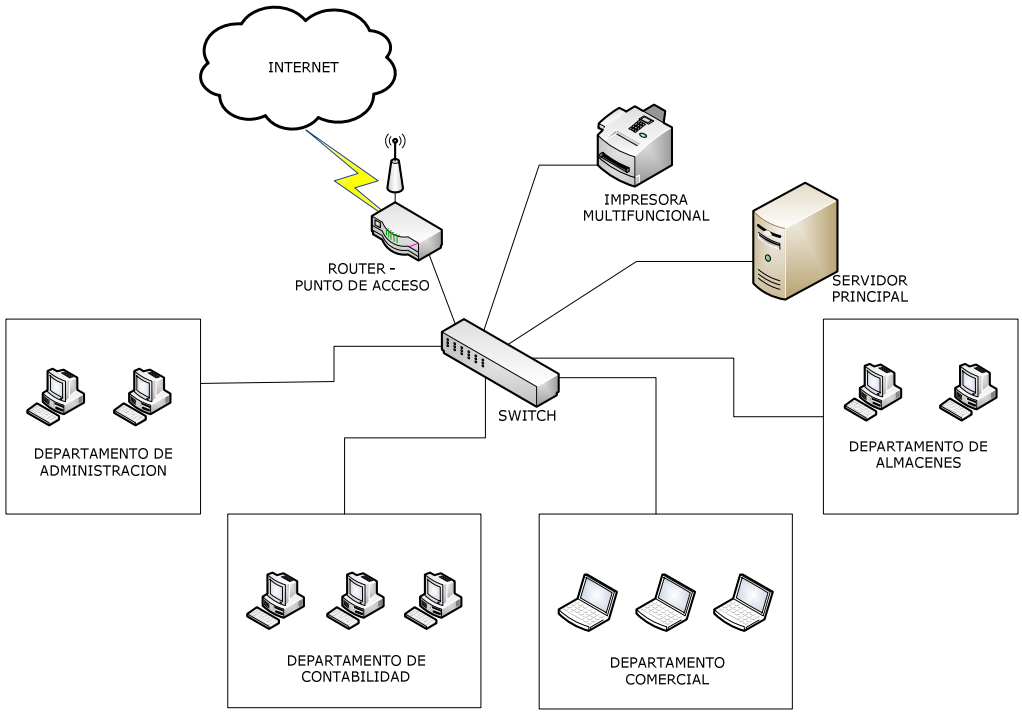


Figura 3.1. Modelo de red actual de la Empresa Minera SOMINEX SRL.
Fuente: Elaboración Propia

Como se puede observar, el servidor está conectado a la red local y la red local se conecta a Internet a través de un router. La red local e Internet, no están separadas por ningún dispositivo que filtre los paquetes y las aplicaciones que llegan del exterior, esa es la función de un firewall, pero la red actual no posee ningún dispositivo de red con esta finalidad.

La red local y el servidor, están directamente conectados a un conmutador, este conmutador se encarga de distribuir datos a la red local de la organización, lo cual permite gozar de un muy buen medio para el transporte de la información a lo largo de las instalaciones de la misma. Cabe aclarar, que solo existe un conmutador y todos los equipos computacionales, incluido el servidor, están conectados en una sola red física.

El hecho que exista una sola red que incluya a todos los equipos computacionales, tiene repercusiones importantes en la seguridad, ya que si se logra vulnerar, pasando el router, se puede acceder a cualquier equipo, causando daños que serían más peligrosos si están dirigidos al servidor.

La red implementada actualmente en la organización, permite brindar los servicios de correo electrónico, páginas web, archivos y carpetas compartidas mediante administración de directorios y finalmente, cuentas de usuario personales para la autenticación[5] al dominio[6] corporativo, estos servicios son usados por todo el personal.

El servicio de Internet, permite el acceso a páginas web y servicios de mensajería instantánea sin restricciones ya que la empresa no tiene definidas políticas de seguridad. El correo electrónico corporativo, es accesible por el empleado dueño de una cuenta, desde cualquier lugar del mundo mediante un servicio de webmail, el espacio de buzón de correo es ilimitado. Mediante el servicio de directorio y archivos compartidos, todos los empleados pueden obtener documentos de la red corporativa, estos documentos son almacenados en un solo servidor de archivos accesible por todos los usuarios y administrado en algunas ocasiones por personal eventual del área de sistemas.

Todos los movimientos sobre las transacciones comerciales referentes al movimiento de concentrado de mineral así como, información acerca de los proveedores y clientes con los que se trabaja, vale decir, creación, modificación, anulación, liquidación sobre los minerales, pagos, deudas, precios, leyes, cotizaciones y términos de contrato son registrados mediante un sistema interno informático transaccional que está desarrollado en un entorno Unix con una base de datos relacional.

3.1.2. Identificación de las vulnerabilidades

Por vulnerabilidad se entiende a la exposición latente a un riesgo o amenaza, es decir, a la capacidad y posibilidad de un sistema de responder, reaccionar o de recuperarse ante una amenaza o un daño. Con la adopción de Internet como instrumento de comunicación y colaboración en la Empresa Minera SOMINEX SRL., los riesgos se han incrementado y,

[5] Autenticación: Servicio de seguridad que garantiza que el origen de datos, o entidad homóloga, son quienes afirman ser.

[6] Dominio: Sistema de denominación de equipos computacionales en una red, consta de un conjunto de caracteres que identifica un sitio de la red accesible por un usuario.

ahora, la institución se encuentra vulnerable a recibir ataques de todo tipo incluyendo negación de servicio, accesos no autorizados y amenazas combinadas.

En general, las herramientas para la detección de vulnerabilidades obedecen a dos tipos diferentes: las basadas en la red y las basadas en el host. Centrándose las primeras en la identificación de cuestiones relacionadas con los servicios que, como HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) y SMTP (Simple Mail Transfer Protocol), corren en los sistemas de la red.

3.1.2.1. Identificación de vulnerabilidades basadas en la red

La identificación de vulnerabilidades basadas en la red, se realizo mediante la ayuda de la herramienta de software Nmap, con el cual se procedió al escaneo de puertos, en busca de puntos débiles en la red de la organización.

Tras el escaneo de puertos se obtuvieron los siguientes resultados ver tabla 3.1:

- Puertos Cerrados: 1690.
- Puertos Abiertos, algunos se detallan a continuación:

PUERTO	**ESTADO**	**SERVICIO**
21/tcp	Abierto	ftp
22/tcp	Abierto	Ssh
53/tcp	Abierto	Dominio
80/tcp	Abierto	Http
143/tcp	Abierto	Imap
389/tcp	Abierto	Ldap
3128/tcp	Abierto	Squid-http

Tabla 3.1. Resultado de Escaneo de Servicios y Puertos abiertos.
Fuente: Elaboración Propia.

De acuerdo a los datos mostrados en la tabla 3.1, no existen puertos abiertos que ofrezcan servicios no comunes o sospechosos, pero cabe aclarar, que esto no garantiza una invulnerabilidad de la red. Tomando solamente el servicio de páginas web (http - puerto 80), se han detectado las vulnerabilidades que podrían causar los siguientes incidentes de seguridad:

- Traceado de sitio cruzado, que permite depurar aplicaciones remotamente.
- Denegación de servicio, ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- Inyección SQL, que puede causar la captura de datos sensibles.

Estos son solo algunos de los incidentes de seguridad que pueden ocurrir, por lo que, afirmar que no existen vulnerabilidades y que la protección es total, es considerado un mito; el hecho de que la red este conectada a Internet, abre la posibilidad a incidencias a la seguridad de la misma, esto lleva a revisiones periódicas del estado de vulnerabilidades para tomar medidas de seguridad.

3.1.2.2. Identificación de vulnerabilidades basadas en el host

Con la identificación de vulnerabilidades basadas en el host, se pretende obtener puntos débiles a nivel de sistema, como permisos de archivos, propiedades de cuenta de usuario y establecimiento de registros, para realizar este estudio se siguieron una serie de procesos que son explicados a continuación:

En primera instancia se verifico, que el acceso al sistema se realiza mediante el ingreso de una contraseña por parte del usuario, con el uso de la herramienta de software LOphtcrack se observo que esta contraseña posee un grado de dificultad mínimo, por lo que toda la información contenida en ese equipo, corre peligro ya que usuarios no deseados pueden acceder a la información, y causar grandes daños a la organización.
Posteriormente, se pasó a verificar si se tiene configurada las directivas para contrarrestar contraseñas en el Sistema Operativo Windows XP, sistema usado actualmente por la

Empresa Minera SOMINEX SRL., esta es una medida implementada por Microsoft, para imponer a los usuarios a que usen contraseñas más fuertes ver Figura 3.2

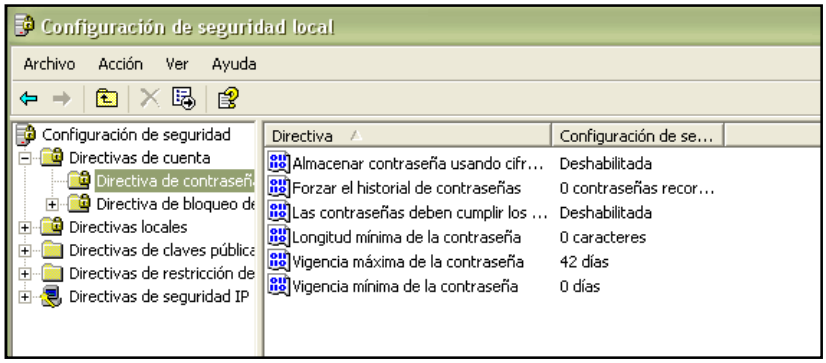


Figura 3.2. Directiva para contrarrestar contraseña
Fuente: Imagen obtenida del Sistema Operativo Windows XP usado en los equipos de la Empresa SOMINEX SRL.

Se pudo evidenciar que no tienen configuradas ninguna de estas directivas, lo que significa que el usuario está en la libertad de poner una contraseña con cualquier grado de dificultad, este es un aspecto negativo para resguardar la seguridad de la información, si un usuario utiliza una contraseña simple.

Otra de las directivas a verificar, es uno de los pasos más importantes que se debe tomar cuenta para mitigar los ataques de adivinación de contraseña, consistiendo esta directiva en el establecimiento del umbral de bloqueo de cuenta, como se observa en la siguiente Figura 3.3 la empresa tampoco tiene implementada esta directiva.

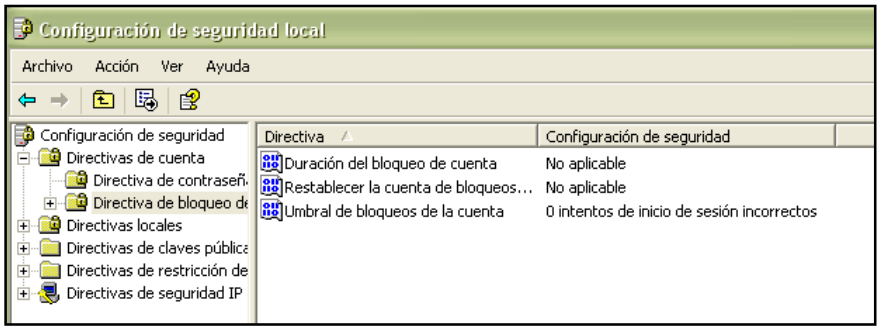


Figura 3.3. Directiva en el establecimiento del Umbral de Bloqueo
Fuente: Imagen obtenida del Sistema Operativo Windows XP usado en los equipos de la Empresa SOMINEX SRL.

Por otra parte, se tiene otra directiva para contrarrestar la adivinación de contraseñas, que consiste en el anuncio de inicio de sesión personalizado en TS (Terminal Service), se implementa mediante una observación legal personalizada para el inicio de sesión de Windows ver Figura 3.4, con la finalidad de obstruir ataques, de igual manera esta opción no se encuentra configurada en este equipo.

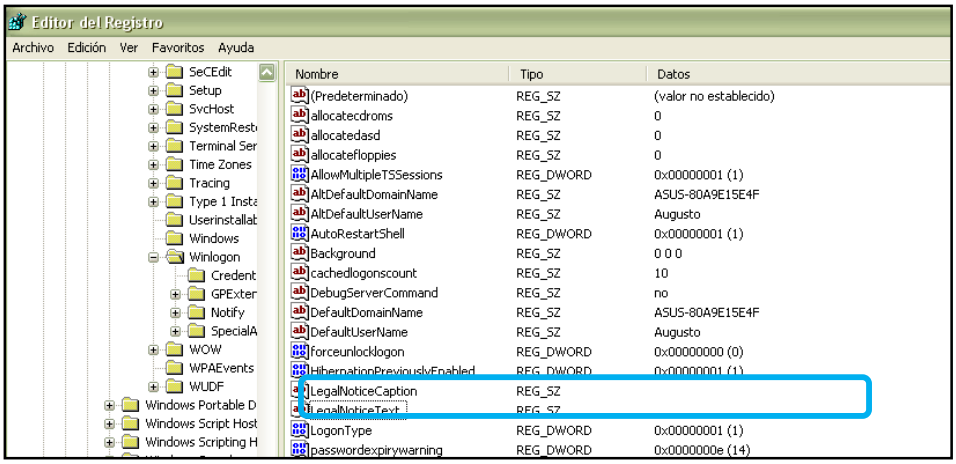


Figura 3.4. Directiva de Anuncio de Inicio de sesión personalizado
Fuente: Imagen obtenida del Sistema Operativo Windows XP usado en los equipos de la Empresa SOMINEX SRL.

Otra directiva que no está implementada es el de auditoría y registros, aunque es probable que nunca entre alguien a su sistema por medio de una adivinación de contraseña, porque ha implementado la complejidad de contraseña y la directiva de bloqueo, aún resulta inteligente registrar intentos de inicio de sesión fallidos ver Figura 3.5.

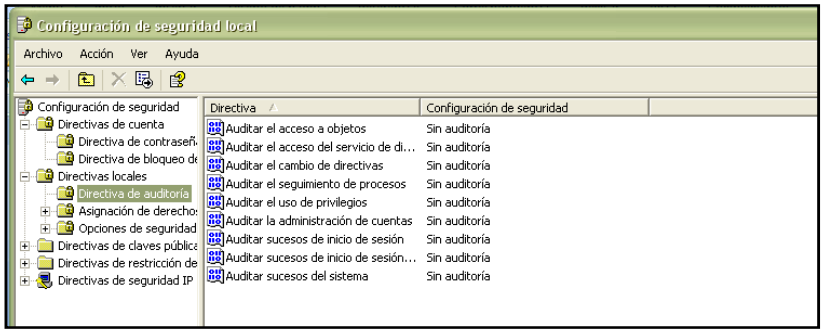


Figura 3.5. Directiva Auditoría y registros
Fuente: Imagen obtenida del Sistema Operativo Windows XP usado en los equipos de la Empresa SOMINEX SRL.

Otra de las directivas que debería ser aplicada en el entorno de la empresa es evitar el escalamiento de privilegios, como se observa en la siguiente Figura 3.6 el inicio de sesión no está restringido a nadie, pudiendo, tener acceso cualquier usuario de la empresa.

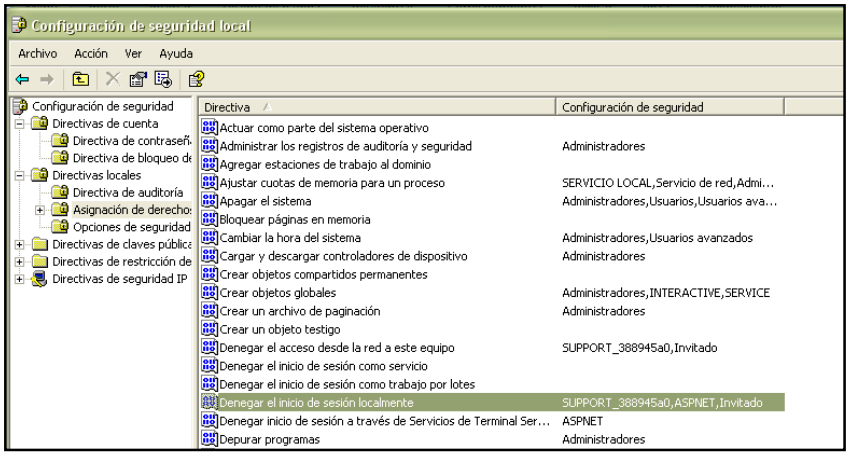


Figura 3.6. Configuración para evitar el escalamiento de Privilegios
Fuente: Imagen obtenida del Sistema Operativo Windows XP usado en los equipos de la Empresa SOMINEX SRL.

Es necesario recalcar que la identificación de vulnerabilidades, se realizo en todos los equipos de la empresa, además de verificar que todos tienen la misma configuración podemos determinar las siguientes conclusiones:

Entre los errores de seguridad más comunes que se pudieron encontrar, está el de instalar cualquier software del sistema sin quitar los servicios innecesarios, ni instalar todos los parches de seguridad recomendados. También la falta de contraseñas, o el uso de estas con pocos caracteres, es un problema de seguridad enorme para cualquier corporación. También deberían evitarse las contraseñas débiles, predefinidas o por defecto.

Demasiados puertos abiertos para que algún usuario pueda conectarse a su PC es contraproducente. Las recomendaciones pertinentes son cerrar todos los puertos y luego solo abrir los que realmente se necesiten.

Cuando alguien utiliza asistencia remota de Windows para conectarse a un equipo, esta persona puede ver el escritorio, los documentos abiertos y cualquier información privada

visible. Además, si permite que la persona que le ayuda controle su equipo con su mouse y teclado, podrá realizar tareas como eliminar archivos o cambiar configuraciones. Por lo tanto, sólo debe permitir el acceso o el control compartido de su equipo a personas en las que confíe.

3.1.3. Determinación de problemas y necesidades

3.1.3.1. Problemas

Tradicionalmente el uso de estos sistemas y elementos como los cortafuegos son utilizados como sistemas de seguridad puramente defensivos y reactivos debido a que estos toman un tipo de acción ya sea de inspección o de clausura de intercambio de información al tener un tipo de ataque contra él o la red que protege. Debido a esto, es que el uso de herramientas adicionales que conjuntamente interactúen y realicen actividades proactivas de seguridad son mandatorios, dando la facultad de ser manejadores de intrusos y sus ataques, resguardando de una mejor manera la información en los periodos de incidente y no bajo un esquema de presentarse a merced del atacante que es lo que se logra con un esquema defensivo, como el que actualmente utiliza la empresa.

El no establecimiento de políticas o mecanismos de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, el almacenamiento de la información critica la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos, constituyen uno de los principales problemas que tiene la Empresa Minera SOMINEX SRL., de la misma manera tampoco se cuenta con un sistema de seguridad que este orientado al desarrollo de Honeynets Virtuales, gracias a la cual se puede aprender sobre las herramientas, tácticas, y motivos de la comunidad de atacantes, información que es crítica para las organizaciones para entender mejor y protegerse de las amenazas que tienen.

Los problemas se pueden resumir de manera puntual en el siguiente listado:

- Ausencia de reglamentos, mecanismos y/o políticas de seguridad, para manipular de manera adecuada la información y/o responder ante una incidencia o ataques informáticos.
- Falta de sistemas o herramientas de seguridad proactivas que formen en conjunto un sistema de seguridad.
- Falta de protección a los recursos y la información con se cuenta en la red, a través de herramientas y de procedimientos basados en una política de seguridad que permitan un control adecuado.
- No se realiza copias de seguridad periódicas de toda la información gestionada y almacenada.
- No se actualizan los sistemas, ni aplicaciones tanto en software como en hardware de los componentes de seguridad debido a que la tecnología cambia constantemente.
- Inconsciencia por parte del personal de la empresa, respecto a la peligrosidad que implica estar conectados a Internet.
- Falta de conocimiento por parte del personal de la empresa, respecto a herramientas y políticas de seguridad.
- No existe un monitoreo constante de la información contra ataques constantes y técnicas novedosas implementadas por lo intrusos informáticos.

3.1.3.2. Necesidades

Debido a que muchos sistemas están expuestos a, agujeros de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Es necesario que en la actualidad se disponga de mecanismos o políticas de seguridad, con la finalidad de asegurar la información, como también es imprescindible contar con el diseño de una herramienta de solución de seguridad, la cual impida el acceso de usuarios no deseados , un mejor aseguramiento del servidor ya que tiene toda la información critica y además que fortalezca la red interna para así proteger la información y datos importantes que se transmiten a través de toda la infraestructura de red de la organización, la mayoría de las veces por simple

desconocimiento se empieza a preocupar solo cuando ocurre algún problema algunas ocasiones con muy poco remedio.

Por tal razón es muy importante y necesario, el desarrollo de una herramienta de seguridad puesto que los sistemas Honeynet presentan un enfoque innovador con respecto a los sistemas de seguridad tradicionales. En vez de repeler las acciones de los atacantes, constituyen un punto de distracción de los sistemas reales ante cualquier ataque o atacante, con la finalidad de utilizar técnicas para monitorizarlas y registrarlas de esa manera se aprende mucho sobre los intrusos, desde como entran en los sistemas, como se comunican y por qué atacan sistemas, como también las amenazas a las que se enfrenta la empresa diariamente.

Al igual que los problemas, las necesidades que tiene la empresa, se pueden resumir de manera puntual en el siguiente listado:

- Contar con mecanismos de seguridad, que permitan proteger y gestionar de manera adecuada la información de la empresa, con la finalidad de proteger la red de ataques externos e internos.
- Es necesario que los empleados de la empresa, se informen y capaciten sobre las políticas de seguridad aplicables a la gestión de la información.
- Contar con un sistema de seguridad integral que este orientado el desarrollo de Honeynets virtuales que permita la captura y control de datos, para aprender sobre los intrusos.
- Es necesario, fortalecer la seguridad existente y complementaria con una herramienta que se presenta como un sistema vulnerable que desviara la atención de los atacantes de los sistemas o servicios en producción protegiéndolos de accesos no autorizados.
- Mantener resguardada la información de la red contra constantes ataques cada vez con técnicas novedosas que son empleadas por los intrusos informáticos.

3.1.4. Estudio de factibilidad

Los estudios de factibilidad establecen si el proyecto es posible realizarse, a fin de que se cuente con los recursos y capacidades para cumplir con los objetivos y necesidades, con el propósito de considerar que es apropiado, aceptable e importante para desarrollarse.

3.1.4.1. Factibilidad Técnica

La seguridad de la información, requiere de la aplicación de tecnologías que permitan confiabilidad, disponibilidad y escalabilidad para ser expandidas o modificadas, según la dinámica del entorno. Este trabajo, contempla la integración de tecnologías de herramientas de seguridad en redes, con una combinación adecuada, que permite una adaptación al entorno.

- **Hardware requerido**

El CDROM Honeywall debe ser instalado en un sistema con al menos 256MB de RAM., también se debe considerar que los datos recolectados y el tiempo de recolección pueden requerir gran capacidad de almacenamiento. Por este motivo es necesario discos duros adicionales o uno con capacidad mínima de 100 GB. Por el momento sólo se soporta IDE; no hay soporte para SCSI. La velocidad del procesador requerida por el Honeywall también depende de la cantidad de tráfico de la red. Se sugiere contar como mínimo con un Pentium III o equivalente. Al menos dos interfaces de red son necesarias para utilizarlo como pasarela y opcionalmente puede utilizarse una tercera interfaz para accesos de administración remota.

Es así, que el hardware requerido para la implementación del Honeywall se resume en la siguiente tabla:

Descripción de componente	**COSTO**
- Un procesador Intel Pentium III. - Un módulo de memoria RAM de 256MB	

- Un Disco duro IDE 100 GB. - Tarjeta de video 128 MB - Tarjeta de sonido 32 Bits - Tres tarjetas de red de 10/100/1000 Mbps - Lector u quemador de CD's interno - Un Monitor ACER de 17" - Un Teclado Ergonómico - Un Mouse "Genius Net Mouse"	700$
SUBTOTAL	700$

Tabla 3.2 Especificación de hardware requerido para el Honeywall

Fuente Elaboración propia

De la misma manera, el hardware requerido para la implementación de los Honeypots se resume en la siguiente tabla:

Descripción de component	**COSTO**
- Dos procesadores Intel Pentium III. - Dos módulos de memoria RAM de 256MB - Dos discos duros IDE 30 GB. - Dos tarjetas de video 128 MB - Dos tarjetas de sonido 32 Bits - Dos tarjetas de red de 10/100/1000 Mbps - Dos lectores o quemadores de CD's internos - Dos monitores ACER de 17" - Dos teclados ergonómicos - Dos mouses "Genius Net Mouse"	1400$
SUBTOTAL	1400$

Tabla 3.3 Especificación de hardware requerido para los Honeypots

Fuente Elaboración propia

Al proponer una solución que incluya la utilización de una herramienta de software que permita virtualizar los tres equipos de computación requeridos, además de contar con un equipo proporcionado para esta finalidad, con lo que se reduce enormemente los costos que involucrarían implementar la solución propuesta, es así que las características con las que cuenta este equipo son las siguientes:

Descripción de componente
- Un procesador Intel Core i3, 2.13 GHz - Un módulo de memoria RAM de 4 GB - Un Disco duro IDE 500 GB. - Tarjeta de video NVIDIA GeForce 310 MB - Adaptador de red Gigabit Ethernet - Lector u quemador de CD's interno

Tabla 3.4 Especificación de hardware disponible

Fuente Elaboración propia

- **Software requerido**

En cuanto al software requerido para la instalación de la herramienta de seguridad Honeynet Virtual, se mencionan los siguientes:

DESCRIPCIÓN	**COSTO**
VMware Workstation 6	150$
Linux – Debian	0
CD-ROM Honeywall	0
Sebek	0
Nephentes	0
SUBTOTAL	150$

Tabla 3.5 Especificación de software requerido

Fuente Elaboración propia

Como se puede observar, la mayoría de estas herramientas son de distribución libre, y se pueden obtener desde sus correspondientes páginas web.

Por lo tanto, desde el punto de vista técnico, es realizable, ya que se dispone en el mercado del equipo necesario para dar soporte al diseño que se va desarrollar, que es el desarrollo de la propuesta de una Honeynet Virtual, para la detección de posibles ataques informáticos orientada a los requerimientos y necesidades de la Empresa Minera SOMINEX SRL., también se cuenta con el software requerido para poder implementar esta herramienta.

3.1.4.2. Factibilidad operacional

La implementación de medidas de seguridad, es un proceso técnico administrativo, proceso que debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por la Gerencia General, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria requerida. Resulta claro que proponer la implementación de un sistema de seguridad con Honeynet Virtual genera ganancias a toda la organización, pero trae una nueva tarea para la parte técnica, es importante recalcar un componente muy importante para la protección de los sistemas, que consiste en la atención, vigilancia continua y sistemática por parte de los responsables de la seguridad de la información y de la red.

Debido a que el personal de la empresa no cuenta con los conocimientos necesarios para realizar este tipo de tareas, es preciso llevar a cabo sesiones de capacitación dirigida al personal selecto de la empresa, con la finalidad de proporcionar el conocimiento necesario para mantener una Honeynet Virtual.

3.1.4.3. Factibilidad económica

La información representa uno de los activos más valiosos de la empresa, por ser una fuente para generar conocimiento que es propio de la organización y tener el control más eficiente y eficaz del movimiento del negocio, para luego proyectar un mejor desempeño financiero. El

hecho de ser propio, implica que no puede ser compartido de manera pública sin conocimiento de la organización.

Al proponer una solución que incluya la utilización de una herramienta de software que permita virtualizar los tres equipos de computación requeridos, además de contar con un equipo proporcionado para esta finalidad, se reduce enormemente los costos que involucrarían implementar la solución propuesta. Por otra parte debido a que la mayoría del software a utilizar es completamente gratuito, representa un gasto económico mínimo para la empresa, frente a los beneficios que se obtendrán tras la implementación de la propuesta.

Dentro de la factibilidad económica del sistemas solo fue considerado el aspecto referido al software:

CARACTERÍSTICAS DE SOFTWARE

DESCRIPCIÓN	**COSTO**
VMware Workstation 6	150$
Linux – Debian	0
CD-ROM Honeywall	0
Sebek	0
Nephentes	0
SUBTOTAL	150$

Tabla 3.6 Especificación de software requerido
Fuente Elaboración propia

RESUMEN DE COSTOS DE HARWARE Y SOFTWARE

HARDWARE	0$
SOFTWARE	150$
TOTAL	**150$**

Tabla 3.7 Resumen de costos en hardware y software
Fuente Elaboración propia

Monto accesible para la empresa por lo que no es necesario adquirir algún tipo de préstamo. Este proyecto, plantea asegurar la información, con la adaptabilidad ante sucesos que incidan a la seguridad de la red, lo que implica un ahorro económico ante la eventualidad pérdida de datos, por la ausencia de herramientas de seguridad en la red.

3.2. Propuesta de solución

Una solución viable para resguardar la integridad de la infraestructura de la red de datos de la Empresa Minera SOMINEX SRL., es la herramienta denominada Honeynet, la cual recoge información sobre los atacantes y permite tomar medidas de protección para los sistemas importantes a un bajo costo, resultando ser una herramienta ideal para ser desarrollada e implementada.

En principio se describen las alternativas que existen en el mercado a la hora de diseñar una Honeynet, se discuten cuales son las principales ventajas e inconvenientes que plantea cada producto, y en qué tipo de entornos es más recomendable su implementación. Para luego describir el proceso de diseño e implementación de una Honeynet utilizando el software Honeywall. El diseño contempla la configuración de una red virtual, a partir de la cual se explican las posibilidades que ofrece la aplicación.

Se implementará una Honeynet de tercera generación, por ser la generación más segura, estable y se encuentra en vigencia como herramienta de análisis forense. Para elegir el tipo de Honeynet de tercera generación que se va a implementar se tiene dos tipos como se menciona en el Capítulo 2.

a) Implementación de una Honeynet con los mismos requerimientos de hardware que una red de computadores de producción, en la cual todos sus equipos son físicos y reales, nada es emulado o virtualizado.

b) Implementación de una Honeynet Virtual, virtualizando sistemas operativos o servicios en uno o varios equipos, se debe buscar la manera de disminuir los requerimientos de hardware y los costos sin comprometer la calidad de la solución.

En base a el análisis de los tipos de Honeynet descritos en el Capítulo 2, en el que se mostraron las ventajas y desventajas de usar soluciones de virtualización para el desarrollo de las Honeynet, y considerando que ninguna de las desventajas atentan con la calidad de la solución, ya que todas son a nivel de seguridad y pueden ser controladas con un mantenimiento periódico de la Honeynet, se ha decido usar la Honeynet Virtual, que será implementada utilizando el software comercial de virtualización VMware, que es un programa con un excelente entorno de desarrollo para tecnologías Honeynet.

Dentro de las Honeynet Virtuales se tiene dos opciones para elegir:

a) Honeynet Virtual Autocontenida.
b) Honeynet Virtual Híbrida.

Para poder elegir se debe considerar que las diferencias principales entre ambas Honeynets virtuales son el número de equipos que usan, la portabilidad y la facilidad en la administración, tal como se mostró en el Capítulo 2. Dado que ambas cumplen con los requerimientos de la solución, pero el equipo con el que se cuenta tanto en características como en cantidad, se ajusta para la implementación, se decidió optar por la segunda opción la Honeynet Virtual Autocontenida ver Figura 3.7.

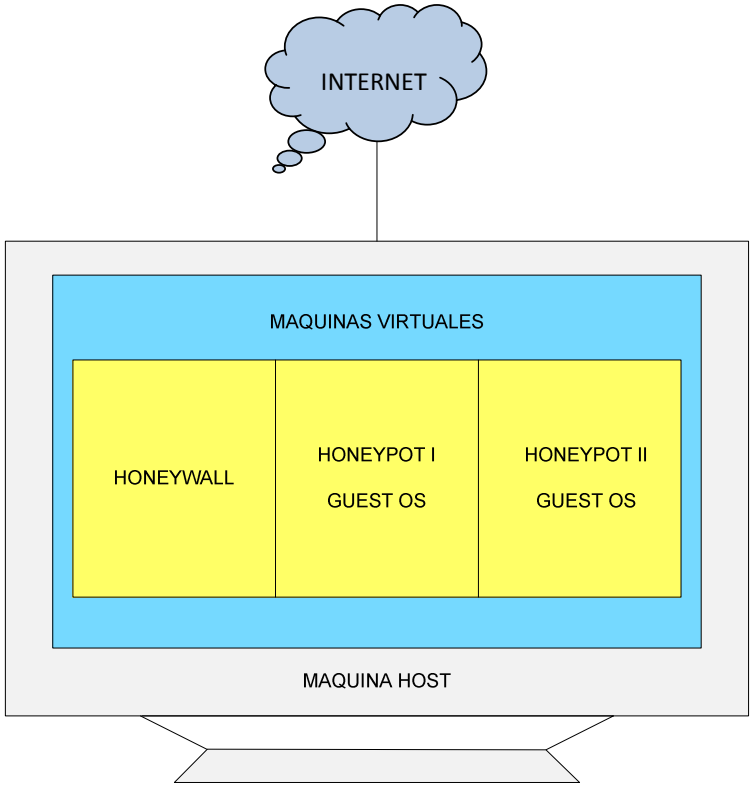


Figura 3.7 Honeynet Virtual Autocontenida

Fuente Elaboración propia

3.2.1. Modelo de red propuesto

La Honeynet propuesta, está formada por un conjunto de equipos vulnerables, los cuales consisten de dos honeypots, y una Honeywall que es el principal componente de la red, encargado del control y captura de datos, la Figura 3.8 muestra el diseño general de la Honeynet Virtual Autocontenida, en el cual se puede observar a la red Honeynet conectada y funcionando dentro de la misma red de producción, en la que solamente es necesario una máquina física que levantará como máquinas virtuales a todos los elementos que conforman la Honeynet.

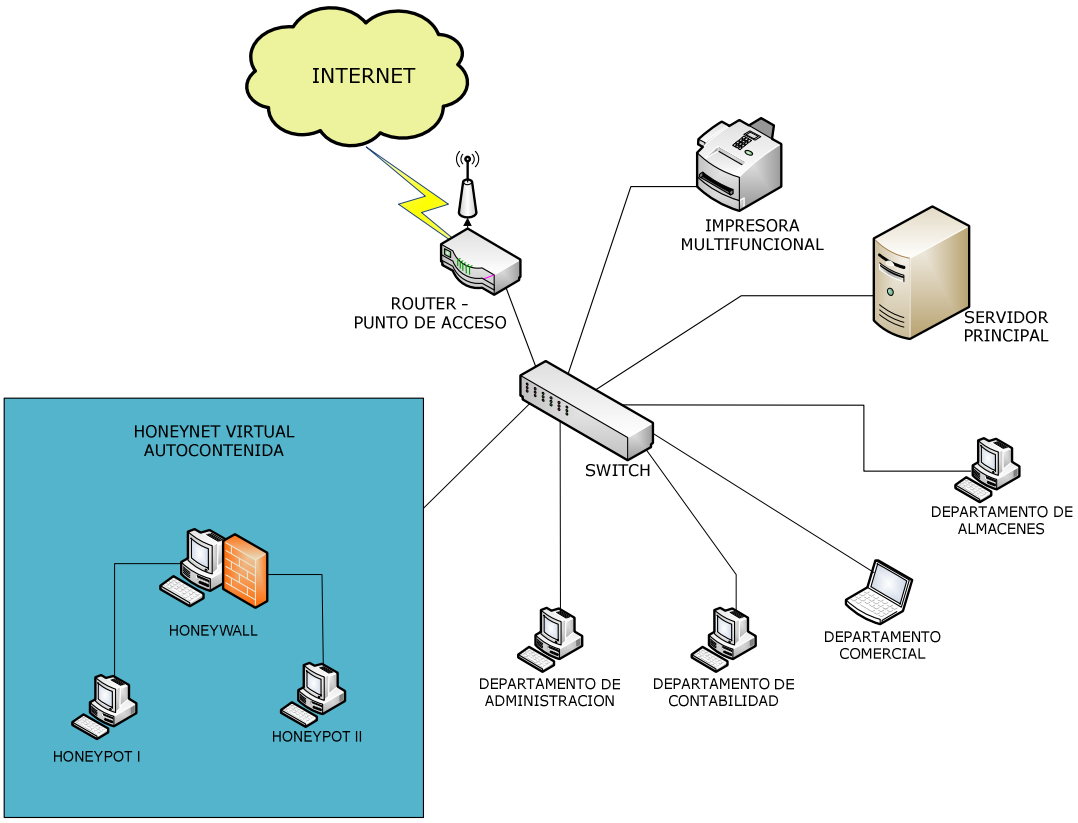


Figura 3.8 Modelo de red propuesto para la Empresa Minera SOMINEX SRL.
Fuente Elaboración propia

La Figura 3.8, muestra la máquina física que usa una aplicación de virtualización para levantar tres máquinas virtuales, una corresponde al Honeywall, las dos siguientes son Honeypots que usan los sistemas operativos Windows XP y Debian 4.0., que serán configurados con los requerimientos de hardware que se detallan en la Tabla 3.8

Sistema Operativo(s)	Disco Duro (s)	Memoria (s)
Windows XP	30 GB	512 MB
Debian 4.0	30 GB	512 MB
Honeywall (Roo V1.4)	100 GB	256 MB

Tabla 3.8 Sistemas operativos configurados en la Honeynet Virtual Autocontenida
Fuente Elaboración propia

El diagrama de red de la Figura 3.9, muestra la Honeynet de la Empresa Minera SOMINEX SRL. , con sus componentes físicos y virtuales necesarios. Una sola máquina física se

encuentra conectada directamente al switch junto a la red de producción, esta máquina cuenta, con una distribución de Windows 7 y un software virtualización VMware Workstation 6 utilizado para levantar 3 máquinas virtuales usadas dentro de esta Honeynet. La máquina virtual Honeywall utiliza dos interfaces virtuales de red: una en modo bridge y otra en modo host-only, los Honeypots utilizan cada uno una interfaz de red en modo host-only, los mismos se conectan por medio del Honeywall a la red externa, al usar el modo host-only se obliga a crear una red entre el Honeywall y los Honeypots permitiendo el paso de los paquetes a través del Honeywall, si se usara el modo bridge para las interfaces de red de los Honeypots I y II, estos estarían de igual forma conectados hacia la red externa pero sus paquetes no serían registrados ni atravesarían el Honeywall.

El modo host-only permite interconectar máquinas virtuales entre sí, así como también el sistema que las contiene, creando una red privada interna aislada del resto de la red externa. El modo bridge se asocia una interfaz física de red del sistema host por la cual las máquinas virtuales utilizan su propia IP y les permite acceder y pertenecer al mismo segmento de red a la cual está conectada la máquina que la contiene.

La arquitectura y la configuración de la red se encuentra detallada en la Figura 3.9 que muestra una máquina física (Host) junto a la red de producción conectada directamente al switch, la cual albergará a las máquinas virtuales Honeypots I y II y también el Honeywall.

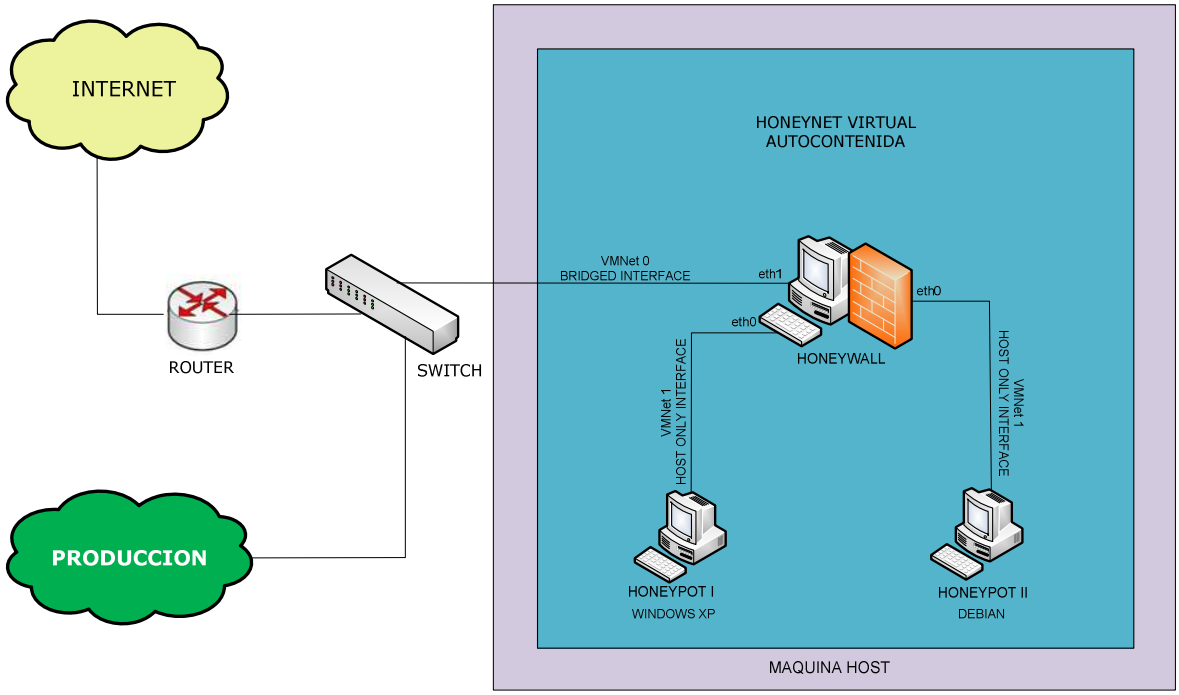


Figura 3.9 Honeynet Virtual Autocontenida en la red de la Empresa Minera SOMINEX SRL.

Fuente Elaboración propia

En la siguiente Tabla 3.9, se detalla la configuración de red utilizada para ambos Honeypots I y II, tanto en Windows XP y Debian 4.0

	Honeypot I	**Honeypot II**
Sistema Operativo	Windows XP	Debian 4.0
Dirección IP	192.168.174.131	192.168.174.130
Netmask	255.255.255.0	255.255.255.0
Network	192.168.174.0	192.168.174.0
Broadcast	192.168.174.255	192.168.174.255
Gateway	192.168.172.1	192.168.172.1

Tabla 3.9 Configuración de red de la Empresa Minera SOMINEX SRL.

Fuente Elaboración propia

Con esta configuración, se da paso a la instalación y configuración de los componentes que forman parte de solución planteada, dicha instalación y configuración será detallada y explicada en el siguiente capítulo.

3.2.2. Herramientas a ser utilizadas

3.2.2.1. Software para virtualización

La estación VMware es una opción de virtualización muy usada y establecida, está diseñada para el usuario de escritorio y disponible para plataformas Linux y Windows. Las ventajas de usar la Estación VMware como una Honeynet Virtual son:

- Amplia gama de sistemas operativos soportados, donde se puede ejecutar una gran variedad de sistemas operativos dentro del entorno virtual llamado GuestOS, incluyendo Linux, Solaris, Windows y FreeBSD.
- Opciones de red, la estación provee dos formas de manejar las redes. La primera es en modo puente (bridge), que es útil para redes de Honeynet Virtuales Híbridas porque permite a un Honeypot usar la tarjeta del computador y parecer ser otra máquina en la red Honeynet. La segunda opción es redes sólo en la máquina, esto es bueno para Honeynet Virtuales Auto-Contenidas porque se puede controlar mejor el tráfico con un cortafuegos.
- La estación VMware crea una imagen de cada Sistema Operativo Guest, estas imágenes son simplemente unos archivos, lo que la hace muy movible. Esto significa que se puede tranferir a otros computadores. Para restaurar un Honeypot a su estado original, se puede simplemente copiar una copia de seguridad en su lugar.
- Fácil de usar, la estación VMware viene con una interfaz gráfica en Windows y en Linux que hace que sea muy simple instalar, configurar y ejecutar los sistemas operativos.
- Es un producto comercial, debido a eso la estación VMware viene con soporte, actualizaciones, y parches.

3.2.2.2. Honeywall CD-ROM

El Honeywall CD-ROM ROO es un CD que contiene todas las herramientas necesarias para crear y administrar un Honeywall de tercera generación. Actualmente es un CD auto ejecutable que está en su versión 1.4, basado en la distribución de Linux Centos que instala las herramientas necesarias para levantar y administrar el Honeywall y desde su última versión incluye una herramienta de análisis de datos.

- **Componentes del Honeywall CD-ROM**

A continuación se detallan los componentes del Honeywall en la Tabla 3.10:

Componentes	**Descripción**
Snort	Sistema de detección de intrusos basado en reglas, capaz de realizar el análisis del tráfico de la red en tiempo real y también registrar paquetes de redes IP.
Snort_inline	Es una versión modificada del Snort que toma decisiones sobre el tráfico saliente siempre y cuando tenga ataques conocidos.
Session Limit	Control de límite de sesiones.
Sebek	Es una herramienta de captura de datos diseñada para capturar al atacante sobre las actividades de un Honeypot.
Walleye	Proporciona al administrador herramientas de análisis de datos de manera remota. Los administradores pueden acceder a todos los datos capturados por snort-inline y Sebek, estos datos incluyen la dirección IP, datos

	transferidos y acciones de los atacantes en los Honeypots. Walleye se ejecuta sobre un servidor web (apache) también instalado con la distribución de ROO.
Pcap	Interfaz de captura de datos del kernel de Linux.
Iptables	Firewall de Linux integrado en el kernel, usado para limitar los paquetes en el control de datos y para registrar los datos en la captura de datos.
Swatch	Es una herramienta que comunica al administrador por medio de un correo electrónico tan pronto como sucede un incidente.
Argus + Hflow	Información de flujos de tráfico y relaciones.
Menú	Una interfaz gráfica usada para mantenimiento y control de la Honeynet

Tabla 3.10 Componentes del CD-ROM roo V1.4

Fuente Elaboración propia

3.2.2.3. Sebek

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

3.2.2.4. Nepenthes

Nepenthes es una solución de Honeypot virtual de baja interacción que tiene la característica de recolectar malware de forma automática. Trabaja emulando vulnerabilidades en servicios de red. A diferencia de un Hoynepot normal que levanta los servicios de red, Nepenthes los emula, de esta forma reduce el riesgo en un Honeypot de ser comprometido. Como el proceso de ataque es una emulación, es más efectivo en el tipo de ataques autonómicos. La finalidad del Nepenthes es recoger y descargar la herramienta usada para ejecutar el ataque, principalmente gusanos, que luego servirán para un mejor análisis del mismo. De esta forma tenemos un Honeypot recolectando malwares para Windows sin ser comprometido en el proceso.

3.2.3. Establecimiento de políticas de seguridad

El establecimiento de políticas y/o mecanismos de seguridad no son otra cosa que una cultura y educación que se deben adquirir para evitar problemas futuros en usos de equipos y sistemas. Hoy en día es tan común que se utilicen computadoras, cajeros automáticos, tecnologías de comunicaciones, redes e Internet, que no se cae en la cuenta de toda la que la información que manejamos, nuestra propia información, correos electrónicos, información a través de chat, datos bancarios, archivos de interés y todo nuestro trabajo cotidiano se encuentra precisamente manejado por computadoras y equipo que son vulnerables y que en un abrir y cerrar de ojos pueden sufrir de una ataque, alteraciones o descomposturas.

La seguridad en un equipo, nodo o computadora: Uno de los primero puntos a cubrir son las claves de acceso, no se deben usar claves que en su constitución son muy comunes, como es el caso de las iniciales del nombre propio y la fecha de nacimiento, apodos o sobrenombres que todo mundo conoce, o constituirlas de solo letras o solo números; estos tipos de claves son en las que los intrusos, hackers y ladrones buscan de primera mano; se tienen que realizar combinaciones de letras mayúsculas, minúsculas y números alternadamente. No se tiene que compartir las claves, es común que cuando alguien más necesita usar algunos equipos, computadoras y sistemas los usuarios dan a conocer sus claves de uso y muchas veces hasta en voz alta, enfrente de muchas personas que no son parte de la empresa. Hay que cambiar

periódicamente las claves de acceso, los equipos o computadoras que se encuentran más expuestos, tienen que tener un cambio más recurrente.

En cada nodo y servidor se tiene que usar antivirus, actualizado o configurado para que automáticamente integre las nuevas actualizaciones del propio software y de las definiciones o bases de datos de virus registrados.

Si los equipos, computadoras o servidores tienen niveles de permisos de uso de archivos y de recursos, se tienen que configurar de acuerdo a los requerimientos de la empresa o usuario, y no usar la configuración predeterminada que viene de fábrica, así como nombres y usuarios. Los intrusos, ladrones y hackers conocen muy bien las configuraciones predeterminadas y son las que usan al momento de realizar un ataque.

En computadoras que utilicen sistemas operativos de Microsoft, se tienen que realizar actualizaciones periódicamente, ya que constantemente los hacker y creadores de virus encuentran vulnerabilidades en dichos sistemas operativos. También, se tienen que utilizar programas que detecten y remuevan "spywares" (programas o aplicaciones que recopilan información sobre una persona u organización sin su conocimiento), existen diferente softwares que realizan esta tarea, algunos son gratuitos y trabajan muy bien; así la recomendación es contar con uno de ellos y realizar un escaneo periódico de el equipo o computadora.

La seguridad administrativa: Esta se basa en políticas y normas que se deben de implantar y seguir. Las políticas proporcionan las reglas que gobiernan el cómo deberían ser configurados los sistemas, también cómo deberían actuar los empleados de una organización en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales. Define lo que debería de ser la seguridad dentro de la organización y pone a todos en la misma situación, de modo que todo el mundo entienda lo que se espera de ellos.

Toda política debe de tener un propósito y procedimiento bien específico que articule claramente por qué fueron creadas tales políticas o procedimientos y qué beneficios espera la organización derivada de las mismas.

Entendido lo anterior, es necesario establecer políticas de seguridad que deberán basarse en los siguientes aspectos:

- Identificar y seleccionar lo que se debe proteger (información sensible)
- Establecer niveles de prioridad e importancia sobre esta información
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla.
- Implementar respuesta a incidentes y recuperación para disminuir el impacto.

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente se habrá identificado y definido los sistemas y datos a proteger.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Es así que se propone las siguientes políticas básicas de seguridad:

- Aplicar buenos procedimientos de administración de contraseña.
- Asegurarse de que todos los usuarios tengan una contraseña que se amolda a la directiva organizacional.
- Forzar un cambio de contraseña cada 30 días para cuentas privilegiadas y cada 60 días para usuarios normales.
- Implementar un tamaño de contraseña mínimo de ocho caracteres que contenga, por lo menos, un carácter alfanumérico, uno numérico y uno no alfabético.
- Registrar fallas múltiples de autentificación.

- Configurar servicios para desconectar clientes después de tres intentos de inicio de sesión no válidos.
- Implementar bloqueo de cuentas donde sea posible. Esté al pendiente de posibles problemas de negación del servicio de cuentas bloqueadas intencionalmente por un atacante.
- Deshabilitar servicios que no están en uso.
- Implementar herramientas de composición de contraseñas que prohíban al usuario seleccionar una mala contraseña.
- No use la misma contraseña para cada sistema en que inicie sesión.
- No escribir su contraseña.
- No decir su contraseña a otros.
- Use las contraseñas de una sola vez cuando sea posible.
- Asegúrarse de que las cuentas predeterminadas como "setup" y "admin" no tengan contraseñas predeterminadas.

CAPITULO IV

RESULTADOS

4.1. Configuración de la Honeynet Virtual

4.1.1 Instalación y configuración de las maquinas virtuales

El software de virtualización que se utilizo para la creación de las máquinas virtuales es VMware Workstation 6, el cual debe estar instalado y configurado correctamente dentro de la computadora que levantará las máquinas virtuales.

Como primer paso se creó la máquina virtual Honeywall la misma será configurada con los requerimientos de hardware (memoria y disco) establecidos en la Tabla 3.9, es necesario cambiar el tipo el disco duro virtual a IDE caso contrario no será soportado por el sistema que se va a instalar el cual está basado en Centos. Posteriormente se agregará dos tarjetas de red adicionales de tal manera que eth1 esté en modo bridge y eth0 en modo host-only, tal como se muestra la Figura 4.1

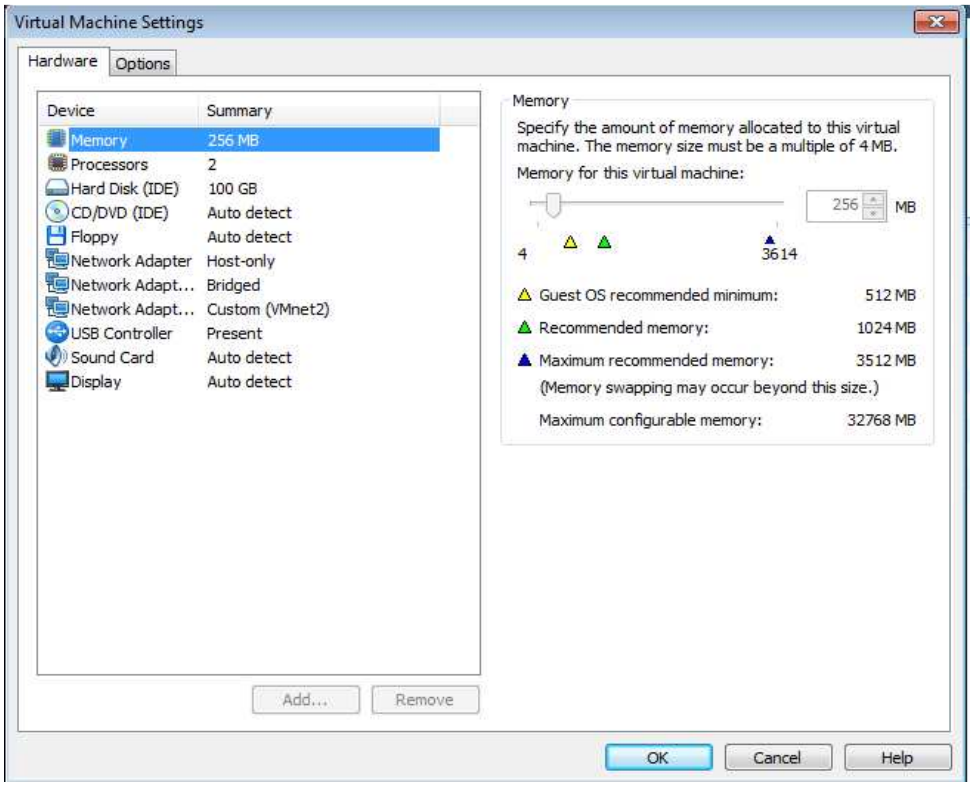


Figura 4.1 Configuración de la Honeywall, en la aplicación VMware

Fuente: Imagen obtenida de la configuración del Honeywall

Una guía más detallada sobre la creación y configuración de máquinas virtuales usando VMware Workstation se encuentra en el Anexo 3.

4.1.2 Instalación y configuración del Honeywall

La versión del Honeywall que se utilizo es V1.4, la cual se puede descargar desde el sitio web www.honeynet.org, se levanto la máquina virtual y se booteo la imagen del disco CDROM Roo previamente descargado, con esto se inicia el proceso de instalación automático, después de que la instalación esté completa el sistema se reiniciará iniciando el sistema desde el CD-ROM. El Honeywall viene con dos cuentas de sistemas por defecto: roo y root, las cuales comparten el mismo password honey, que pueden ser cambiados en cualquier momento.

Para poder iniciar en el sistema se debe ingresar con el usuario roo, pero para iniciar la configuración es necesario utilizar la cuenta root con el comando su-, con el comando menú

ingresamos al panel de administración del Honeywall, desde el cual podemos configurar parámetros como: información sobre la red, datos de los Honeypots. Para un mayor detalle en la configuración y administración del Roo, revisar la guía de configuración que se encuentra en el Anexo 4.

4.1.3 Instalación y configuración de los Honeypots

Se instalaron dos máquinas virtuales que corresponden a los Honeypots I y II, usando los sistemas operativos Windows XP y Debian 4.0, además las tarjetas de red se debe configurar en modo host-only para cada Honeypot.

4.1.3.1 Configuración del Honeypot I

Una vez instalado el sistema Operativo Windows XP se procedió a la configuración correspondiente de la interfaz de red.

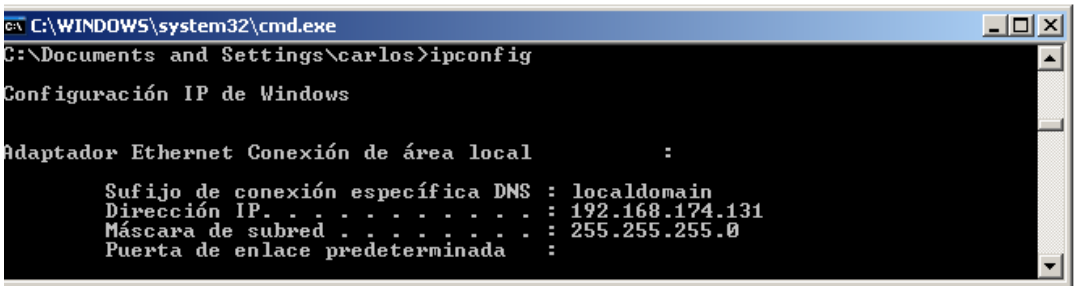


Figura 4.2 Configuración del Honeypot I Windows XP

Fuente: Imagen obtenida de la configuración de red del Honeypot I

Los servicios disponibles en esta Honepot serán: TELNET, FTP, HTTP, MYSQL, para los cuales se escogió una herramienta de fácil instalación llamada XAMPP 1.5 que contiende Apache 2.2.3, MYSQL 5.0.27, Filezila 0.9.20 XAMPP está diseñado para ser una herramienta de desarrollo y no de producción debido a que contiene problemas en la seguridad tales como:

- El usuario root de MYSQL no tiene password

- El demonio MYSQL es accesible vía red
- phpMyAdmin es accesible vía red.
- Los ejemplos incluidos son accesibles vía red
- Los usuarios del Filezila Server son públicos y conocidos.

Estos paquetes de software individuales son seguros pero debido a la mala configuración cuando se los instala con una herramienta como XAMPP el sistema entero ser vuelve vulnerable a ataques. Este error es cometido muy frecuentemente por administradores de red, por este motivo se decidió usarla para analizar sus defectos.

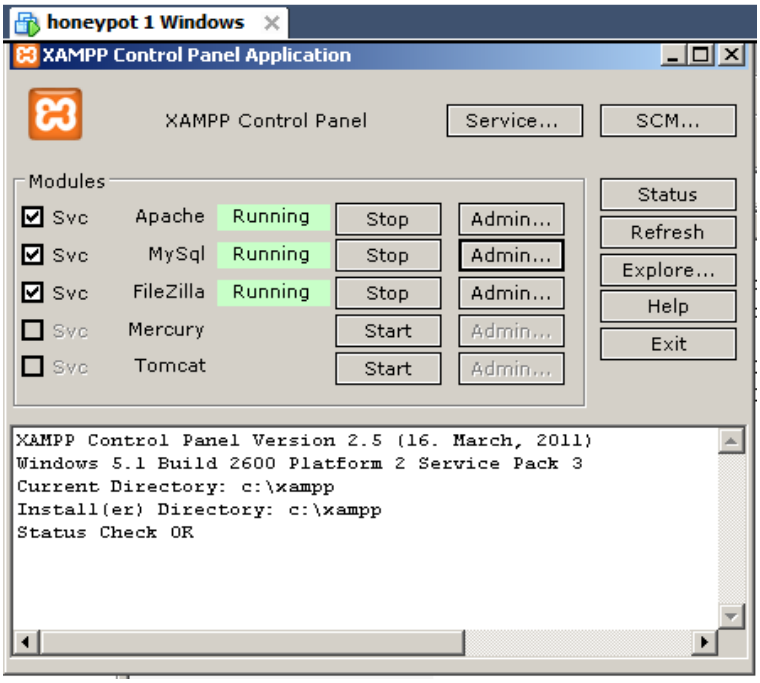


Figura 4.3 Configuración de los servicios en el Honeypot I Windows XP
Fuente: Imagen obtenida de la configuración de servicios del Honeypot I

Finalmente es necesario instalar la herramienta de captura Sebek Client, la cual será detallada a continuación:

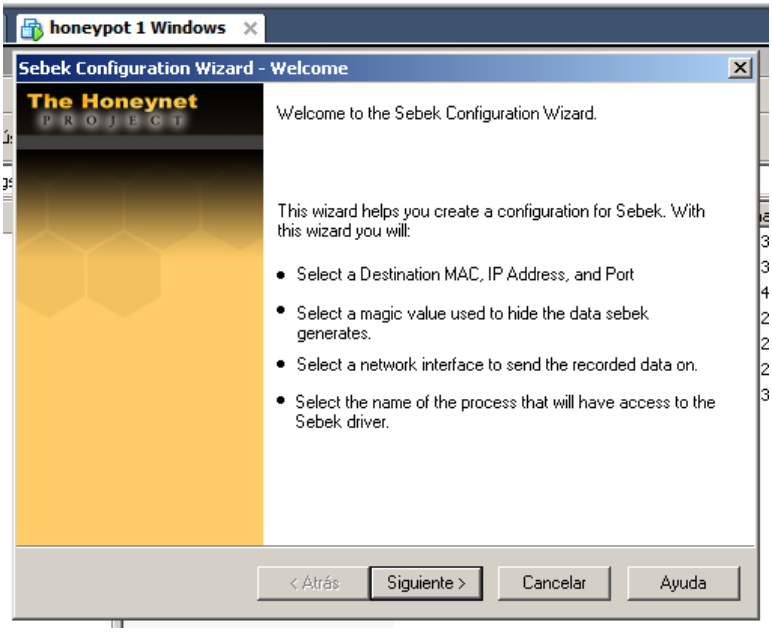


Figura 4.4 Instalación de Sebek Client en el Honeypot I Windows XP

Fuente: Imagen obtenida de la instalación de Sebek Client del Honeypot I

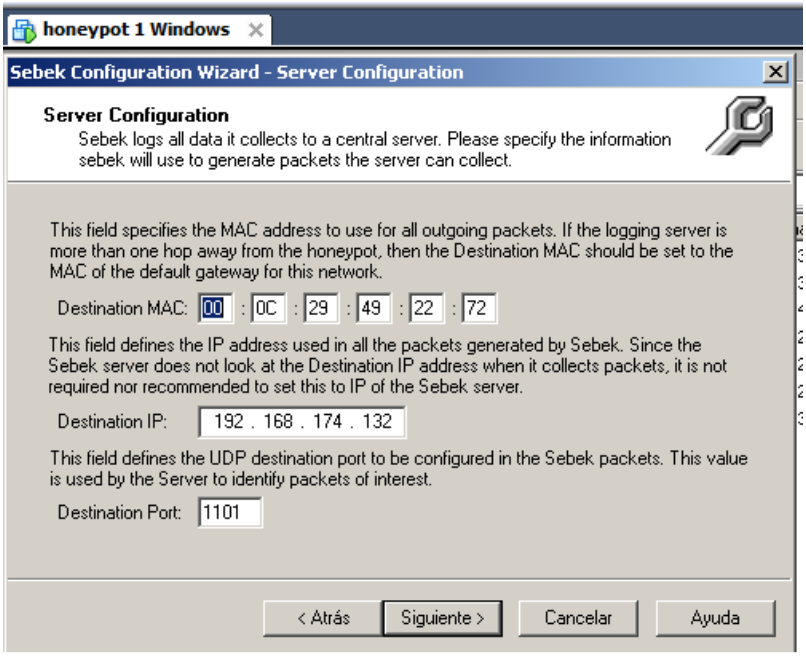


Figura 4.5 Configuración de Sebek Client en el Honeypot I Windows XP

Fuente: Imagen obtenida de la configuración de Sebek Client del Honeypot I

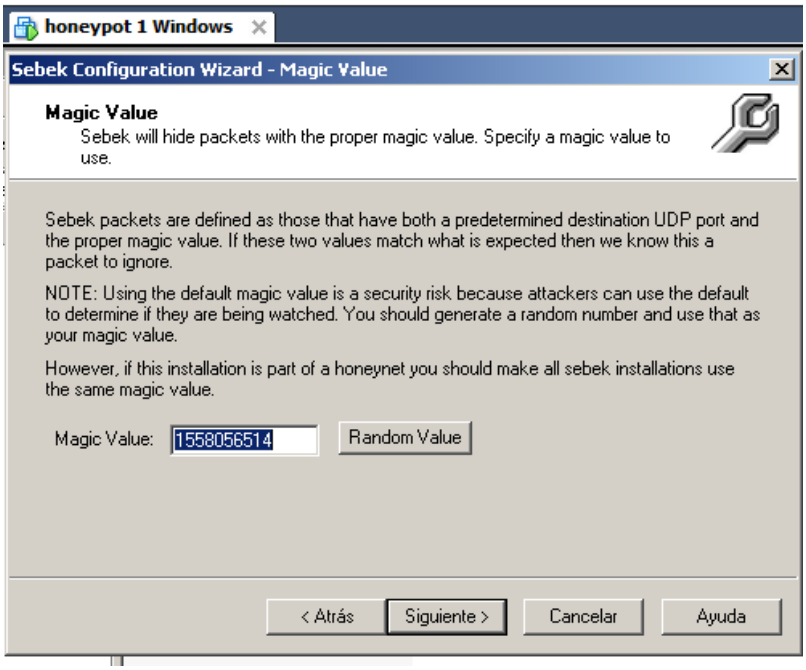


Figura 4.6 Configuración de magic value en el Honeypot I Windows XP

Fuente: Imagen obtenida de la configuración de Sebek Client del Honeypot I

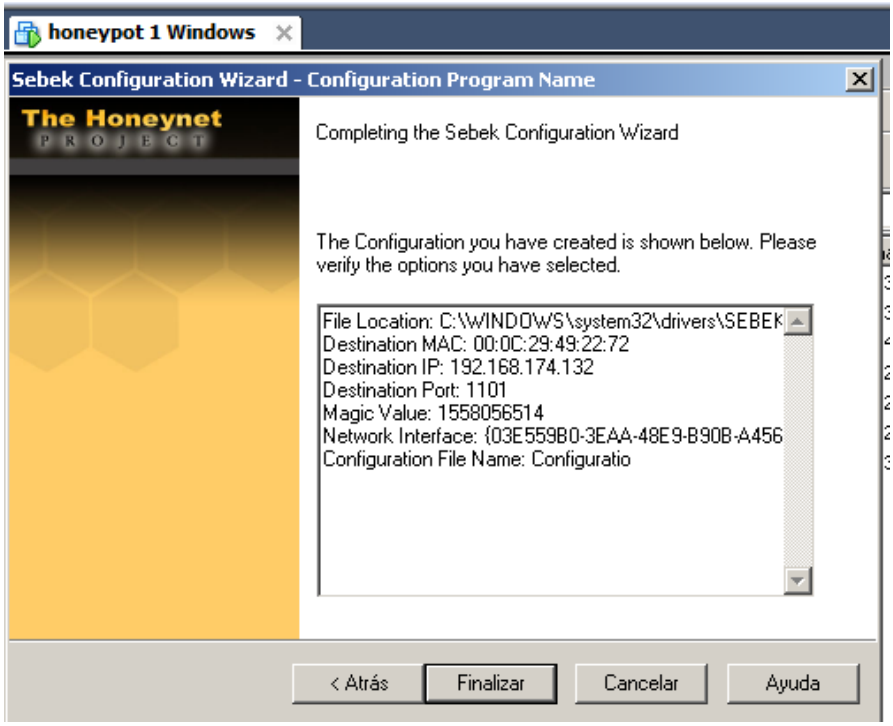


Figura 4.7 Resumen de la configuración del Sebek Clien en el Honeypot I Windows XP

Fuente: Imagen obtenida de la configuración de Sebek Client del Honeypot I

4.1.3.2 Configuración del Honeypot II

Una vez el sistema operativo instalado, procedemos a la configuración correspondiente de la interfaz de red.

Este Honeypot no usará sus servicios como recursos de red ya que se instalará una herramienta de captura llamada Nepenthes que simula los servicios de red y vulnerabilidades como se explicó anteriormente.

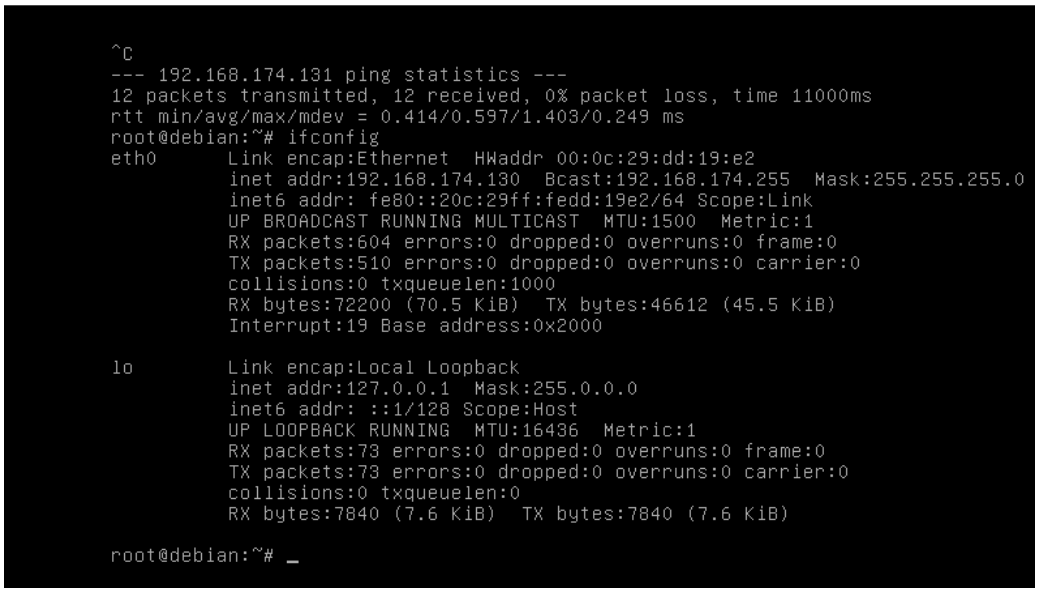


Figura 4.8 Configuración de red en el Honeypot II Debian
Fuente: Imagen obtenida de la configuración de red del Honeypot II

4.2 Resultados obtenidos durante la configuración de la Honeynet Virtual

Una vez implementada la Honeynet se deben hacer las pruebas de funcionamiento para ver si los host emulados están funcionando correctamente, para ello nos basaremos en las herramientas más comunes de red.

En una primera instancia los Honeypots deben poder establecer conexiones entrantes y salientes a la red interna mediante el uso de las peticiones de eco (Packet Internet Groper – Rastreador de Paquetes Internet), se realiza esta prueba con el propósito de que los Honeypots accedan en ambas direcciones a la red interna.

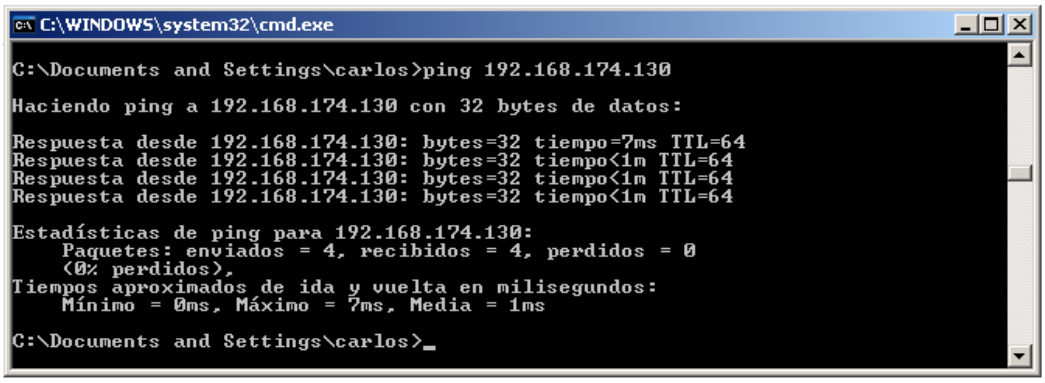


Figura 4.9 Ping Honeypot I al Honeypot II

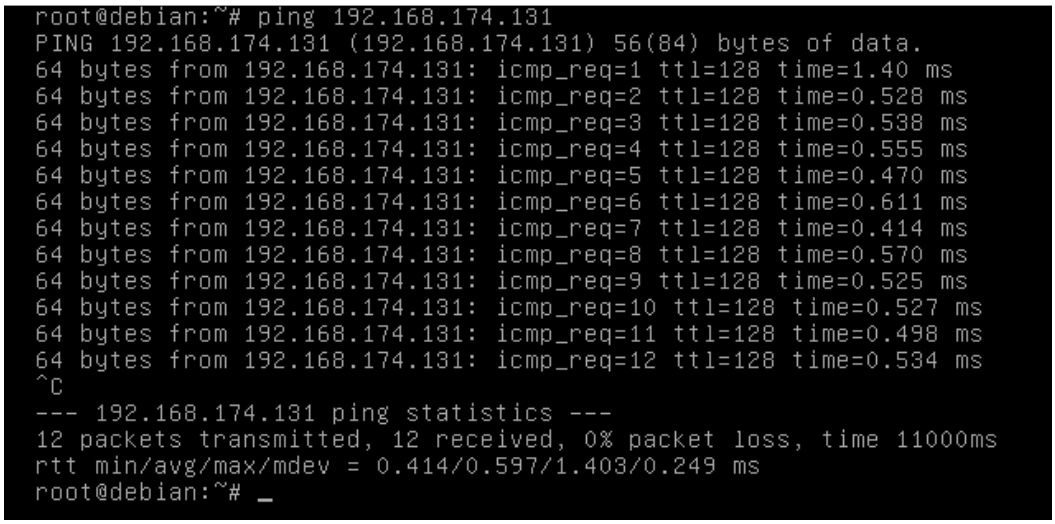


Figura 4.10 Ping Honeypot II al Honeypot I

Por otra parte, los Honeypots deben poder establecer conexiones entrantes y salientes a la red externa usando el protocolo IP, se realiza esta prueba con la finalidad de que los Honeypots accedan en ambas direcciones a la red externa.

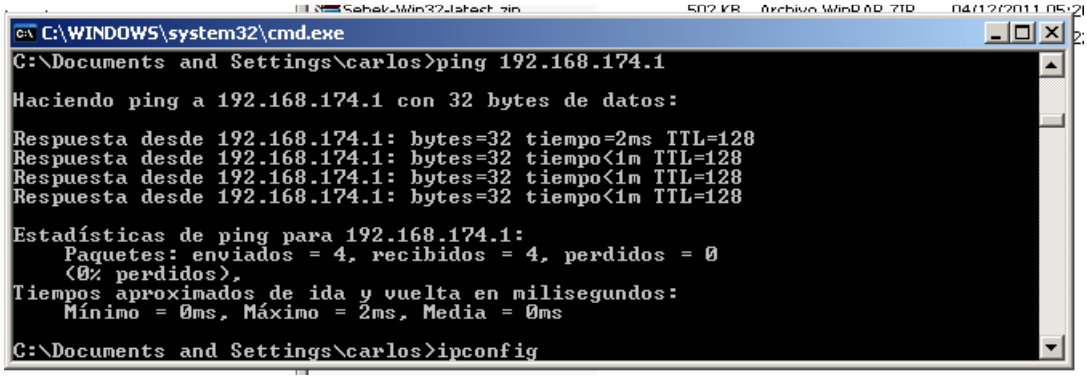


Figura 4.11 Ping Honeypot I a la maquina externa

Por último es necesario verificar que el Honeywall este registrando el tráfico, ya que el Honeywall puede no estar levantando Snort, para hacerlo es necesario ir al menú y seleccionar "Recargar Honeywall", para realizar la verificación de la Honeywall, se tiene que ingresar al Honeywall como root, se seleccionar en el Menu, Status, Inbount Connections/Onbout Connections, luego comprobar las entradas con el protocolo ICMP correspondientes a los Ping realizados en pruebas anteriores.

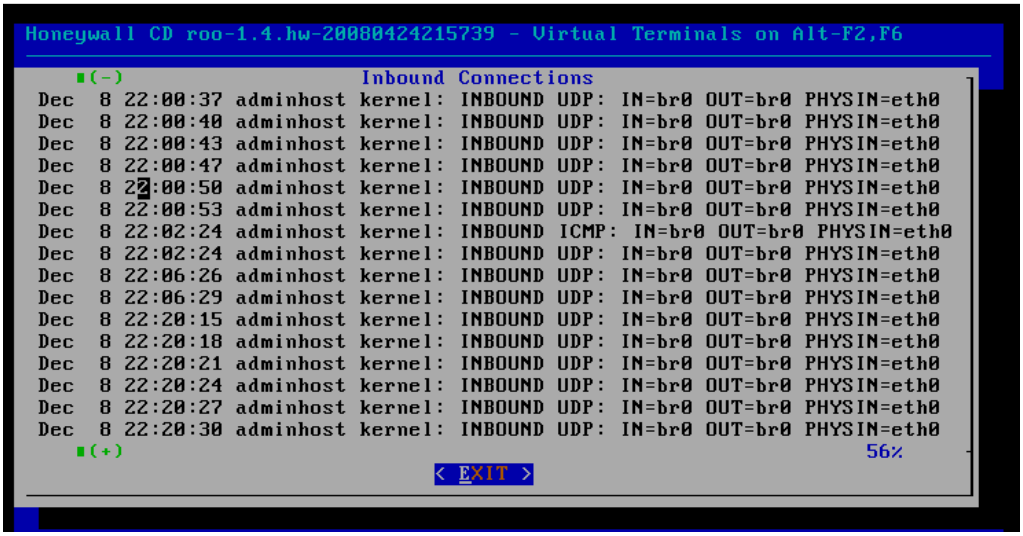


Figura 4.12 Conexiones registradas en el Honeywall

La instalación que se ha presentado en este trabajo puede personalizarse en muchos aspectos: como el establecimiento de configuraciones de red más complejas, cambiar parámetros adicionales de los equipos virtuales o de su ubicación en la red.

4.2.1 Procedimiento que usan los atacantes para comprometer un sistema

Gracias a la implementación de la Honeynet Virtual en la red de datos de la Empresa Minera SOMINEX SRL., se pudieron determinar los procedimientos que usan los atacantes para comprometer un sistema, aclarando que estos procedimientos pueden variar de acuerdo a la herramienta de seguridad, arquitectura, tipo de empresa en la que se esté trabajando y sobre todo, el tipo de atacante.

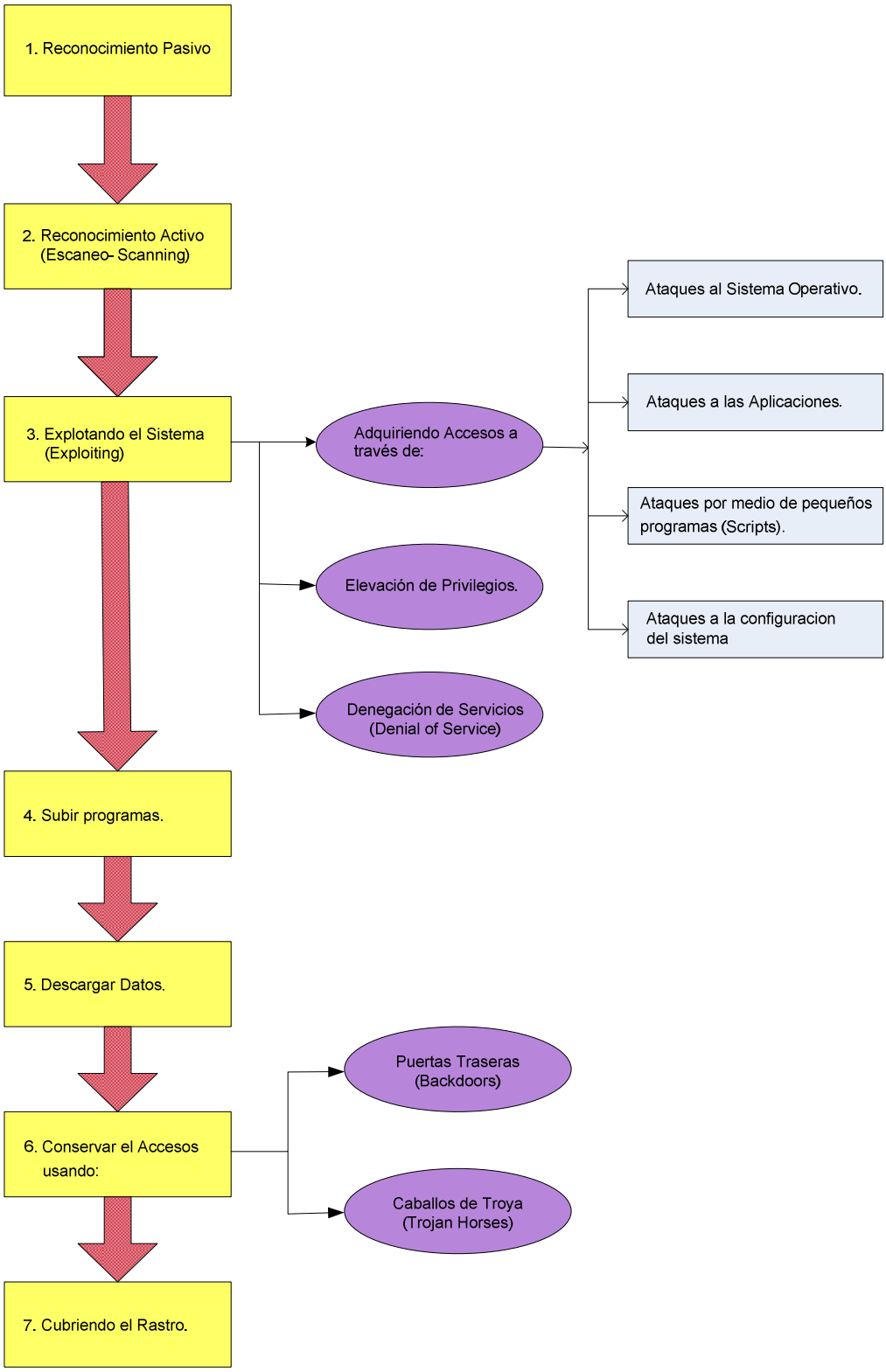


Figura 4.13 Procedimientos utilizados por un atacante

Fuente: Elaboración propia

- **Reconocimiento pasivo**

Para violar un sistema, un atacante debe tener cierta información de carácter general; si no, él no sabe qué atacara. La reunión pasiva de la información no es siempre útil por sí mismo, sino que es paso de progresión necesario, porque sabe que la información es necesaria de antemano para realizar otros pasos de progresión.

- **Reconocimiento activo**

A este punto, un atacante tiene bastante información para intentar hacer un reconocimiento o una exploración contra un sitio, el atacante prueba el sistema para encontrar información adicional. Algunas de las cosas que el atacante puede descubrir son: Computadores que son accesibles, ubicación y reconocimiento de switches (segmentadores), routers (enrutadores), firewalls (cortafuegos) y hubs, sistemas operativos que se corren sobre los equipos, puertos que están abiertos, servicios que están corriendo, versiones de aplicaciones que están corriendo, etc.

- **Explotando el sistema**

Mucha gente piensa que explotar el sistema es obtener acceso, pero actualmente se trabaja en dos áreas adicionales: La elevación de privilegios y la denegación de servicios. Los tres son útiles al atacante dependiendo del tipo de ataque que él desea lanzar.
Es importante observar que un atacante puede utilizar un sistema de una red para atacar a otra red.

- **Adquiriendo acceso**

Esta es una de las maneras más populares de explotar un sistema. Son varias maneras que un atacante puede acceder a un sistema, pero en el nivel fundamental, él debe aprovecharse de un cierto aspecto de una entidad. Esa entidad es generalmente un sistema operativo o una aplicación; pero si estamos incluyendo vulnerabilidades físicas de la seguridad, podría ser

una debilidad en la construcción del sistema como tal, esto puede proporcionar debilidades que puedan ser comprometidas. La clave es reducir al mínimo esas debilidades para proporcionar un ambiente seguro.

Los siguientes son algunas maneras que un atacante puede acceder a un sistema:

- *Ataques al sistema operativo*; La instalación por defecto de un sistema operativo, deja muchos servicios corriendo y puertos abiertos. La razón por la que la mayoría de los fabricantes hacen esto es simple, dinero.
- *Ataques a las aplicaciones*; Los ataques del nivel de la aplicación se aprovechan de la poca seguridad que encuentra hoy a nivel lógico del software. El ciclo de desarrollo de programación para muchas aplicaciones es demasiado corto sin tener en cuenta para nada su seguridad. Un problema importante con la mayoría del software que se esté desarrollando actualmente es que los programadores y los probadores están bajo plazos muy apretados para la versión final de un producto. Para proporcionar un alto nivel de seguridad, la aplicación tiene que ser diseñada así desde el principio.
- *Ataques por medio de pequeños programas (scripts)*; Especialmente en las versiones de UNIX, los pequeños programas conocidos también con el nombre de ***"scripts"***, son responsables de una gran cantidad de entradas y de problemas de seguridad. Cuando el sistema operativo o las aplicaciones están instalados en una PC, los fabricantes distribuyen archivos y los scripts simples de modo que el propietario en el sistema pueda entender mejor cómo funciona o trabaja y puede utilizar los scripts para desarrollar nuevas aplicaciones.
- *Ataques a la configuración del sistema*; Son varios los casos, en que un sistema tiene muchos problemas de seguridad porque no fueron configurados correctamente. Son muchos los administradores que instalan un sistema con las opciones por defecto o por otra parte al tratar de instalar un nuevo programa modifica una serie de opciones hasta que logra que un producto trabaje. El problema con esto es que él nunca deshace lo que hizo o limpia el trabajo extraño realizado. Esta es una de las mayores razones del por qué cierto sistema son quebrantados y otros no. Para maximizar la configuración correcta de una máquina, se necesario quitar cualquier servicio innecesario o software.

- **Elevación de privilegios**

La última meta de un atacante es tener el "root" o el acceso del administrador en un sistema. En algunos casos, un atacante puede adquirir directamente el acceso de los servidores. En otros casos, un atacante tiene que tener un acceso con una cantidad mínima de privilegios y después elevarlos para tener acceso completo.

- **Denegación de servicios (denial of service)**

Los dos tipos principales de ataques activos son Denegación del Servicio y Ruptura Interna. Los ataques de denegación de servicios produce en un sistema el rechazo al acceso legítimo a un recurso. Estos pueden extenderse a bloquear usuarios que ingresan a través de Web Site para impedir su ingreso a la red.

- **Subir programas**

Después de que un atacante haya accesado a un sistema, él realiza generalmente un cierto conjunto de acciones sobre el servidor. Son pocos los casos donde un atacante accede apenas por el motivo de acceder. Lo más común son las cargas o descargas de archivos o programas del sistema. Si un atacante está indagando para robar la información, después de que se tenga el acceso, la meta es descargar la información lo más secretamente posible y luego salir del sistema.

- **Descargar datos**

Con algunos ataques, como espionaje corporativo, un atacante solo le interesa la información. Esta información puede ser datos de investigación y desarrollo de un nuevo producto, una lista de direcciones de clientes, o el futuro de una compañía. En todos estos casos, el atacante desea el acceso ilegal al sitio para luego hacer una trasferencia de los datos a otra localización.

- **Conservando el acceso**

Después de que un intruso ingresa al sistema, el puede colocar una puerta trasera (backdoor) para acceder fácilmente en el momento que desee. Si al atacante le cuesta mucho trabajo conseguir el acceso al sistema. La meta principal de conservar el acceso es mantener dicho acceso pero cubrir sus huellas de modo que siga siendo desapercibido.

- **Cubriendo el rastro**

Después de que un atacante compromete la seguridad de una máquina y crea una puerta trasera, lo siguiente es cerciorarse de no ser descubierto. Por tanto el atacante debe cubrir sus huellas, lo más sencillo es limpiar los registros del sistema que se generan diariamente, estos archivos contienen un expediente que indican que personas ingresaron al sistema y cuando, así que si cualquier persona que visualice el contenido de los logs puede detectar fácilmente que persona no autorizada ingreso al sistema y determinar también el trabajo realizado sobre la maquina.

CONCLUSIONES Y RECOMENDACIONES

- La herramienta Honeynet, representa una solución de bajo costo complementaria a todas las herramientas de seguridad comerciales en el mercado, permitiendo a la Empresa SOMINEX SRL. u organizaciones interesadas en proteger y resguardar de una mejor forma el activo primordial, la información.

- Con el presente diseño, se podrá realizar un mejor aseguramiento a la red de datos de la Empresa SOMINEX SRL., siendo la herramienta Honeynet Virtual, un punto de distracción de los sistemas reales ante cualquier ataque o atacante, salvaguardando la información.

- Con la implementación de la herramienta de seguridad se podrá contar con elementos para el análisis de situaciones anómalas o ataques, teniendo la información necesaria para poder evitar y realizar correcciones y/o mejoras respecto a el aseguramiento en los componentes externos para cerrar las posibles entradas que pudiese tener un atacante.

- El análisis y la implementación del Honeynet Virtual proporcionaron una visión más clara sobre la importancia en el diseño de red.

- En el proceso de recolección de información del medio en el que se desenvuelve el presente trabajo, se llego a la conclusión de que lamentablemente con la brecha tecnológica, que va reduciendo gradualmente, muy pocas son las instituciones que cuenten con políticas de seguridad reales y acordes al avance de la tecnología.

- Es importante recalcar que la herramienta de seguridad propuesta no ha sido desarrollada para sustituir a ninguna de las soluciones de seguridad existentes, su labor consiste principalmente en reducir la carga de trabajo de los responsables de seguridad.

- En cuanto a la tecnología Honeynet puede ayudar a las organizaciones a controlar las intrusiones que tienen lugar en sus redes informáticas, constituye un mecanismo de

seguridad sencilla y efectiva que puede implementarse sin necesidad de realizar cambios en la arquitectura de red o en los equipos de producción existentes.

- La revisión de sitios web, bibliografía y revistas relacionadas con Seguridad Informática permitió comprender más detalladamente el marco teórico en el que se encuentra inmerso el proyecto, a fin de identificar claramente los distintos tipos de Honeypots, el objetivo que persiguen y sus diferencias. Todo esto se ve plasmado en los capítulos II y III de este documento de Tesis.

- El impacto que implica este prototipo se puede ver reflejado en un cambio de mentalidad respecto a la seguridad informática, ya que permite ver desde un punto de vista mucho más proactivo. Esto, mejora la seguridad de la empresa ya no que no sólo se reacciona a los acontecimientos sino que se predicen ataques y se mejoran las políticas de seguridad.

- Si bien este proyecto de tesis fue diseñado como prototipo fue posible obtener conclusiones realmente importantes en cuanto a seguridad informática que permiten dar a conocer al personal de la empresa las nuevas tecnologías que se están utilizando en esta materia a nivel mundial, sentando un precedente para la realización de otros proyectos de investigación en este campo de la Informática, que es y será una parte fundamental en cualquier organización.

- Las Honeynets constituyen una tecnología con un gran potencial como técnica de seguridad, por lo que se trata de una tecnología joven, pero con muchas posibilidades, parece claro que, dentro de las muchas implementaciones que se puede encontrar, las Honeynets son las que más posibilidades ofrecen por lo cual se recomienda ampliamente su implementación e investigación no solo para fines institucionales o empresariales sino también para fines educativos.

- El potencial real de las Honeynets y los Honeypots no se alcanzará hasta que las organizaciones que instalan señuelos de este tipo no compartan la información que cada uno recoge y se realice una correlación a gran escala es por eso que es recomendable conformar grupos de estudio y análisis de estas herramientas para formar profesionales

capacitados no solo para implementar defensas inquebrantables, si no que, también sean capaces de aprender de los ataques.

- Las Honeynets no solucionarán sus problemas de seguridad, por lo que se recomienda encarecidamente que las organizaciones se centren primero en mejores prácticas como la autenticación fuerte, uso de protocolos cifrados, revisión de registros del sistema, y versiones seguras del sistema. Mediante la prioridad en políticas y procedimientos adecuados, las organizaciones pueden reducir considerablemente los riesgos.

REFERENCIAS BIBLIOGRÁFICAS

[1] BRADANOVIC, T. Conceptos Básicos de Seguridad Informática [en línea], [disponible en: http://www.bradanovic.cl/pcasual/ayuda3.html],[fecha de consulta: 8-11-2011]

[2] NANDO, Curso seguridad en sistemas de información [en línea], [disponible en: http://www.slideshare.net/nyzapersa/curso-seguridad-en-sistemas-de-informacion#], [fecha de consulta: 9-08-2011]

[3] GALLEGO, E., Honeynets: Aprendiendo del Atacante [en línea], [disponible en: http://jungla.dit.upm.es/~jlopez/publicaciones/mundointernet04.pdf], [fecha de consulta: 10-08-2011]

[4] VENTURA, Y., RODRIGUEZ, N. Diseño y desarrollo de Honeynets Virtuales utilizando Vmware para la detección de intrusos informáticos, Tesis Ingeniero en Telecomunicaciones, Universidad Francisco Gavidia, San Salvador, Marzo 2008, 193p

[5] SPITZNER, L., Honeypots: Tracking Hackers, Addison Wesley professional, 2002.

[6] HONEYNET PROJECT, Conoce a tu enemigo: Honeynets [en línea] , [disponible en: http://his.sourceforge.net/honeynet/papers/honeynet/], [fecha de consulta: 6-11-2011]

[7] CARVAJAL, A., Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático [en línea], [disponible en: http://www.acis.org.co/fileadmin/Articulos/ TecnicasAtaqueComputacionForense.pdf], [fecha de consulta: 6-11-2011]

[8] HONEYNET PROJECT, Know Your Enemy: Honeynets [en línea], [disponible en: http://old.honeynet.org/papers/honeynet/], [fecha de consulta: 6-11-2011]

BIBLIOGRAFÍA

BORGUELLO, C. Seguridad Informática sus Implicancias e Implementación, Tesis Licenciatura en Sistemas, Universidad Tecnológica Nacional, Septiembre 2001, 309p

BRADANOVIC, T. Conceptos Básicos de Seguridad Informática [en línea], [disponible en: http://www.bradanovic.cl/pcasual/ayuda3.html],[fecha de consulta: 8-11-2011]

CARVAJAL, A., Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático [en línea], [disponible en : http://www.acis.org.co/fileadmin/Articulos/ TecnicasAtaqueComputacionForense.pdf], [fecha de consulta: 6-11-2011]

FERNANDEZ, H., Detección y limitaciones de ataques clásicos con Honeynets virtuales, Tesis para la Carrera Licenciatura en Ciencias de la Computación, Universidad Nacional del Comahue, Argentina, Octubre 2009, 120p

GALLEGO, E., Honeynets: Aprendiendo del Atacante [en línea], [disponible en: http://jungla.dit.upm.es/~jlopez/publicaciones/mundointernet04.pdf], [fecha de consulta: 10-08-2011]

GONZALES, D., Sistemas de Detección de Intrusiones [en línea], [disponible en: http://dgonzalez.net/papers/ids/html/cap04.htm#_Toc44738959*]*, [fecha de consulta: 10-08-2011]

HONEYNET PROJECT, Conoce a tu enemigo: Definiendo honeynets virtuales [en línea], [disponible en: http://his.sourceforge.net/honeynet/papers/virtual/], [fecha de consulta: 6-11-2011]

HONEYNET PROJECT, Conoce a tu enemigo : Honeynets [en línea] , [disponible en: http://his.sourceforge.net/honeynet/papers/honeynet/], [fecha de consulta: 6-11-2011]

HONEYNET PROJECT, Conoce a tu enemigo: Aprendiendo con User-Mode Linux [en línea], [disponible en: http://his.sourceforge.net/honeynet/papers/uml/], [fecha de consulta: 6-11-2011]

HONEYNET PROJECT, Conoce a tu enemigo: Aprender con VMware [en línea], [disponible en: http://his.sourceforge.net/honeynet/papers/vmware/], [fecha de consulta: 6-11-2011]

HONEYNET PROJECT, Know Your Enemy: Honeynets [en línea], [disponible en: http://old.honeynet.org/papers/honeynet/], [fecha de consulta: 6-11-2011]

MOGROVEJO, C., Arquitectura de Red Activa para el Aseguramiento de Información en Instituciones, Proyecto de Grado, Universidad Católica Boliviana "San Pablo", Bolivia, 2008, 95p

NANDO, Curso seguridad en sistemas de información [en línea], [disponible en: http://www.slideshare.net/nyzapersa/curso-seguridad-en-sistemas-de-informacion#], [fecha de consulta: 9-08-2011]

PROVOS, N., Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley professional, 2007.

REVISTA RED, Seguridad Informática [en línea], 2002 [disponible en: http://www.ciberhabitat.gob.mx/museo/cerquita/redes/], [fecha de consulta: 9-08-2011]

REVISTA SEGU-INFO, Amenazas Lógicas – Tipos de Ataques [en línea], 2009 [disponible en: http://www.segu-info.com.ar/ataques/tipos.htm], [fecha de consulta: 10-08-2011]

SAMPIERI, R., Metodología de la Investigación.2a ed. La Paz: McGraw-Hill Interamericana, 2003

SPITZNER, L., Honeypots: Tracking Hackers, Addison Wesley professional, 2002.

VENTURA, Y., RODRIGUEZ, N., Diseño y desarrollo de Honeynets Virtuales utilizando Vmware para la detección de intrusos informáticos, Tesis Ingeniero en Telecomunicaciones, Universidad Francisco Gavidia, San Salvador, Marzo 2008, 193p

WALDEMAR, J., ICIHONEY: Diseño e Implementación de una Red Trampa en el Instituto de Informática de la Universidad Austral de Chile, Tesis para optar al Título de Ingeniero Civil en Informática, Universidad Austral de Chile, Chile, 2009, 257p

ANEXOS

ANEXO 1: CUESTIONARIO APLICADO A LOS EMPLEADOS DE LA EMPRESA SOMINEX SRL.

NOMBRE DEL PROYECTO: Diseño e implementación de una Honeynet Virtual para la detección y análisis de posibles ataques informáticos en la red de datos de la Empresa SOMINEX SRL.

OBJETIVO: Determinar si existe la factibilidad para realizar el proyecto a través del cuestionario, el cual reflejara la opinión y el conocimiento que los empleados de la Empresa SOMINEX SRL., tienen en cuanto a seguridad en redes de datos.

INDICACIONES: Marcar con una X en el cuadro correspondiente a su respuesta.

1. ¿Utiliza algún mecanismo o política de seguridad para proteger su información y evitar que esta sea, borrada o modificada por usuarios malintencionados?

SI ☐

NO ☐

2. ¿Conoce usted el riesgo al que podrían estar expuestos los sistemas que actualmente poseen, al estar conectados al servicio de Internet?

SI ☐

NO ☐

3. ¿Utiliza alguna estrategia o medida para la detección de intrusos?

SI ☐

NO ☐

4. ¿Se usa alguna estrategia para la prevención de ataques a la información?

SI ☐

NO ☐

NO SABE ☐

5. ¿Es de conocimiento suyo, si se ejerce algún tipo de control y/o monitoreo periódico en la red de su Empresa?

SI ☐

NO ☐

NO SABE ☐

6. ¿Le gustaría conocer los mecanismos de seguridad e implementar un sistema de seguridad con herramientas gratuitas?

SI ☐

NO ☐

7. ¿Le gustaría implementar una herramienta de seguridad cuya infraestructura permita monitorear y asegurar la red de datos de su empresa?

SI ☐

NO ☐

8. ¿Es de su conocimiento la herramienta de seguridad Honeynet Virtual?

SI ☐

NO ☐

9. ¿Le gustaría conocer una propuesta de diseño que incluya la herramienta de seguridad informática Honeynet Virtual, para proteger a su institución contra diversas amenazas?

SI ☐

NO ☐

ANEXO 2: VALORACIÓN E INTERPRETACIÓN DE LOS RESULTADOS OBTENIDOS

A continuación, se presentan los gráficos y tablas de cada pregunta con su respectiva interpretación

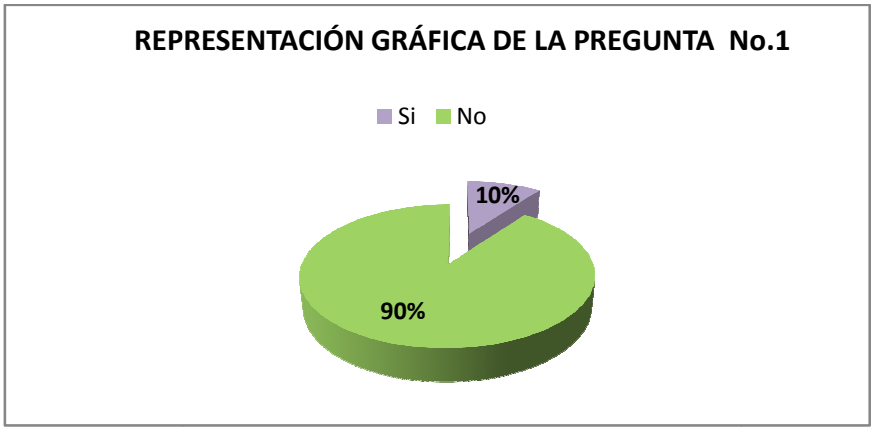
Pregunta No. 1

¿Utiliza algún mecanismo o política de seguridad para proteger su información y evitar que esta sea, borrada o modificada por usuarios malintencionados?

Objetivo:

Conocer si el personal de la Empresa SOMINEX SRL., tiene conocimiento sobre los mecanismos o políticas de seguridad adecuados para gestionar su información.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	1	10
No	9	90
TOTALES	10	100



Interpretación:

La mayoría de las personas encuestadas no tienen conocimiento sobre los mecanismos adecuados para proteger su información.

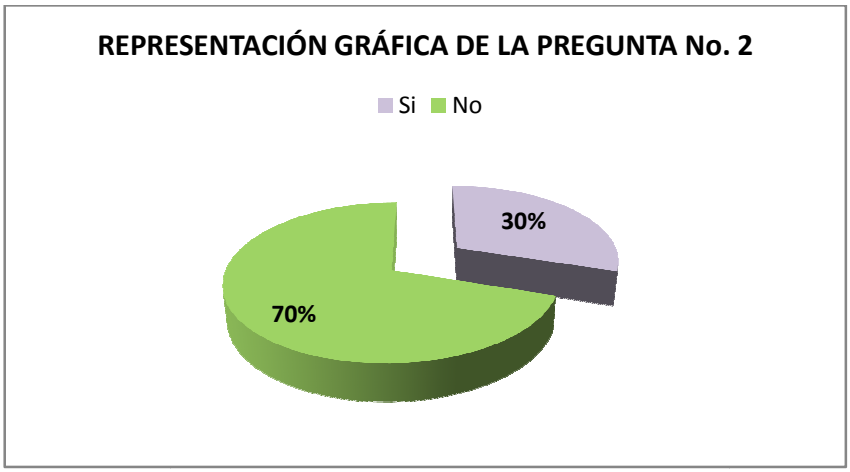
Pregunta No. 2

¿Conoce usted el riesgo al que podrían estar expuestos los sistemas que actualmente poseen, al estar conectados al servicio de Internet?

Objetivo:

Conocer si el personal de la Empresa SOMINEX SRL., tiene conocimiento sobre el riesgo que implica estar conectado al servicio de Internet, sin tener mecanismos de seguridad adecuados para gestionar su información.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	3	30
No	7	70
TOTALES	10	100



Interpretación:

La mayoría de las personas encuestadas no tienen conocimiento sobre los riesgos a los que están expuestos los sistemas que poseen, cuando se conectan a los servicios de Internet.

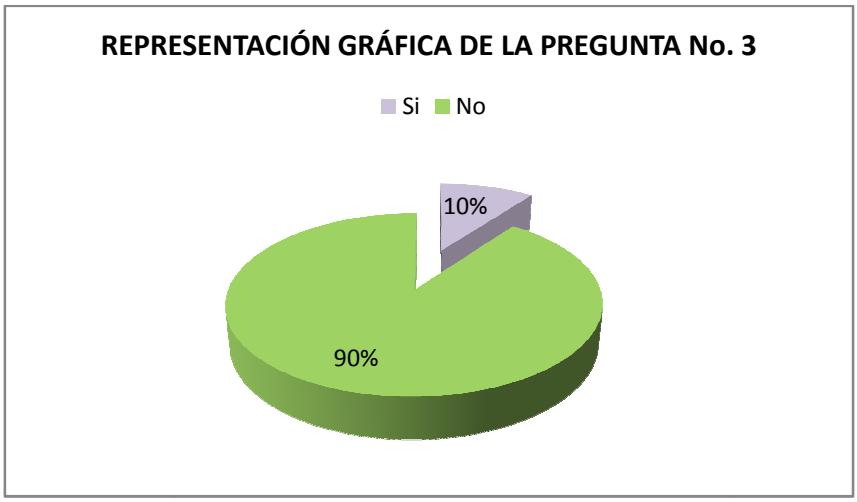
Pregunta No. 3

¿Utiliza alguna estrategia o medida para la detección de intrusos?

Objetivo:

Conocer si el personal de la Empresa Minera SOMINEX SRL., utiliza alguna estrategia o medida para la detección de intrusos.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	1	10
No	9	90
TOTALES	10	100



Interpretación:

De acuerdo al resultado obtenido se pudo afirmar que la mayoría de las personas encuestadas no utiliza alguna estrategia o medida para la detección de intrusos.

Pregunta No. 4

¿Se usa alguna estrategia para la prevención de ataques a la información?

Objetivo:

Conocer si el personal de la Empresa Minera SOMINEX SRL., utiliza alguna estrategia para la prevención de ataques a su información.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	1	10
No	7	70
No sabe	2	20
TOTALES	10	100



Interpretación:

De acuerdo al resultado obtenido se pudo afirmar que la mayoría de las personas encuestadas no utiliza alguna estrategia para la prevención de ataques a su información, por otra parte un 20% del personal encuestado no tiene conocimiento respecto a estrategias utilizadas en la prevención de ataques.

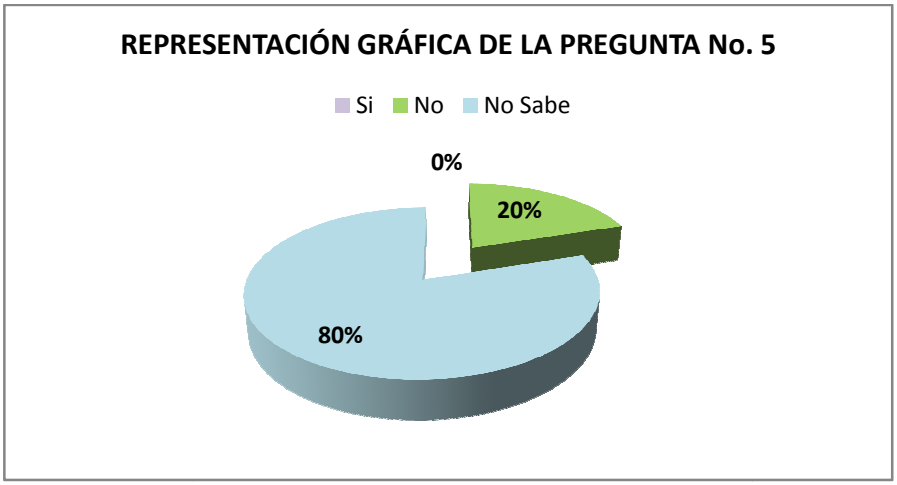
Pregunta No. 5

¿Es de conocimiento suyo, si se ejerce algún tipo de control y/o monitoreo periódico en la red de su Empresa?

Objetivo:

Conocer si la Empresa SOMINEX SRL., monitorea la red de datos con periodicidad para prevenir los ataques informáticos.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	0	0
No	2	20
No sabe	8	80
TOTALES	10	100



Interpretación:

De acuerdo al resultado obtenido se pudo afirmar que la mayoría de las personas encuestadas no tienen conocimiento sobre la realización de controles y/o monitoreos a la red de datos.

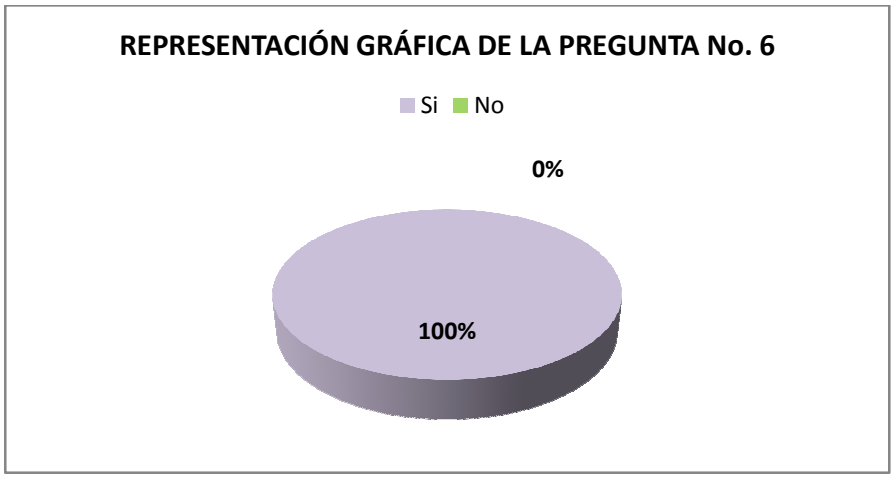
Pregunta No. 6

¿Le gustaría conocer los mecanismos de seguridad e implementar un sistema de seguridad con herramientas gratuitas?

Objetivo:

Conocer si el personal de la Empresa SOMINEX SRL., están interesados en informarse acerca de las políticas de seguridad con que deberían contar, así mismo si están interesados en implementar un sistema de seguridad con herramientas gratuitas

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	10	100
No	0	0
TOTALES	10	100



Interpretación:

De acuerdo al resultado obtenido se pudo determinar que todas las personas consultadas afirman que están interesadas en informarse acerca de los mecanismos de seguridad adecuados, y en la implementación de un sistema de seguridad con herramientas gratuitas.

Pregunta No. 7

¿Le gustaría implementar una herramienta de seguridad cuya infraestructura permita monitorear y asegurar la red de datos de su empresa?

Objetivo:

Determinar si el personal de la Empresa SOMINEX SRL., está interesado en la implementación de una herramienta de seguridad que permita monitorear y asegurar la red de datos.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	0	0
No	10	10
TOTALES	10	100



Interpretación:

De acuerdo al resultado obtenido se pudo evidenciar que todas las personas consultadas afirman que están interesadas en la implementación de una herramienta de seguridad que permita monitorear y asegurar la red de datos.

Pregunta No. 8

¿Es de su conocimiento la herramienta de seguridad Honeynet Virtual?

Objetivo:

Determinar si el personal de la Empresa SOMINEX SRL. tiene conocimiento sobre las herramienta de seguridad Honeynet Virtual.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	0	0
No	10	10
TOTALES	10	100



Interpretación:

De acuerdo al resultado obtenido se pudo determinar que todas las personas consultadas afirman que no tiene conocimiento sobre la existencia de la herramienta de seguridad Honeynet Virtual.

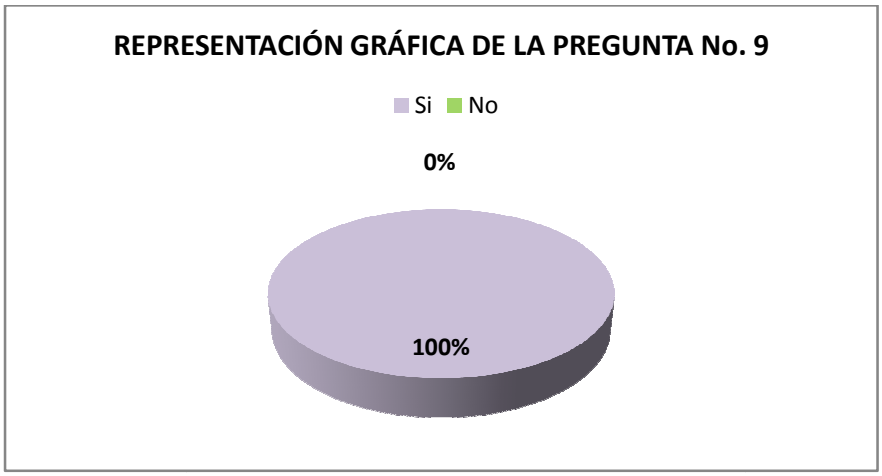
Pregunta No. 9

¿Le gustaría conocer una propuesta de diseño que incluya la herramienta de seguridad informática Honeynet Virtual, para proteger la red de datos de su institución contra diversas amenazas?

Objetivo:

Conocer si la Empresa Minera SOMINEX SRL., está interesada en conocer la propuesta de diseño que incluya la herramienta de seguridad Honeynet Virtual para proteger la red de datos de la institución contra diversas amenazas.

ALTERNATIVAS	FRECUENCIA	PORCENTAJE (%)
Si	10	100
No	0	0
TOTALES	10	100



Interpretación:

De acuerdo al resultado obtenido se pudo determinar que todas las personas consultadas afirmas que están interesadas en la propuesta de diseño de la herramienta de seguridad Honeynet Virtual para la protección de la red de datos contra diversas amenazas.

ANEXO 3: INSTALACIÓN DE LA IMAGEN HONEYWALL EN VMWARE WORKSTATION

La versión del VMWare Workstation que se utilizó para la Honeynet Virtual es la versión 7, la cual se descargo del sitio web www.vmware.com. Posteriormente se procedió a la configuración de la maquina virtual en la que se instalo la Honeywall.

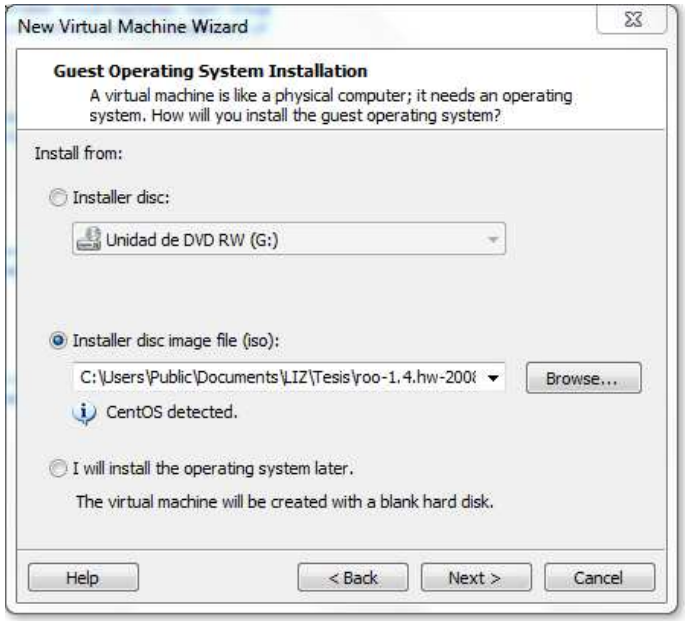


Figura 5.1 Inicio de la configuración de la maquina virtual

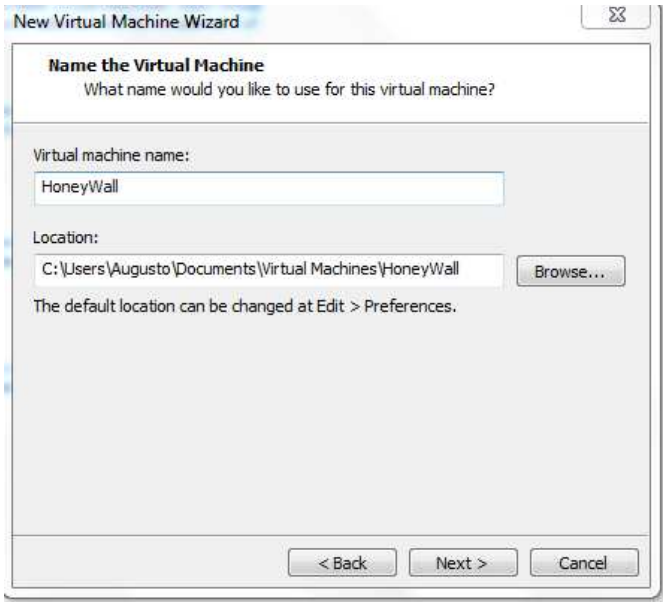


Figura 5.2 Asignación del nombre a la maquina virtual

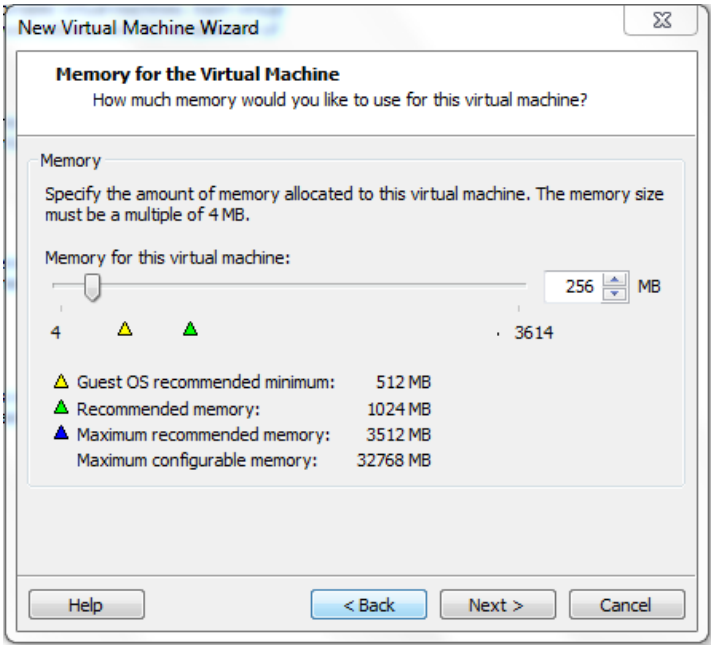


Figura 5.3 Asignación del memoria a la maquina virtual

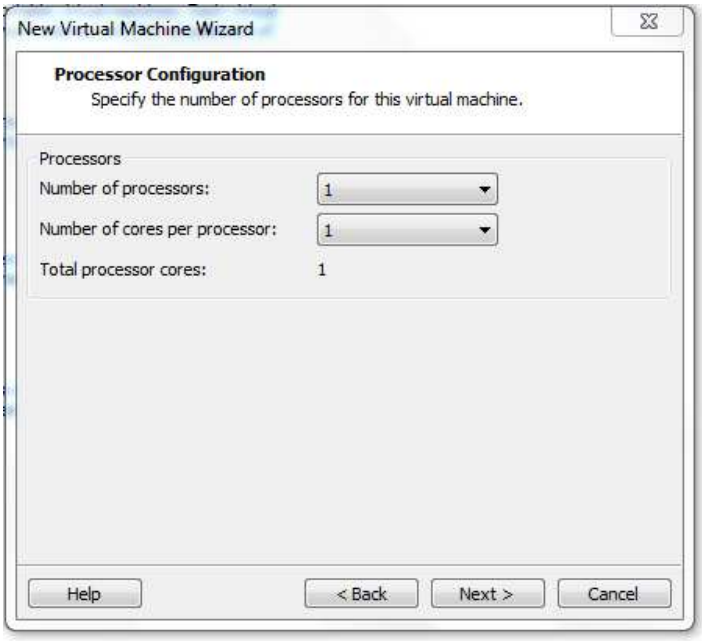


Figura 5.4 Configuración de número de procesadores de la maquina virtual

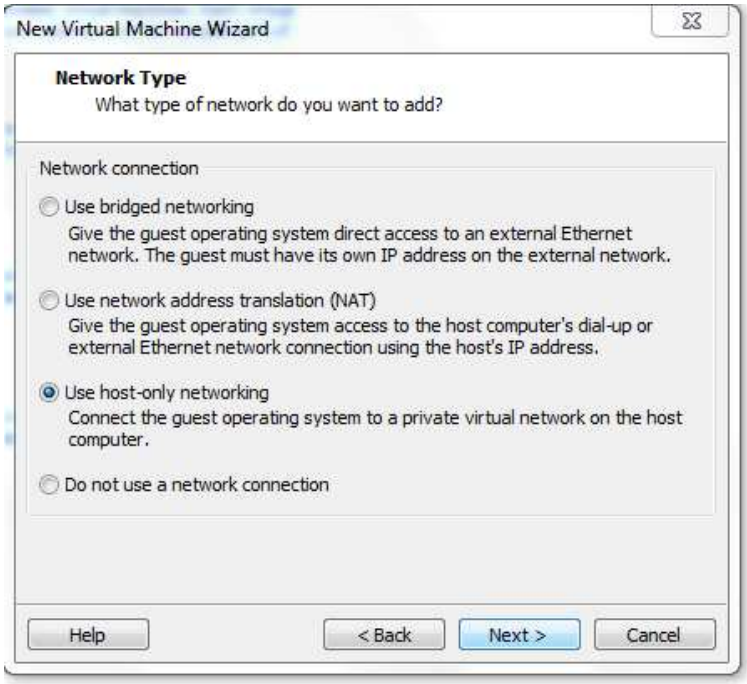


Figura 5.5 Configuración de las interfaces de red de la maquina virtual

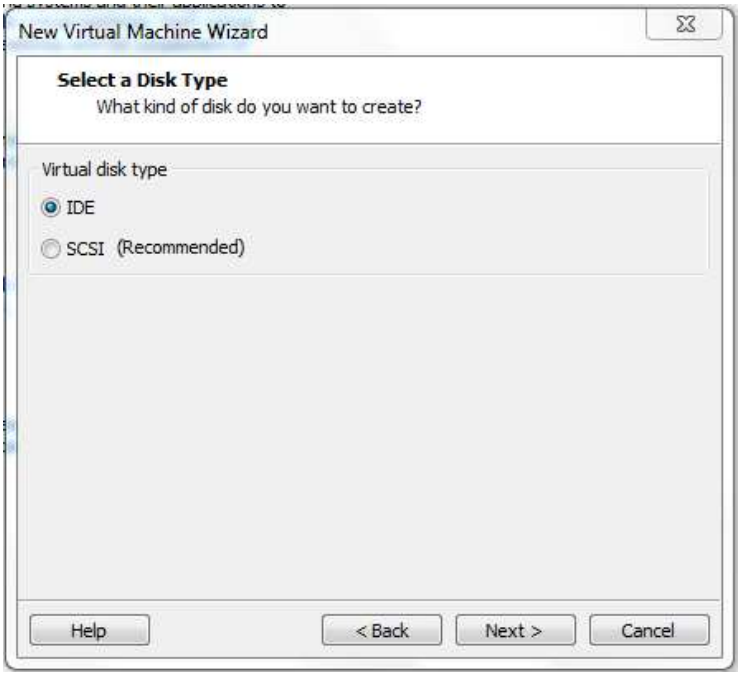


Figura 5.6 Configuración del tipo de disco a ser utilizado en la maquina virtual

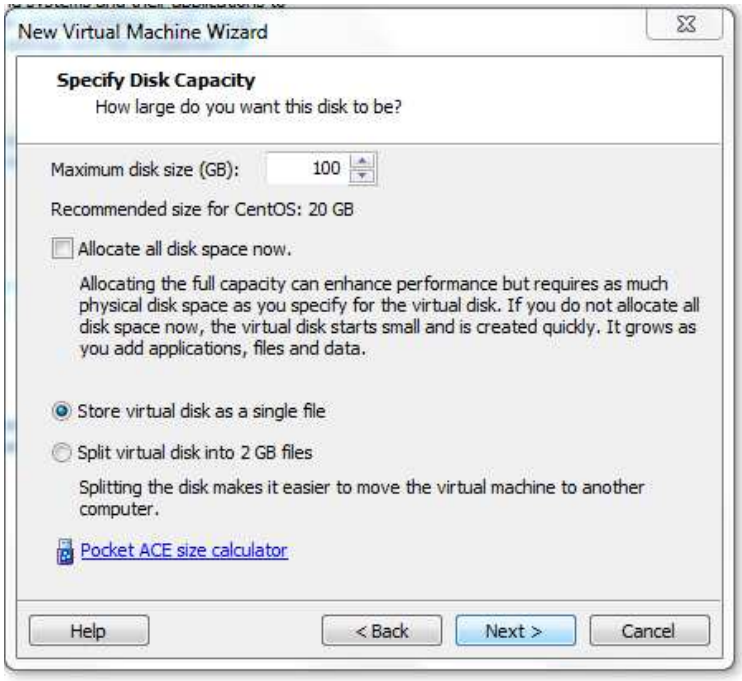


Figura 5.7 Configuración de la capacidad del disco a ser utilizado en la maquina virtual

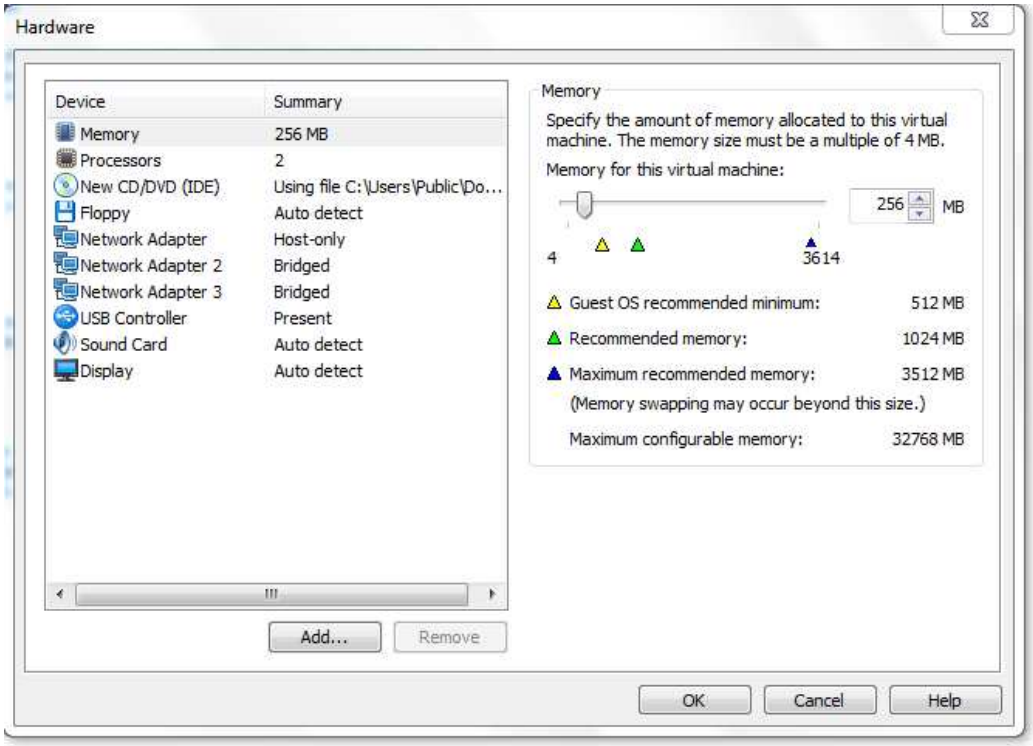


Figura 5.8 Resumen general de la configuración a ser utilizada en la maquina virtual

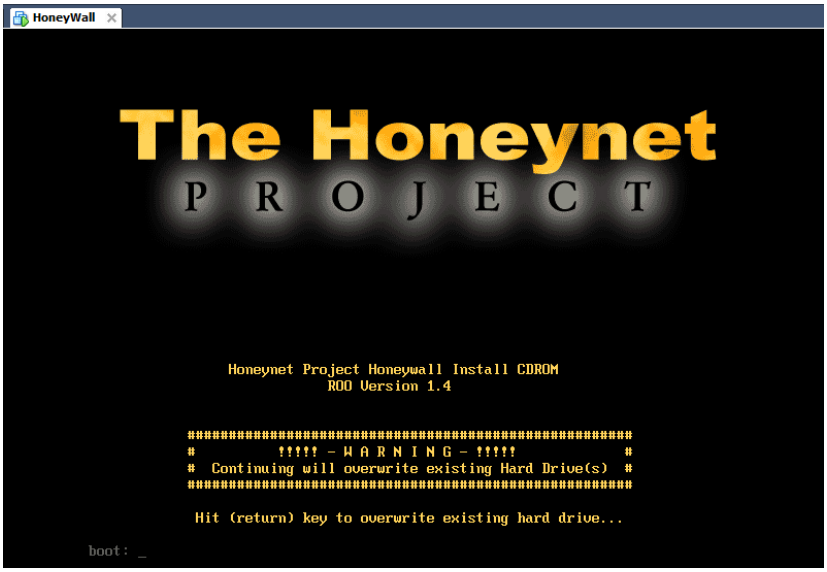


Figura 5.9 Inicio del proceso de instalación de la Honeywall en la maquina virtual

ANEXO 4: CONFIGURACIÓN DEL HONEYWALL ROO V1.4

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

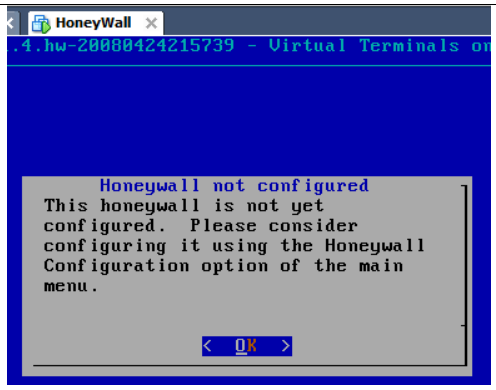


Figura 6.1 Pantalla de advertencia para configurar el Honeywall

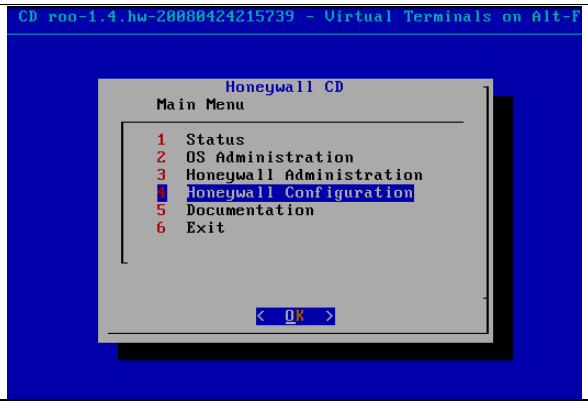


Figura 6.2 Inicio de la configuración del Honeywall

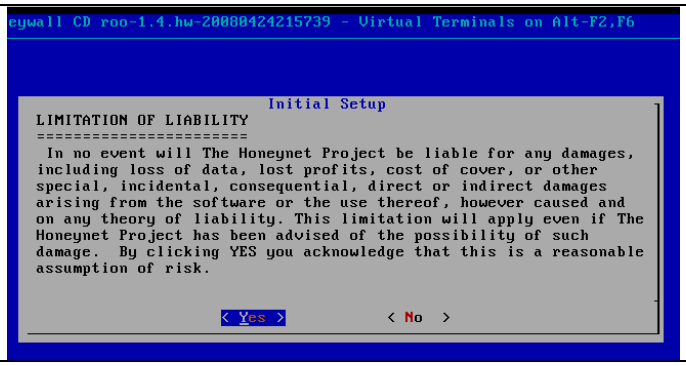


Figura 6.3 Inicio de la primera sección de configuración

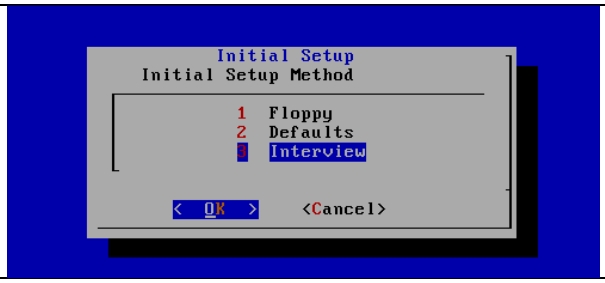


Figura 6.4 Selección del tipo de configuración

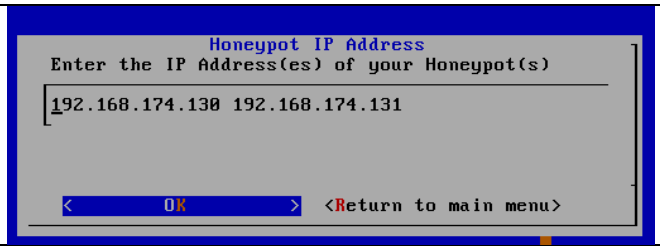


Figura 6.5 Ingreso de la direcciones Ips de los Honeypots

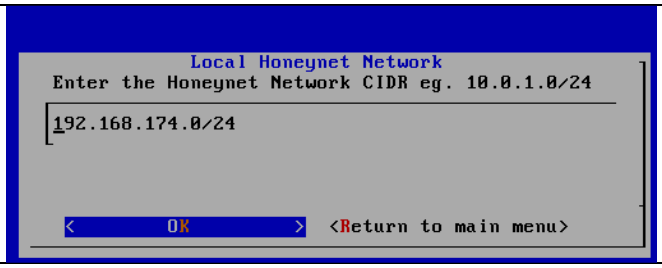


Figura 6.6 Ingreso de la red utilizada para la Honeynet



Figura 6.7 Interface eth0 y eth1 encontrada

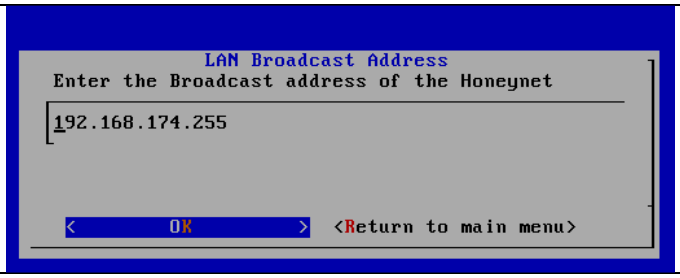


Figura 6.8 Ingreso de las direcciones broadcast de la red LAN



Figura 6.9 Finalización de la primera sección de la configuración



Figura 6.10 Inicio de la configuración de interface de administración

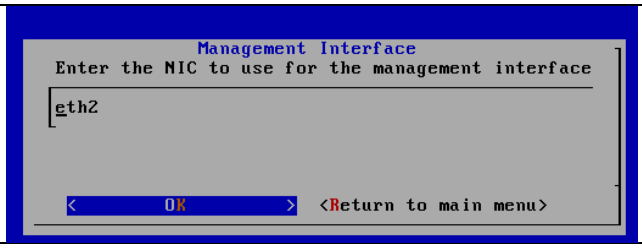


Figura 6.11 Ingreso del NIC de la interface de administración

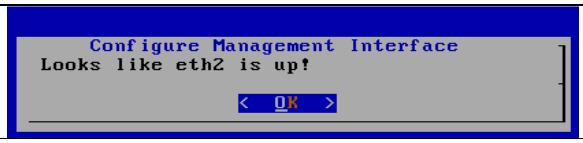


Figura 6.12 Interface de administración activa

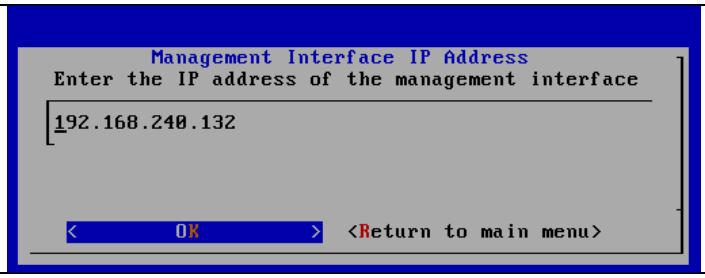


Figura 6.13 Ingreso de la dirección IPs de administración

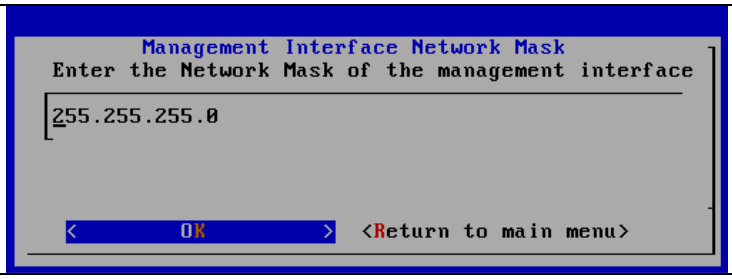


Figura 6.14 Ingreso de la máscara para la interfaz de administración

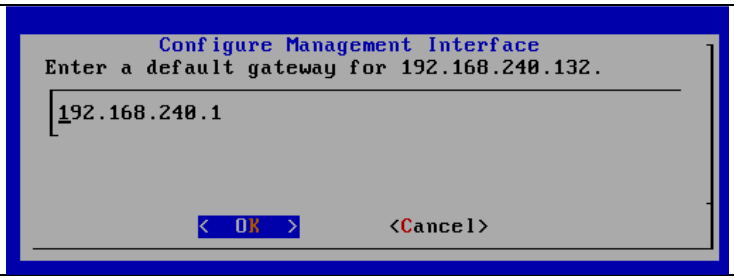


Figura 6.15 Ingreso de la default gateway para la interface de administración

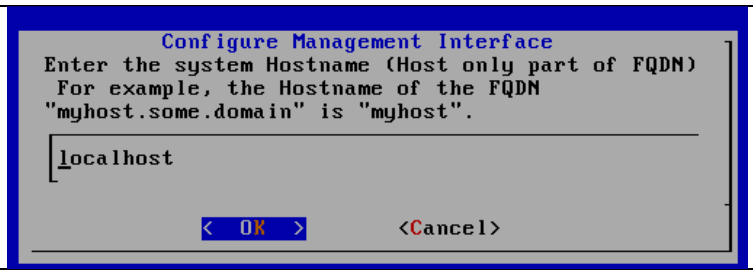


Figura 6.16 Configuración de interfaz

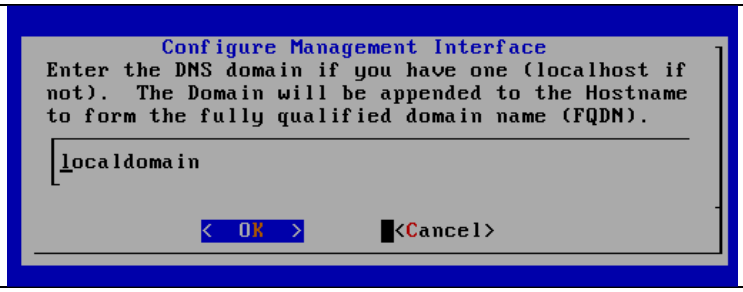


Figura 6.17 Configuración de interfaz

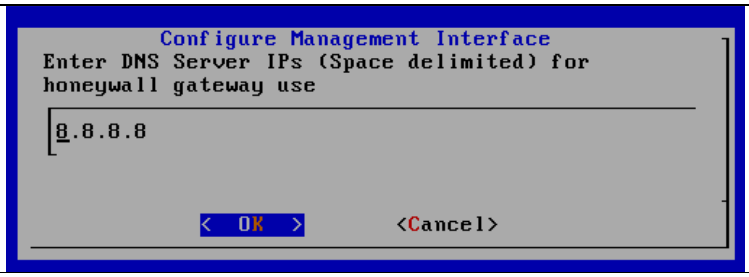


Figura 6.18 Ingreso de las direcciones IPs de los servidores DNS



Figura 6.19 Activación de la interface de administración



Figura 6.20 Iniciar la interface de administración en el siguiente boteo

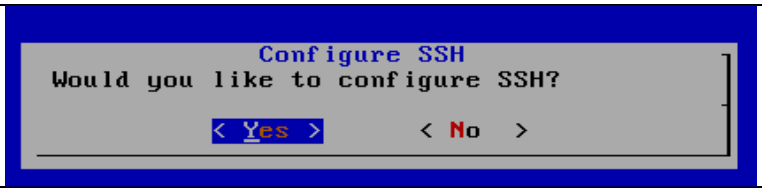


Figura 6.21 Iniciar la configuración de SSH

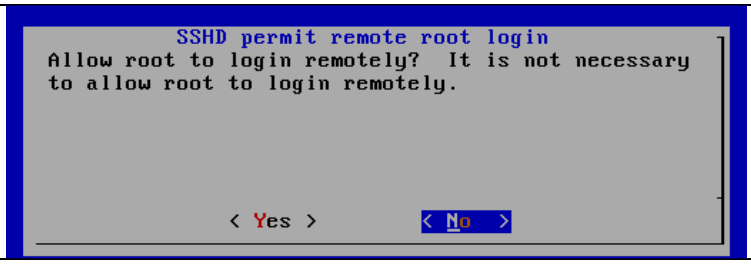


Figura 6.22 Permitir el loguearse remotamente por SSHD

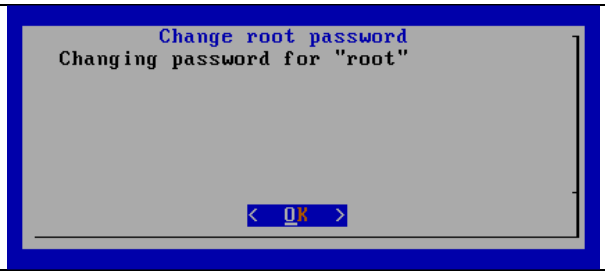


Figura 6.23 Cambio de la contraseña del root



Figura 6.24 Ingreso de la nueva contraseña del root



Figura 6.25 Cambio de la contraseña exitoso



Figura 6.26 Cambio de la contraseña del roo



Figura 6.27 Ingreso de la nueva contraseña del roo

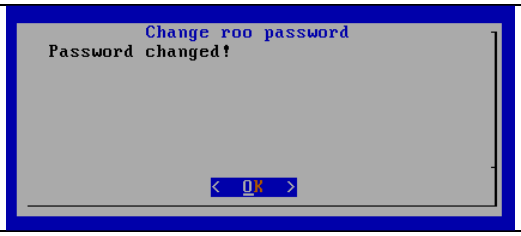


Figura 6.28 Cambio de la contraseña exitosa

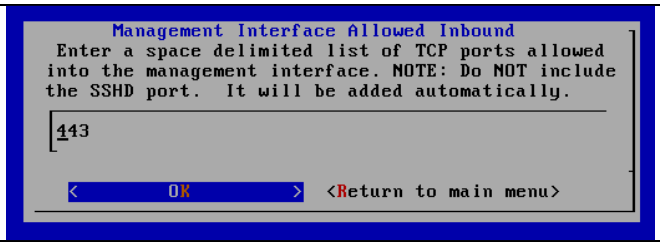


Figura 6.29 Ingreso del puerto TCP permitido para acceder a la administración web del Honeywall

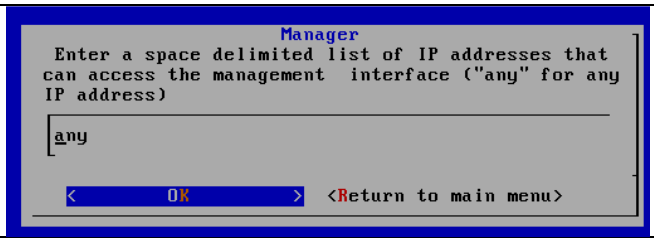


Figura 6.30 Ingreso de la IP para acceder a la web de administración de la Honeywall

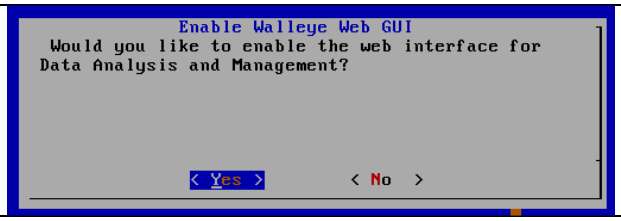


Figura 6.31 Activar la interfaz Walleye

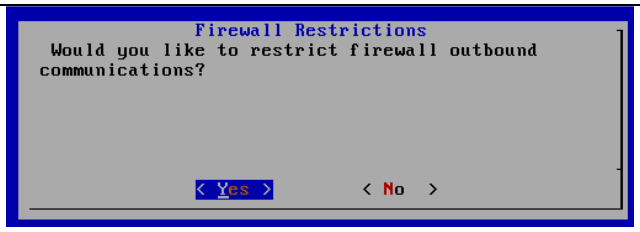


Figura 6.32 Activa r las restricciones del firewall para prevenir troyanos y malware

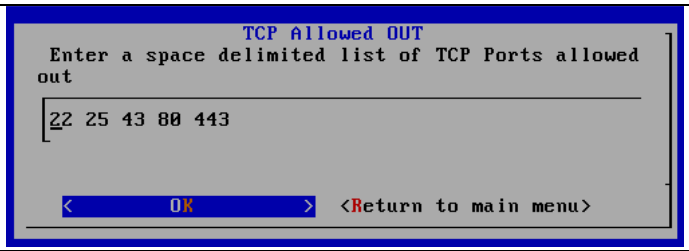


Figura 6.33 Ingreso de los puertos TCP que permiten la salida

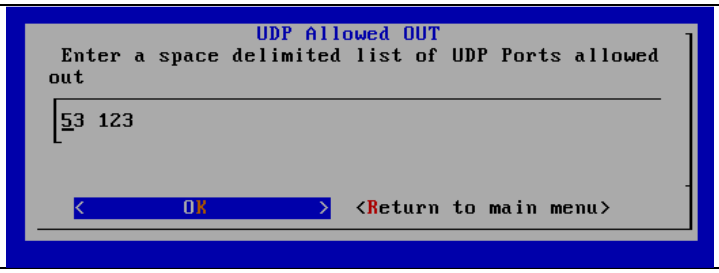


Figura 6.34 Ingreso de los puertos UDP que permitan la salida

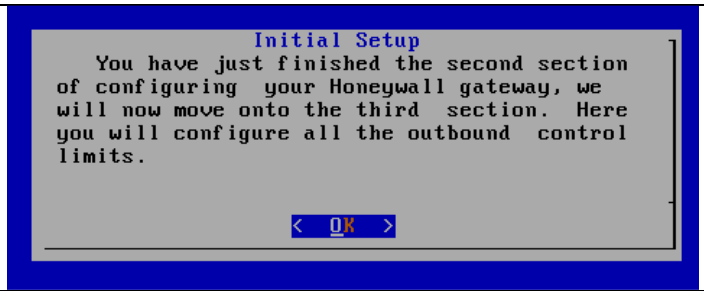


Figura 6.35 Finalización de la segunda sección de configuración del Honeywall

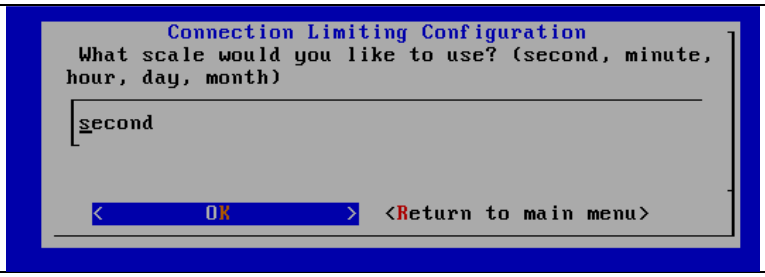


Figura 6.36 Establecer el límite de conexiones salientes. (second, minute, hour, day)

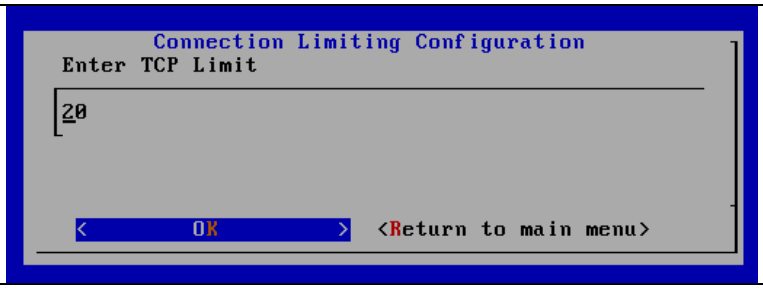


Figura 6.37 Establecer el límite de conexiones TCP

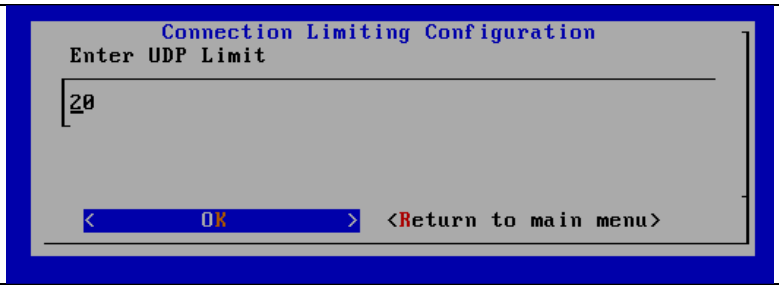


Figura 6.38 Establecer el límite de conexiones UDP

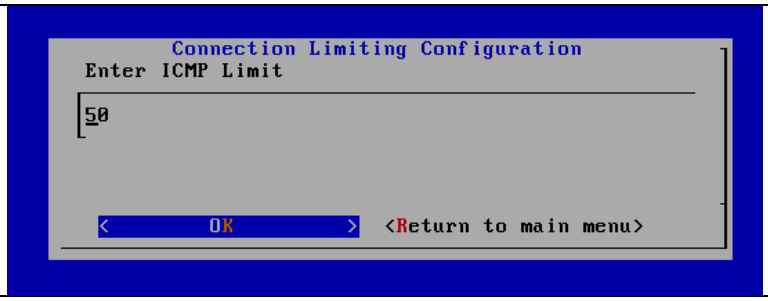


Figura 6.39 Establecer el límite de conexiones ICMP

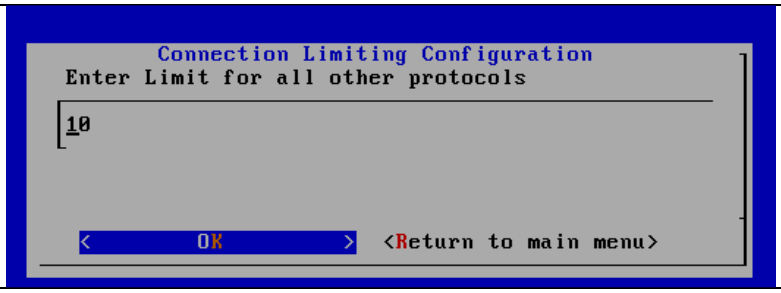


Figura 6.40 Establecer el límite de conexiones de los demás protocolos

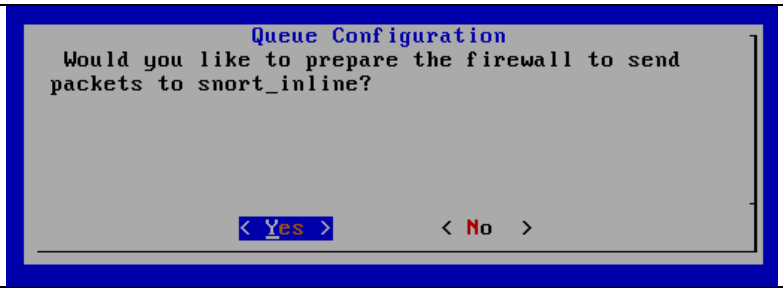


Figura 6.41 Activar el snort-inline para evitar el tráfico malicioso a la red.

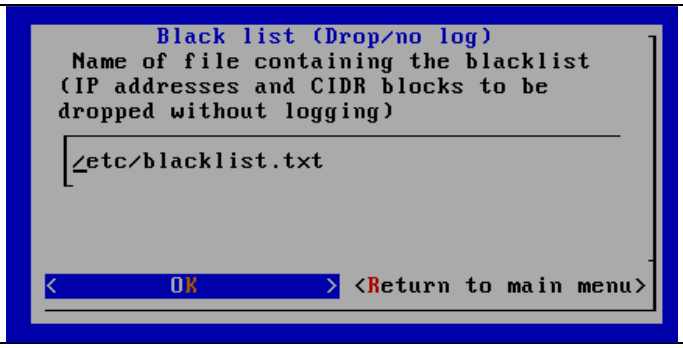


Figura 6.42 Ingrese el nombre del archivo que contiene la lista de direcciones IPs que generan SPAM (Blacklist)

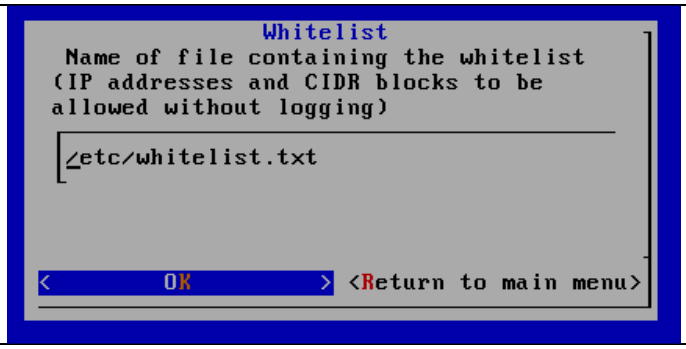


Figura 6.43 Ingrese el nombre del archivo que contiene las direcciones IPs que nunca generan SPAM (WhiteList)

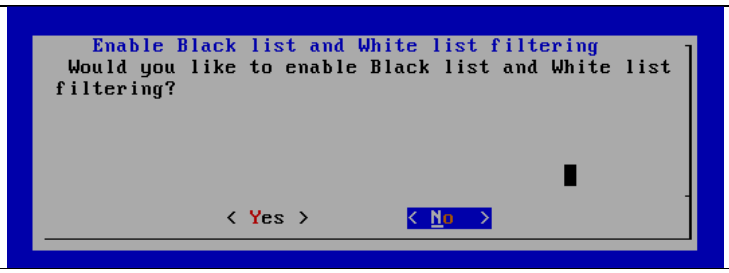


Figura 6.44 Habilitar el filtrado de la lista Blanca y Negra



Figura 6.45 No habilitar “Strict” Capture Filtering

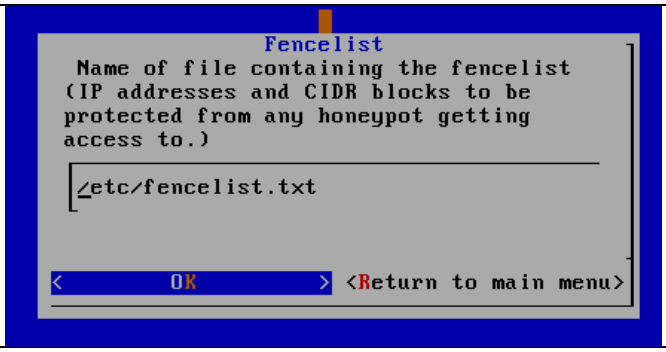


Figura 6.46 Ingrese el nombre del archivo que contiene las direcciones IP que por medio del Fencelist el firewall bloqueará todo el tráfico hacia ellas.

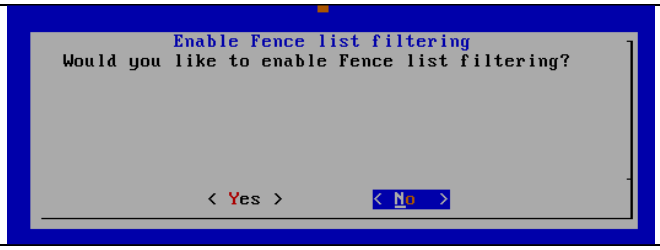


Figura 6.47 No habilitar Fence list Filtering

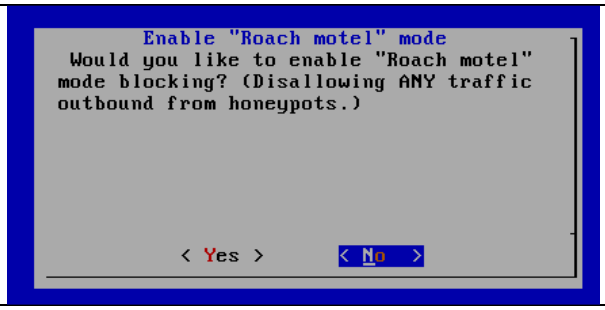


Figura 6.48 No habilitar "Roach Motel" para así desactivar el bloqueo de todo el tráfico saliente de los Honeypots

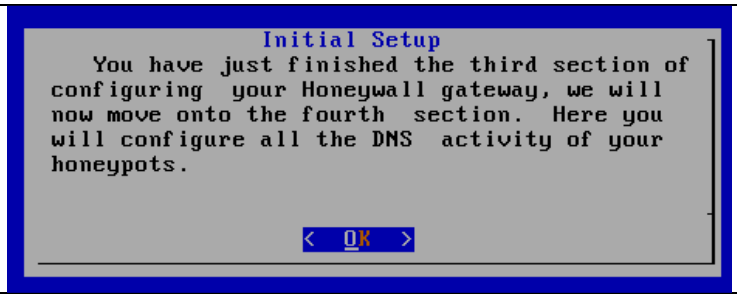


Figura 6.49 Inicio de la tercera sección de configuración del Honeywall

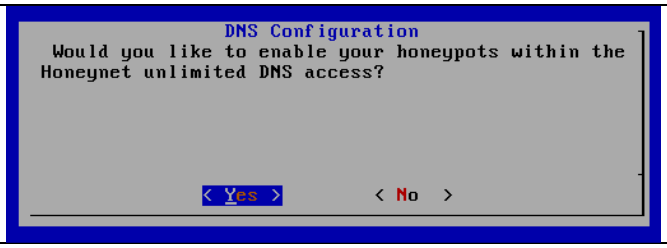


Figura 6.50 Configuración de los DNS para los Honeypots

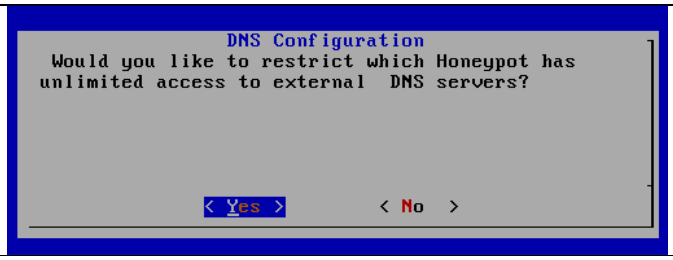


Figura 6.51 Configuración de los DNS para los Honeypots

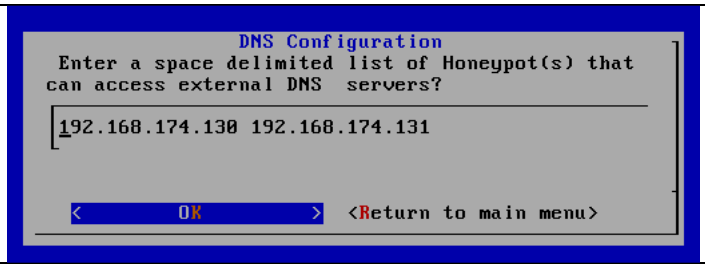


Figura 6.52 Ingresar la lista de IPs de los Honeypots

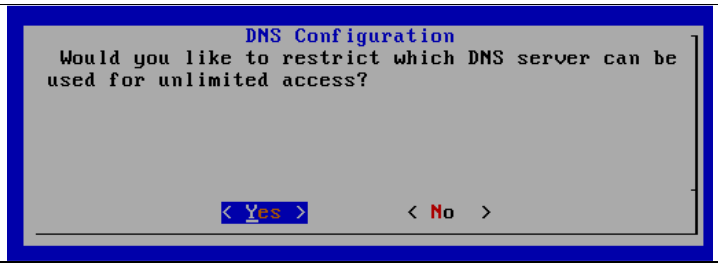


Figura 6.53 Configuración de DNS server que serán usados para no limitar el acceso

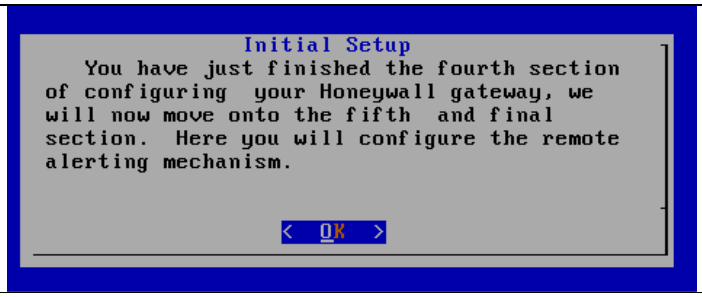


Figura 6.54 Inicio de la cuarta sección de configuración del Honeywall

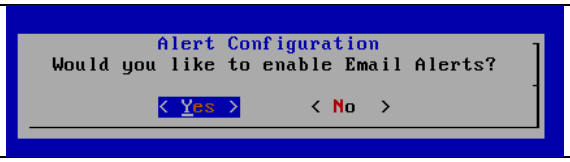


Figura 6.55 Inicio de la configuración de alertas de mail

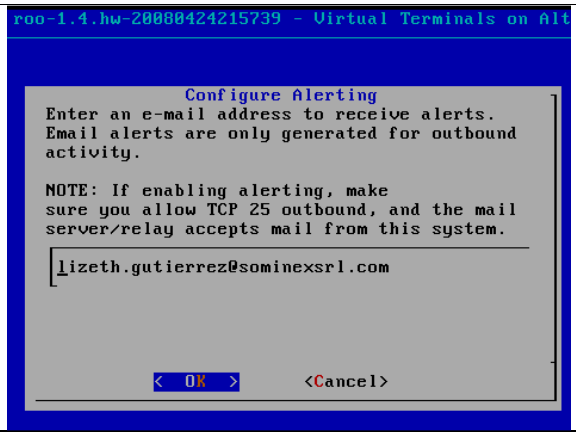


Figura 6.56 Ingreso del correo electrónico usado para recibir las alertas



Figura 6.57 Iniciar la configuración del mail de alertas en el boteo

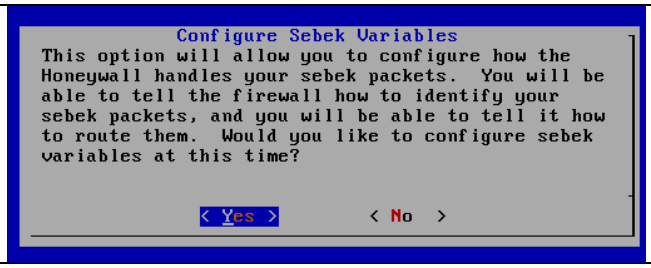


Figura 6.58 Inicio de la configuración de variables del Sebek

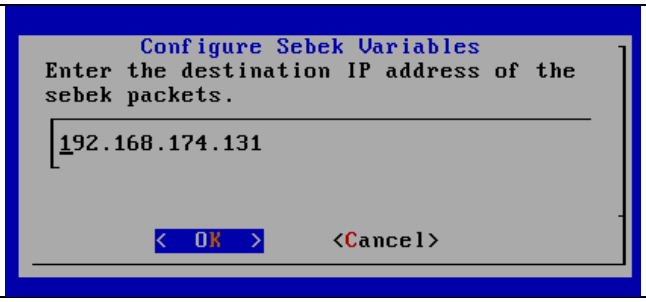


Figura 6.59 Ingreso de la dirección IP destino de los paquetes del Sebek

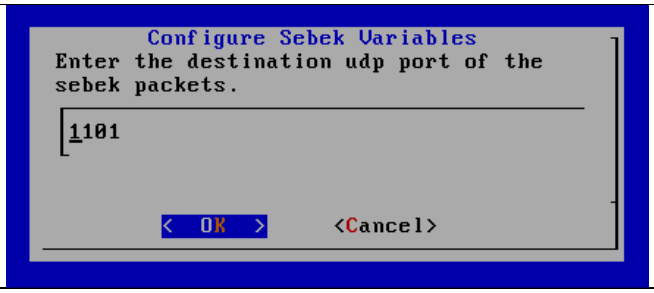


Figura 6.60 Configuración de las variables de Sebek

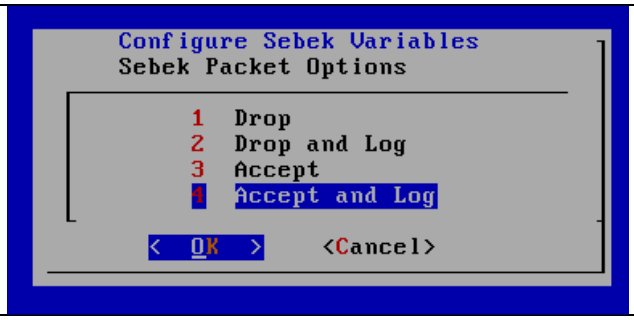


Figura 6.61 Aceptar todas las configuraciones

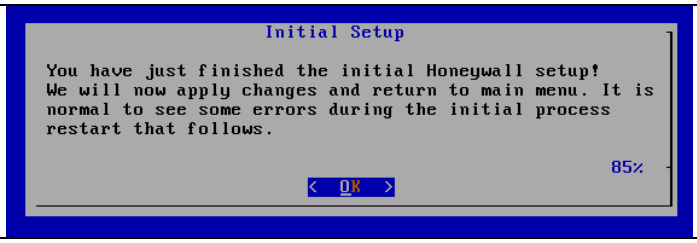


Figura 6.62 Finalización de configuración del Honeywall