PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA SISTEMAS

"IMPLEMENTACIÓN DE UN PROTOTIPO DE SEGURIDAD CON HONEYNET VIRTUALES PARA DESCUBRIR PATRONES DE ATAQUES Y ANALIZAR EL COMPORTAMIENTO Y LAS CONDICIONES DE LOS INTRUSOS, APLICADO EN EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN - LTIC."

DISERTACIÓN DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN

AUTOR: Jhonny Vaca

QUITO, 2014

Dedicatoria

Esta tesis esta dedica a mi Padre Dios quién me ha dado el valor y las fuerzas para enfrentar toda adversidad que se ha presentado en mi vida, él siempre ha levantara bandera a mi favor proclamando victoria sin importar la situación, él nunca me ha abandonado ni me a desamparado, doy toda la honra y la gloria a él.

A mis padres por su amor y apoyo incondicional en los momentos difíciles, por su esfuerzo para proveerme de todos los recursos necesarios para estudiar.

A mí querida esposa por su amor incondicional, quien ha sido una bendición en mi vida en todo momento.

A mi familia en general, quienes siempre han estado presentes con sus palabras de ánimo.

Agradecimiento

Mi sincero agradecimiento a la Pontificia Universidad Católica del Ecuador, y en ella a los distinguidos docentes de la Facultad de Ingeniería quienes con su profesionalismo y ética demostrada en las aulas, nos han compartido sus conocimientos y experiencias para formarnos como profesionales de bien para la sociedad.

A mi Directora y Correctores de tesis, quienes con su experiencia ha sido la guía adecuada, durante el proceso de realización de mi tesis, agradezco su tiempo y su disponibilidad.

ABSTRACT

Muchas organizaciones hoy en día usan Firewall y sistemas de detección de intrusos (IDS) como parte de sus defensas de seguridad en la red. Sin embargo, en los últimos años aparte de estas dos tecnologías, una nueva tecnología llamada honeynet ha recibido mucha atención, como recurso de seguridad en la red. Una Honeynet puede ser pensada como una red señuelo que utiliza el engaño para atraer a los intrusos, esta red puede ser sondeada o atacada la cual captura información acerca de las actividades maliciosas de los atacantes, permitiendo analizar detenidamente dicha información y dar la posibilidad de aprender las tácticas y determinar los patrones de ataques que emplean los intrusos para comprometer los sistemas.

La presente disertación de grado describe el proceso de implementación de un prototipo de Honeynet Virtual Auto contenida, en el entorno de red del Laboratorio de Tecnología de la Información y Comunicación – LTIC de la Facultad de Ingeniería de la PUCE. También se analizará de forma rápida la situación actual del LTIC, en relación a los servicios que presta y sus seguridades tanto lógicas como físicas.

La Honeynet tendrá la opción de mantenerse en ejecución de forma que pueda monitorear, analizar y recolectar información en ambiente real, o simplemente proporcionar recursos educativos de naturaleza demostrativa y de investigación.

Tabla de Contenido

Índice de Gráficos

Índice de Tablas

CAPÍTULO I

REDES INFORMATICAS, ATAQUES Y VULNERABILIDADES

1.1 REDES INFORMÁTICAS

1.1.1 Que es unaRed Informática

Es la unión de dos o más ordenadores o dispositivos de manera que sean capaces de compartir recursos, ficheros, directorios, discos, impresoras.

En otro concepto, unared, más que varios ordenadores conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

La finalidad de una red es que los usuarios de los sistemas informáticos de una organización puedan hacer un mejor uso de los mismos, mejorando de este modo el rendimiento global de la organización.[1]

1.1.2 Evolución de las Redes

Las redes han ido evolucionado conforme lo demandan las necesidades de comunicación, verbal o visual.La primera red fue creada por Arpanet[2],su objetivo principal era que la información militar de los EEUU, no estuviera centralizada y pudiera estar disponible desde cualquier punto del país. Científicos de la Universidad of California, conectaron dos computadoras concableyvieron fluir los datos de una máquina a la otra.

[1]Antonio Bueno. Unidad Didáctica: "Redes Informáticas".
http://www.portaleso.com/portaleso/trabajos/tecnologia/comunicacion/ud_4_redes_v1_c.pdf
[2]**Arpanet:** la red militar que es reconocida como la progenitora de Internet.

Cuando el primer sistema de comunicaciones resulto obsoleto, se creó el protocolo TCP/IP[3], estos fueron adoptados como estándar para todos los ordenadores conectados, surgiendo la red universalllamadaInternet.[4]

1.1.3 Tipos de Redes

1.1.3.1 LAN – Red de área local

Conecta los dispositivos de red en distancias corta, hogares, cibercafés, etc.,

1.1.3.2 WAN - Redes de área amplia

Es una colección de LAN dispersadas geográficamente cientos de kilómetros una de otra. WAN usa protocolos como X.25 y FrameRelay.[5]

1.1.3.3 WLAN -Red de área local inalámbrica

Funcionan de una forma parecida a las redes LAN, comunican los ordenadores usanunatecnología basada en redes inalámbricasWifi.

1.1.3.4 VPN- Una red privada virtual

Es una tecnología de red que permite una extensión segura de la red local (LAN), sobre una red pública o no controlada como Internet.[6]

1.1.4 Protocolos de Red

El concepto de protocolo de red se utiliza para nombrar a las normativas y los criterios que fijan cómo deben comunicarse los diversos componentes de

[3] **TCP/IP:** Protocolo de Control de Transmisión/Protocolo de Internet
[4] Fabián Rene Cruz. (2011). Historia y Evolución de las Redes. http://fumsnuevastecnologias.wordpress.com/2011/10/05/historia-de-las-redes/
[5] **FrameRelay:** Se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.
[6] Clasificación de las Redes Informáticas: PAN, CAN, LAN, MAN y WAN. Redes Públicas y Privadas. http://armarioyuliana.blogspot.com/p/clasificacion-de-las-redes-informaticas.html

un cierto sistema de interconexión. Es decir que, a través de este protocolo, los dispositivos que se conectan en red pueden intercambiar datos.

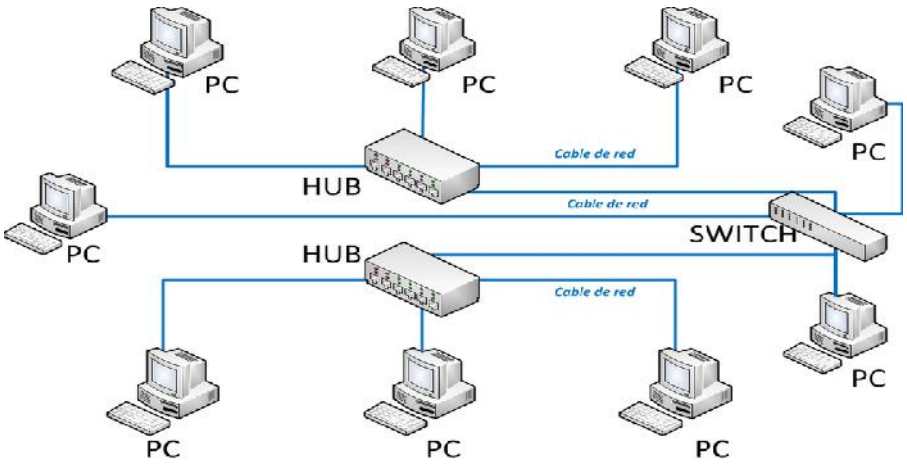
1.1.4.1 MODELO OSI

El Modelo OSI divide en 7 capas el proceso de transmisión de la información entre equipo informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global.[7]

1.1.4.2 Capas del Modelo OSI

1.1.4.2.1 Capa física

Gráfico 1: Capa Física del Modelo OSI[8]



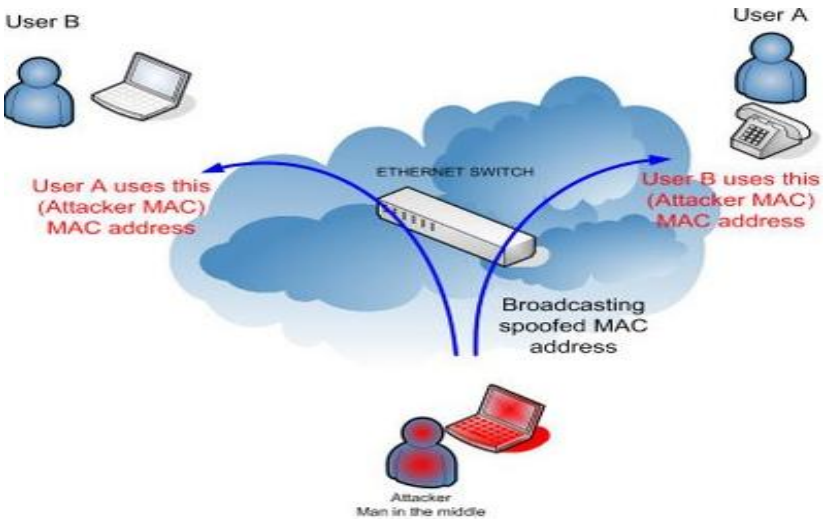
Se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información. Esta Capa define el medio o medios físicos por losque va a viajar la comunicación: cable de pares trenzados, coaxial, aire, fibra óptica.

[7] Ing. Iver Claros. Universidad Privada Cumbre. Modelo OSI. http://belarmino.galeon.com/ http://construiryadministrarredcb7716antonia.blogspot.com/2011/05/modelo-osi-y-sus-siete-capas.html

[8] **Gráfico 1:** Capa Física del Modelo OSI. http://elementosdeinterconexion.blogspot.com/

1.1.4.2.2 Capa de enlace de datos

Gráfico 2: Capa de Enlace de Datos del Modelo OSI[9]



Como objetivo, la capa de enlace de datos se encarga de tomar una transmisión de datos cruda y transformarla en una abstracción libre de errores de transmisión para la capa de red. Este proceso se lleva a cabo dividiendo los datos de entrada entramas de datos (de unos cuantos cientos de bytes), transmite las tramas en forma secuencial, y procesa los marcos de estado que envía el nodo destino. Ejemplos: tarjeta de red, hub, bridge, switch, servidores,ATM,Ethernet,HDLC[10],PPP, Wi-Fi[11],STP.[12]

[9] **Gráfico 2:** Capa de Enlace de Datos del Modelo OSI
http://construiryadministrarredcb7716antonia.blogspot.com/2011/05/modelo-osi-y-sus-siete-capas.htm

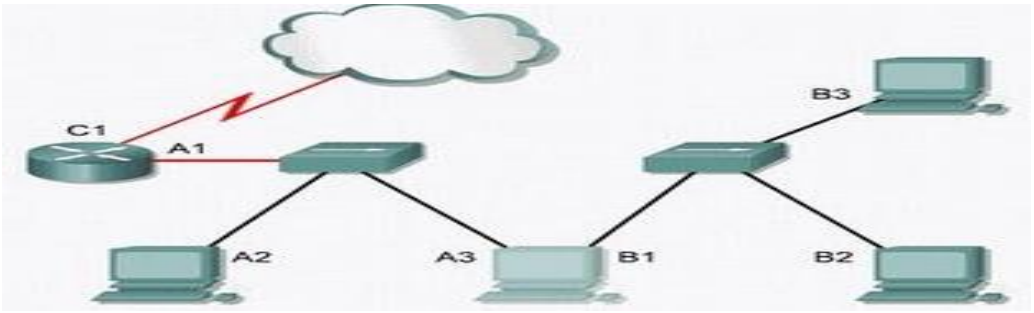
[10] **HDLC** (Control de Enlace de Datos de Alto Nivel): estándar a nivel de enlace de datos que incluye mecanismos para la detección y corrección de errores.

[11] **WI-FI:** Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

[12] **STP:** SpanningTree Protocolo) es un protocolo de red de nivel 2 del modelo OSI. Su función en muchos casos es para garantizar la disponibilidad de las conexiones.

1.1.4.2.3 Capa de red

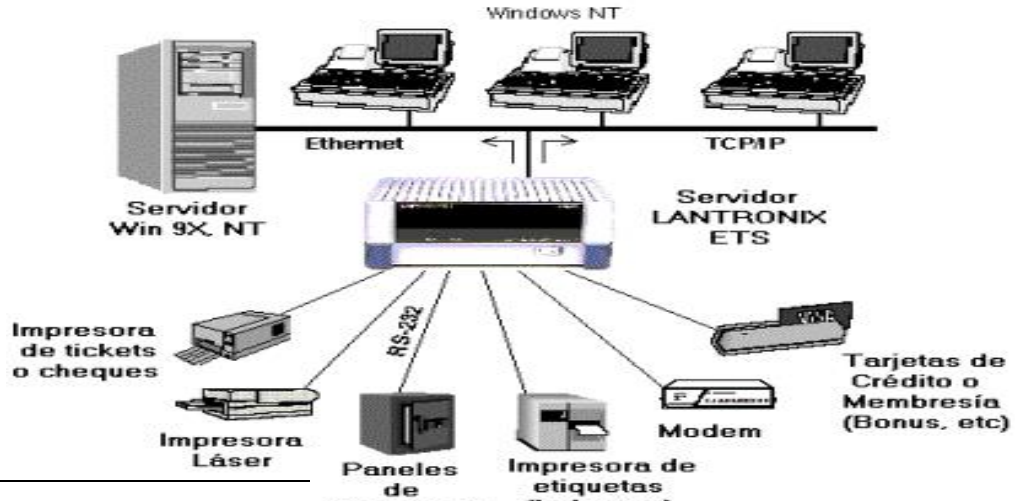
Gráfico 3: Capa de Red del Modelo OSI[13]



El objetivo es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan en caminadores, router, enrutadores. En esta capa se habla de IP[14], IPX,AppleTalk, NetBEUI, etc.[15]

1.1.4.2.4 Capa de transporte

Gráfico 4: Capa de Transporte del Modelo OSI[16]



[13]**Gráfico 3:** Capa de Red del Modelo OSI. http://construiryadministrarredcb7716antonia.blogspot.com/2011/05/modelo-osi-y-sus-siete-capas.htm

[14]**IP:**Internet Protocolo (Protocolo de Internet)

[15]**NetBEUI:** Es un protocolo de nivel de red sin encaminamiento y bastante sencillo utilizado como una de las capas en las primeras redes de Microsoft.

[16] **Gráfico 4:** Capa de Trasporte del Modelo OSI.
http://construiryadministrarredcb7716antonia.blogspot.com/2011/05/modelo-osi-y-sus-siete-capas.htm

Efectúa el transporte de los datos de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. Sus protocolos son TCP[17] y UDP[18]; el primero orientado a conexión y el otro sin conexión.

1.1.4.2.5 Capa de sesión

Gráfico 5: Capa de Sesión del Modelo OSI[19]

Permite que los usuarios de diferentes maquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que esta proporciona y que se utilizan en algunas aplicaciones.Ejemplo: NetBIOS, SQL, RPC

[17]TCP (Transmisión Control Protocol): Orientado a las comunicaciones y ofrece una transmisión de datos confiable.
[18]UDP (UserDatagramProtocol): Está destinado a aquellas comunicaciones que se realizan sin conexión y que no cuentan con mecanismos para transmitir datagramas.
[19]**Gráfico 5:** Capa de Sesión del Modelo OSI. http://construiryadministrarredcb7716antonia.blogspot.com/2011/05/modelo-osi-y-sus-siete-capas.htm

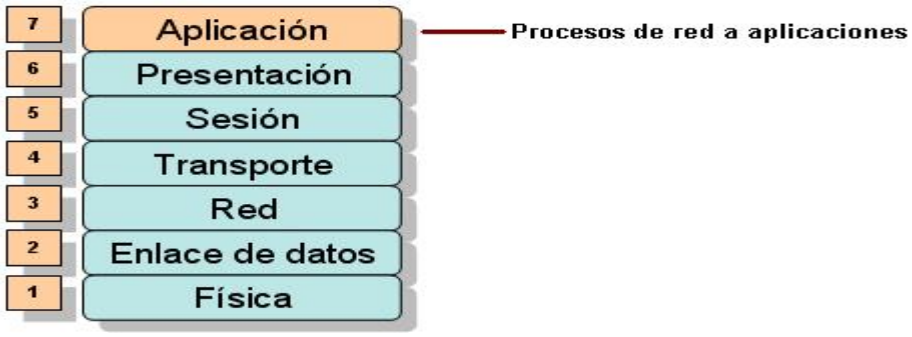
1.1.4.2.6 Capa de presentación

Gráfico 6: Capa Presentación del Modelo OSI[20]

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. Ejemplos:MP3, MPG, GIF, XML[21], etc.

1.1.4.2.7 Capa de aplicación

Gráfico 7: Capa Aplicación del Modelo OSI[22]



[20]**Gráfico 6:** Capa de Presentación del Modelo OSI. http://construiryadministrarredcb7716antonia.blogspot.com/2011/05/modelo-osi-y-sus-siete-capas.htm

[21]**XML:** eXtensibleMarkupLanguage / Lenguaje de Marcas eXtensible') Es un sistema estándar de codificación de información.

[22]**Gráfico 7:** Capa de Aplicación del Modelo OSI. http://construiryadministrarredcb7716antonia.blogspot.com/2011/05/modelo-osi-y-sus-siete-capas.htm

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros (FTP[23]), etc. Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación.

Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. En esta capa se incluyen tecnologías tales como http, DNS[24], SMTP[25], SSH, Telnet[26], etc.[27]

1.2 SEGURIDAD INFORMÁTICA

1.2.1 Que es la Seguridad Informática

Desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de manera alarmante.

La protección de la información tiene que ser una de las prioridades de cualquier departamento de TI. Sin embargo, las organizaciones no se están protegiendo de la manera adecuada,pocas organizaciones usan tecnologías verdaderamente eficientes para protegerse contra las amenazas

[23] **PDF:** Protocolo de Transferencia de Archivos (File Transfer Protocol)
[24] **DNS:** Sistema de Nombres de Dominio (DomainNameSystem)
[25] **SMTP:** Simple Mail Transfer Protocol
[26] **Telnet:** Telecommunication Network. Se trata del nombre de un protocolo de red que se utiliza para acceder a una computadora y manejarla de forma remota.
[27] Ing. Iver Claros. Universidad Privada Cumbre. Modelo OSI. http://belarmino.galeon.com/

informáticas.Al no tener las medidas adecuadas, las compañías se arriesgan a asumir la perdida de la información.

Según, el estándar para la seguridad de la información ISO/IEC 27001[28], que fue aprobado y publicado en octubre de 2005 por la International OrganizationforStandardization (ISO) y por la comisión International ElectrotechnicalCommission (IEC).“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.”

Los tres principales elementos a proteger de cualquier sistema informático son:El hardware, El software, Los datos.[29]

Siendo el principal, los datos, ya que es el amenazado ymás difícil de recuperar, si la máquina se rompe, se puede comprar otra. Si un programa deja de funcionar, se volver a instalar, sin embargo, los datos (documentos,fotos,trabajos,etc.) sólo se pueden recuperarse si previamente se ha hecho alguna copia de seguridad, de locontrario, se pueden perder.[30]

[28]**ISO/IEC 27001** es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005

[29]Elvira Mifsud. (2012). Seguridad Informática. http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

[30]Elvira Mifsud. (2012). Seguridad Informática. http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

1.2.2 Bases de la Seguridad Informática

Para la mayoría de los expertos no existe un sistema 100% seguro. En general, un sistema será seguro o fiable, si se garantiza tres aspectos:

- Confidencialidad: acceso a la información solo mediante autorización y de forma controlada.
- Integridad: modificación de la información solo mediante autorización.
- Disponibilidad: la información del sistema debe permanecer accesible mediante autorización.

Gráfico 8: Base de La Seguridad Informatica[31]

1.2.2.1 Confidencialidad

El objetivo de la confidencialidad es, prevenir la divulgación no autorizada de la información.Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos, para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.[32]

[31]Gráfico 8: Base de la Seguridad Informática, Realizado por: Jhonny Vaca
[32]Elvira Mifsud. (2012). Seguridad Informática. http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

1.2.2.2 Integridad

El objetivo de la integridad es, prevenir modificaciones no autorizadas de la información.La integridad hace referencia a:

- la integridad de los datos (el volumen de la información)
- la integridad del origen (la fuente de los datos, llamada autenticación)

Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

1.2.2.3 Disponibilidad

El objetivo de la disponibilidad es,prevenir interrupciones no autorizadas/controladas de los recursos informáticos. Un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados.

En ambientes bancarios es prioritaria siempre la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer el saldo de otro usuario a que pueda modificarlo.[33]

[33]Elvira Mifsud. (2012). Seguridad Informática. http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

1.2.3 Seguridad Física

1.2.3.1 Amenazas Físicas

Son cualquier error o daño en el hardware, se puede presentar en cualquier momento. Ejemplo, daños en discos, en procesadores, memoria, etc.

1.2.3.2 Desastres Naturales

Los desastres naturales pueden tener graves consecuencias, sobre todo si no se contempla en nuestra política de seguridad y su implantación.

1.2.3.3 Desastres del Entorno

- Acciones naturales: incendio, inundación, condiciones climatológicas, instalaciones eléctricas, ergometría.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.[34]

1.2.3.4 Acciones Hostiles

- Robo:Las computadoras están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero.
- Fraude: Cada año, millones de dólares son sustraídos de empresas y las computadoras son utilizadas como instrumento para dichos fines.
- Sabotaje: Este puede ser un empleado o un sujeto ajeno a la propia empresa.[35]

[34]Elvira Mifsud. (2012). Observatorio Tecnológico. Amenazas en la Red. http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=5

[35] http://www.segu-info.com.ar/fisica/seguridadfisica.htm

1.2.3.5 Control de Accesos

- Utilización de Guardias
- Utilización de Detectores de Metales
- Utilización de Sistemas Biométricos
- Verificación Automática de Firmas (VAF)
- Protección Electrónica[36]

1.2.4 Seguridad Lógica

La mayoría de losdaños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información almacenada y procesada, por lo tanto deben existir técnicas, más allá de la seguridad física que la asegure, estas técnicas lasbrinda la Seguridad Lógica.

El punto más débil de un sistema informático son las personasrelacionadas en mayor o menor medida con él. Entre estos ataquesencontramos:

- Ingeniería social: consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
- ShoulderSurfing: consiste en "espiar" físicamente a los usuarios para obtener generalmente claves de acceso al sistema.
- Basureo: consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo.

[36]UERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open PublicationLicense v.10 o Later. 2 de Octubre de 2000

- Actos delictivos: son actos tipificados claramente como delitos por las leyes, como el chantaje, el soborno o la amenaza.
- Atacante interno: la mayor amenaza procede de personas que han trabajado o trabajan con los sistemas.
- Atacante externo: suplanta la identidad de un usuario legítimo, hasta conseguir un control total de un recurso. [37]

1.2.4.1 Amenazas lógicas

Comprenden una serie de programas que pueden dañar el sistema informático. Estos programas son creados de forma intencionada para hacer daño: software malicioso o malware[38], por error: bugs o agujeros.

1.2.4.1.1 Software Incorrecto

Son errores de programación (bugs).

1.2.4.1.2 Exploits

Son los programas que aprovechan una vulnerabilidad del sistema.

1.2.4.1.3 Bombas Lógicas

Es un código que no se ejecutan hasta que se cumple una condición.

1.2.4.1.4 Virus

Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), ycuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.

[37] ANONYMOUS *Maximun Security* 4rd. Edition U.S.A. Sams Publishing, 2003.
[38] **Malware:** Tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario

1.2.4.1.5 Gusanos

Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, y puede llevar virus.

1.2.4.1.6 Caballos de Troya

Son instrucciones incluidas en un programa que simulan realizar tareas, pero en realidad ejecutan funciones para ocultar la presencia de un atacante.

1.2.4.1.7 Spyware

Programas espía que recopila información sobre una persona u organización sin su conocimiento. La información puede ser vendida empresas publicitarias.

1.2.4.1.8 Adware

Programas que abren ventanas emergentes de publicidad sobre productos y servicios. Normalmente el usuario es consciente de ello y da su permiso.

1.2.4.1.9 Spam

Recepción de mensajes no solicitados. Se suele utilizar esta técnica en los correos electrónicos, mensajería instantánea y mensajes a móviles.

1.2.4.1.10 Técnicas Salami

Robo automatizado de pequeñas cantidades de dinero de una gran cantidad origen. Es muy difícil su detección.[39][40]

[39] Gómez Vieites, Álvaro, *Enciclopedia de la Seguridad Informática Primera edición,* México,Alfaomega Grupo Editor, 2007.

1.3 ATAQUES Y VULNERABILIDADES DE LAS REDES

1.3.1 Tipos de Ataques en las redes

1.3.1.1 Ataque de Escaneo

Se realizan para la recopilación de información sobre posibles puertos de acceso a la red y posteriormente acceder a los recursos a través de ellos.

1.3.1.1.1 Escaneo TCP

Sielpuertoestáescuchando,devolveráunarespuestadeéxito; cualquier otro casosignificaráque el puerto noestáabierto.[41]

1.3.1.1.2 Ataque Snnifing

Sólo recopila y almacena la información que circula por la red.ActualmenteexistenSniffersparacapturarcualquiertipodeinformaciónespecífica.

1.3.1.1.3 Snooping-Downloading

Aquí,además deinterceptareltráficodered,elatacanteingresaalosdocumentos,y otrainformaciónguardada,realizandounacopiadedocumentosdeesainformación asupropiacomputadora.

1.3.1.2 Ataques de Autentificación

Estetipodeataquetienecomoobjetivoengañaralsistemadelavíctimaparaingresa

[40]Elvira Mifsud. (2012). Observatorio Tecnológico. Amenazas en la Red. http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=5

[41]J. Erickson, Hacking: The Art of Exploitation, No Starch Press, 2003.

ralmismo,tomandosesionesyaestablecidasporlavíctima.

1.3.1.2.1 Spoofing-Looping

Spoofingpuedetraducirsecomo"hacersepasarporotro"yelobjetivodeestatécnica,justamente,esactuaren nombredeotrosusuarios.

1.3.1.2.2 IP Spoofing

Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.

1.3.1.2.3 DNS Spoofing

EsteataqueseconsiguemediantelamanipulacióndepaquetesUDPpudiéndosecomprometerel servidor de nombresdedominios.[42]

1.3.1.2.4 Web Spoofing

El atacantecreaunsitiowebcompleto(falso)similaralquelavíctimadeseaentrar y el accesos está monitoreadoporelatacante.

1.3.1.2.5 IP Splicing-Hijacking

Es cuando un atacante consigue interceptaruna sesión yaestablecida.

1.3.1.2.6 Utilización de BackDoors o Puertas Traseras

Sontrozosdecódigoenunprogramaquepermitensaltarselosmétodosusualesde autentificaciónpararealizarciertastareas.

1.3.1.2.7 Utilización de Exploits

Estosprogramasaprovecharladebilidad,fallooerrorenelsistema(hardwareosoft

[42]K. Kaspersky, Hacker Disassembling Uncovered, A-LIST Publishing, 2003.

ware)paraingresaralmismo.

1.3.1.2.8 Obtención de Passwords con Diccionarios

Son ataquessistemáticosconlaayudadeprogramasydiccionariosquepruebanmillonesde posiblesclaveshastaencontrarlaclavecorrecta.

1.3.1.3 Ataques de Modificación-Daño

Este tipo de ataques son los más peligrosos porque actúan sobre los datos o los programas instalados, modificando o borrando los archivos.

1.3.1.3.1 Borrado de Huellas

Esunadelastareasmásimportantesquedeberealizarelintrusodespuésdeingresaral sistema,yaquesisedetectasuingresoeladministradortaparáelhuecodeseguridad para evitarataquesfuturos.LasHuellassontodaslastareasquerealizóelintrusoenel sistemaysonalmacenadasenLogs.LosarchivosLogssonelprincipalenemigo del atacante.[43]

1.3.1.4 Otros Ataques

1.3.1.4.1 Ataques de intromisión

Este tipo de ataque es cuando alguien abre archivos, en nuestra computadora, uno tras otro hasta encontrar algo que le sea de su interés.

[43] J. Long, Google Hacking for Penetration Testers, Syngress, 2005.

1.3.1.4.2 Ataque de Intercepción

Se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivosde cualquier flujo en una red.

1.3.1.4.3 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.

1.3.1.4.4 Ataques de Denegación de Servicios

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.[44]

1.3.2 Intrusos Informáticos

Al Inicio de la informática y con los avances tecnológicos, han ido apareciendo personajes que difunden el miedo en la Red y/o cualquier sistema de cómputo.Todos ellos son catalogados como "piratas informáticos",la nueva generación de "rebeldes "de la tecnología, los piratas se presentan con un cerebro desarrollado y con muy pocas armas: una simple computadora, una conexión a internet. Unos difunden sabiduría y enseñanza, otros, destrucción. Hay que saber bien quien es cada uno de ellos y catalogarlos según sus actos de rebeldía en la mayoría de los casos.

1.3.2.1 Hackers

[44]Nicolas Arrellano. 2012. ipos de Ataques en Redes Informaticas. http://seguridadenlasredescomputacionales.blogspot.com/2012/05/tipos-de-ataques-en-redes-informaticas_15.html

Son intrusos informáticos que se dedican a estas tareas como pasatiempo entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos. Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno.

1.3.2.2 Crackers (Blackhats)

Los crackers son intrusos informáticos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o para provocar algún daño en el sistema o red. En 1985 se separa al cracker del hacker.

1.3.2.3 Sniffers

Son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.

1.3.2.4 Phreakers

Son conocidos por sus conocimientos en telefonía,para poder realizar llamadas gratuitas.[45]

1.3.2.5 Spammers

Son los responsables del envío masivo de miles de correoselectrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.Estos mensajes de correo pueden contener código dañino.

[45]Dr. Santiago Acurio Del Pino. 2010. Pontificia Universidad Católica del Ecuador. Los Delitos Informáticos en el Ecuador

1.3.2.6 Piratas Informáticos

Son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

1.3.2.7 Creadores de Virus y Programas Dañinos

Son expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos.Desarrollan virus con unaclara actividad delictiva.

1.3.2.8 Lamers (Wannabes), (Scriptkiddies) o (Click-kiddies)

Son aquellas personas que han obtenido o descargado determinados programas y herramientas para realizar ataques informáticos,los utilizan sin tener conocimientos técnicos de cómo funcionan.

1.3.2.9 Amenazas del Personal Interno

Son empleados que actúan como “fisgones” en la red de su organización, los empleados desleales que pretenden causar algún daño a la organización.

1.3.2.10 Ex-empleados

Ellos pueden actuar contra su antigua empresa por despecho o venganza, accediendo en algunos casos a través de cuentas de usuario que todavía no han sido canceladas en los equipos y servidores de la organización.[46]

1.3.3 Motivación de los Intrusos informáticos

1.3.3.1 Técnicas

[46]Dr. Santiago Acurio Del Pino. 2010. Pontificia Universidad Católica del Ecuador. Los Delitos Informáticos en el Ecuador

El fin perseguido es demostrar las fallas de los sistemasque, según ellos, fueron dejadas intencionalmente. Ayudan al progreso de la tecnología, forzando a la industria tecnológica a mejorar sus productos.

1.3.3.2 Económicas

Llevar a cabo operaciones fraudulentas; robo de información confidencial que posteriormente es vendida a terceros.

1.3.3.3 Gubernamentales

Causados por un gobierno contra otro. Se llama InformationWarfare.

1.3.3.4 Diversión

Algunos usuarios de Internet realizan estos ataques como una forma de pasar el rato delante de su ordenador.

1.3.3.5 Ideología

Ataques realizados contra determinadas organizaciones, empresas y Websites gubernamentales, con un contenido claramente político.

1.3.3.6 Autorrealización

Comprende a aquellos que al cumplir el objetivo del ataque, sienten satisfacción por el logro alcanzado.

1.3.3.7 Reconocimiento Social

Comprende a aquellos que buscan un reconocimiento social y de un cierto estatus dentro de una comunidad de usuarios[47]

[47]Dr. Santiago Acurio Del Pino. 2010. Pontificia Universidad Católica del Ecuador. Los Delitos Informáticos en el Ecuador

1.3.4 Triangulo de la Intrusión

Para poder llevar a cabo un ataque informático es necesario que exista en el atacante o intruso una MOTIVACIÓN, una OPORTUNIDAD y LOSMEDIOS NECESARIOS (Motivation, Opportunity, Means, según sus siglas eninglés), por lo tanto, cualquier situación que propicie alguna de estas tresvariables será de potencial éxito para el atacante. Estos tres factores constituyen lo que podríamos denominar como el "Triángulo de la Intrusión", concepto que se presenta de forma gráfica en la siguiente figura:

Gráfico 9: Triangulo de la Intrusión[48]

[48] Gráfico 9: Del Documento: Dr. Santiago Acurio Del Pino. 2010. Pontificia Universidad Católica del Ecuador. Los Delitos Informáticos en el Ecuador

CAPÍTULO II

Herramientas de Honeynet Virtuales para analizar el comportamiento de los atacantes a las redes

2.1 HONEYPOTS

2.1.1 Introducción

Los ataques a través de Internet siguen aumentando cada año y la complejidad de los métodos empleados por los atacantes ha ido creciendo paralelamente, al igual que las herramientas que emplean para disimular sus acciones en los equipos una vez que han conseguido acceso al sistema.

Lance Spitzner, consultor y analista informático experto en seguridad, construyó a comienzos del año 2000 una red de seis ordenadores en su propia casa. Esta red la diseñó para estudiar el comportamiento y formas de actuación de los atacantes. Fue de los primeros investigadores en adoptar la idea, y hoy es uno de los mayores expertos en honeypots.

Su sistema estuvo durante casi un año de prueba, desde abril del 2000 a febrero de 2001, guardando toda la información que se generaba. Los resultados hablaban por sí solos, en los momentos de mayor intensidad de los ataques, comprobaba que las vías de acceso más comunes a los equipos de su casa eran escaneadas, desde el exterior de su red, hasta 14

veces al día, utilizando herramientas de ataque automatizadas.[49]

En los últimos años se ha empezado a utilizar honeypots como un mecanismo de seguridad en la red; estos sirven para detectar cuándo se ha producido una intrusión y analizar en profundidad las acciones realizadas por los atacantes.

Estos sistemas simulan hacia el exterior equipos vulnerables que al ser atacados,permiten a los administradores observar las acciones realizadas por los atacantes,pudiendo de esta forma analizarlas.

2.1.2 Definición de los Honeypots

Honeypots es una expresión inglesa que se traduce como “Tarros de miel”. Se denomina honeypot al software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques.

Los honeypots, que alguna vez fueron utilizados principalmente por los investigadores como una forma de atraer a los hackers a un sistema de redes para estudiar sus movimientos y comportamiento, están adquiriendo una importancia cada vez mayor en la seguridad empresarial. En efecto, al brindar detección temprana de actividad no autorizada en las redes, los honeypots son ahora más útiles que nunca para los profesionales de seguridad de TI.

[49] INTECO (Instituto Nacional de Tecnología de la Comunicación), 2009, Honeypots Monitorizando a los Atacantes

Los Honeypots en su forma más básica son servidores de información falsos, posicionados estratégicamente en una red de prueba, los cuales son alimentados con información falsa que es disfrazada como archivos de naturaleza confidencial. A su vez, estos servidores son configurados inicialmente de manera que sea difícil, pero no imposible el hecho de ser penetrados por un atacante informático, exponiéndolos de manera deliberada y haciéndolos altamente atractivos para un "Intruso Informático" en busca de un blanco. El servidor es habilitado con herramientas de monitoreo y rastreo de información, de manera que cada paso y rastro de actividad de un "Intruso Informático" pueda ser registrado en una bitácora que indique esos movimientos de manera detallada.[50]

Los honeypots pueden ayudar a prevenir ataques en varias formas. Estos ataques son basados en herramientas que aleatoriamente escanean redes enteras buscando sistemas vulnerables. Si un sistema vulnerable es encontrado, estas herramientas automatizadas atacarán y tomarán el sistema. Cuando los sistemas son escaneados, estos honeypots interactúan con él y disminuyen la velocidad del ataque.

Protección contra intrusos humanos se conoce como engaño o disuasión. La idea de esta contramedida es confundir al atacante y hacerle perder tiempo y recursos mientras interactúa con el Honeypot. Mientras ese proceso se lleva

[50]2008, Que son los honeypots, http://www.zonavirus.com/articulos/que-son-los-honeypots.asp

a cabo, se puede detectar la actividad del atacante y se tiene tiempo para reaccionar y detener el ataque.[51]

Labor Ciber-Forense:Una vez que un administrador de red se da cuenta que uno(s) de sus servidores fueron comprometidos ilegalmente, es necesario proceder inmediatamente a realizar un análisis forense en el sistema comprometido para realizar un control de daños causados por el atacante. Sin embargo hay dos problemas que afectan a la respuesta al incidente: a menudo los sistemas comprometidos no pueden ser desconectados de la red para ser analizados, como el servidor mail de una organización, esto reduce la habilidad para analizar qué sucedió, cuánto daño hizo el atacante, e incluso si el atacante accedió a otros sistemas de la red. El otro problema es que en el caso de que se desconecte, hay tanta polución de datos que es muy difícil determinar qué es lo que hizo el "Intruso Informático".

Los Honeypots pueden ayudar a solventar ambos problemas. Honeypots son una excelente herramienta de incidencias ya que pueden rápidamente y fácilmente ser sacados de la red para un análisis forense completo, sin el impacto en las operaciones empresariales de todos los días. Recuerden que la única actividad que guardan los honeypots son las relacionadas con el atacante, ya que no las utilizan nadie, excepto de señuelo para los atacantes.[52]

[51] Mauro Maulini, 2010, Que es un Honeypot, http://www.e-securing.com/novedad.aspx?id=66
[52] 2010, Honeypot Seguridad Informática, http://www.cybsec.com/upload/ESPE_Honeypots.pdf

2.1.3 Clasificación de los Honeypots

2.1.3.1 Ambiente de Implementación

2.1.3.1.1 Honeypots para la Producción

Son aquellos que se utilizan para proteger a las organizaciones en ambientes reales de operación. Se implementan de manera colateral a las redes de datos o infraestructuras de TIs y están sujetas a ataques (24/7).

El objetivo que se pretende es la obtención de información sobre las técnicas empleadas para tratar de vulnerar los sistemas que componen dicha infraestructura.

El mayor inconveniente que supone esta elección es el peligro que supone para los sistemas organizativos el permitir (incluso provocar) que el tráfico malintencionado conviva con el legítimo.

2.1.3.1.2 Honeypots para la Investigación

Estos Honeypots no son implementados con la finalidad de proteger redes, sinoque constituyen recursos educativos de naturaleza demostrativa y de investigación cuyo objetivo se centra en estudiar patrones de ataque y amenazasde todo tipo. Gran parte de la atención actual se centra en los Honeypots para la investigación, que se utilizan para recolectar información sobre las acciones de los intrusos.[53]

[53] Alberto Segovia, 2010, Honeypots, http://www.securityartwork.es/2010/04/30/honeypots-ii-para-aprender-perder%E2%80%A6-o-no/

2.1.3.2 Nivel de Interacción

2.1.3.2.1 Baja Interacción

La actividad del atacante se encuentra limitada al nivel deemulación del Honeypot. La ventaja de un Honeypot de Baja Interacción radicaprincipalmente en su simplicidad, ya que estos tienden a ser fáciles de utilizar ymantener con un riesgo mínimo.

La principal desventaja de los Honeypots de Baja Interacción radica en queregistran únicamente información limitada, ya que están diseñados para capturaractividad predeterminada. Debido a que los servicios emulados solo puedenllegar hasta un cierto límite operacional, ésa característica limita la gama deopciones que se pueden anunciar hacia el potencial intruso.[54]

2.1.3.2.2 Alta Interacción

Este tipo de Honeypots constituyen una solución compleja, ya que implica lautilización de sistemas operativos y aplicaciones reales montados en hardwarereal sin la utilización de software de emulación e involucrando aplicaciones realesque se ejecutan de manera normal, muchas veces en directa relación a servicioscomo bases de datos y directorios de archivos compartidos. Por ejemplo:Si se desea implementar un Honeypot sobre un servidor Linux que ejecute unservidor FTP, se tendrá que construir un verdadero sistema Linux y montar unverdadero servidor FTP.

[54] Alberto Segovia, 2010, Honeypots, http://www.securityartwork.es/2010/04/30/honeypots-ii-para-aprender-perder%E2%80%A6-o-no/

Las ventajas es quetiene la posibilidad decapturar grandes cantidades de información referentes al modus operandi de losatacantes debido a que los intrusos seencuentran interactuando frente a unsistema real. De esta manera, se está en posibilidad de estudiar la extensióncompleta de sus actividades. Hoy por hoy, el mejorejemplo de un Honeypot de alta interacción está representado en las Honeynets.[55]

2.1.4 Ventajas y Desventajas de los Honetpots

2.1.4.1 Ventajas

- Nuevas herramientas y tácticas: Los honeypots son diseñados para capturar cualquier cosa que interactúa con él, incluyendo herramientas o tácticas nunca vistas.
- Mínimos recursos: Los honeypots requieren mínimos recursos, sólo capturan actividad irregular. Es decir que un viejo Pentium con 128 mb de RAM puede manejar fácilmente un honeypot.
- Cifrado o IPv6[56]: A diferencia de la mayoría de las tecnologías para la seguridad, como los IDS, honeypots trabajan bien en entornos cifrados como IPv6. No importa lo que los "Intrusos Informáticos" lancen hacia el honeypot, el honeypot lo detectará y lo capturará.

[55] Alberto Segovia, 2010, Honeypots, http://www.securityartwork.es/2010/04/30/honeypots-ii-para-aprender-perder%E2%80%A6-o-no/

[56] IPv6: Protocolo de Internet versión 6) es una versión del protocolo Internet Protocol (IP), diseñada para reemplazar a Internet Protocol versión 4, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

- Simplicidad: Los honeypots son conceptualmente simples. No hay por qué desarrollar algoritmos raros, ni complejas tablas que mantener, o firmas que actualizar. Mientras más simple sea la tecnología, menos posibilidades de errores o des configuraciones habrá.
- Este tipo de sistemas sirven tanto para posibles atacantes internos como externos.
- Desvían la atención del atacante de la red real del sistema, de manera que no se comprometan los recursos principales de información.
- Forman perfiles de atacantes y sus métodos de ataque preferidos, de manera similar a la usada por una corporación policiaca para construir el archivo de un criminal basado en su modus operandi.

2.1.4.2 Desventajas

- Como en cualquier otra tecnología, los honeypots también tienen su debilidad. Esto es debido a que no reemplaza a la actual tecnología, sino que trabaja con las existentes.
- Visión Limitada: Los honeypots pueden sólo rastrear y capturar actividad que interactúen directamente con ellos. Los Honeypots no podrán capturar ataques a otros sistemas vecinos, al menos que el atacante o la amenaza interactúe con el honeypot al mismo tiempo.

- Riesgo: Todas las tecnologías de seguridad tienen un riesgo. Los firewalls tienen el riesgo de que sean penetrados, el cifrado tiene el riesgo de que sean rotos, sensores IDS tienen el riesgo de que fallen al detectar ataques. Los honeypots tienen el riesgo de que sean apoderados y controlados por los "Intrusos Informáticos" y que lo utilicen para dañar otros sistemas.[57]

2.2 HONEYNETS

2.2.1 Definición de Honeynet

La idea de Honeypot (Red Trampa), fue adoptada por TheHoneynet Project[58]; una organización no lucrativa, fundadapor Lance Spitzner. Este grupo está compuesto por expertos en seguridad, cuyo objetivoes aprender las herramientas, tácticas y motivos de los atacantes.

Una Honeynet es una herramienta de investigación. Es un tipo de Honeypotqueconsiste en una red diseñada para ser comprometida por intrusos. Sirve para estudiar lastécnicas utilizadas por los intrusos que han comprometido laseguridad de la red. Elobjetivo principal es conocer al enemigo, aprender de él, en definitiva es una herramientadiseñada con propósitos académicos.

Una Honeynet no es un sistema solitario, sino una red. Esta red puede estarcompuesta por distintos sistemas trampa, tales como Linux, Windows,

[57] 2010, Honeypot Seguridad Informática, http://www.cybsec.com/upload/ESPE_Honeypots.pdf

[58] **TheHoneynet Project:** Es una organización de investigación no lucrativa dedicada al aprendizaje de las herramientas, tácticas y motivos de la comunidad blackhat y a compartir las lecciones aprendidas.

Solaris,routers, conmutadores, etc. El hecho de proporcionar un entorno de red aporta unambiente más creíble, más real desde el punto de vista del intruso, del atacantede la red. Un entorno de sistemas heterogéneos permite además, captar laatención de más intrusos, algunos de los cuales están especializados en atacardeterminados sistemas operativos o servicios. Por otra parte, permite aprender unmayor y variado número de tácticas de ataque.

Los Honeynets son herramientas de seguridad con un punto de vista diferente altradicional, que es un comportamiento defensivo, tradicionalmente se intenta defender deataques una red, mediante cortafuegos, medios de cifrado o sistemas de detección deintrusos (IDS). Los Honeynets son herramientas diseñadas básicamente para aprendery adquirir experiencia en el área de seguridad.

Todos los sistemas situados dentro de una Honeynet son sistemas comerciales estándar. Nada es emulado ni se hace nada para que los sistemas sean menos seguros. Los riegos y vulnerabilidades encontradas en una Honeynet son las mismas que existen hoy en muchas organizaciones. Uno simplemente puede tomar un sistema de un entorno comercial y situarlo dentro de una Honeynet. [59]

2.2.2 Funcionamiento de una HoneyNet

[59]Honeynet Project (http://www.honeynet.org), 2003, Conoce a tu Enemigo: Honeynets, http://his.sourceforge.net/honeynet/papers/honeynet/

El punto crucial que asegura el éxito de la honeynet es la creación de un ambienteque permita monitorizar todos y cada uno de los movimientos que el intruso llegue arealizar dentro de ella. Estos movimientos que realiza el intruso son monitorizadosmediante la información que van dejando al utilizar herramientas, mediante las cuales siguen unas tácticas para conseguir algún objetivo que se imponen, es decir las Honeynets una red parecida a una pecera, se puede ver todo lo que ocurre dentro de ella. Igual que a un pez, se puede observar a los hackers interactuar con su entorno virtual. Esta red controlada se convierte en su Honeynet.[60]

Tradicionalmente, el gran problema de los profesionales de la seguridad reside en que la detección y captura de actividad blackhat supone una sobrecarga de información. El reto para muchas organizaciones es determinar de entre una enorme cantidad de información qué es tráfico productivo y qué es actividad maliciosa. Herramientas y técnicas como los Sistemas de Detección de Intrusiones, análisis forenses de las máquinas, o los análisis de los registros del sistema intentan resolver esto mediante una base de datos de marcas conocidas o algoritmos para determinar qué es tráfico de producción y qué es actividad maliciosa. Sin embargo, la sobrecarga de información, la contaminación de los datos, actividades no

[60]Eduardo Gallego, 2009, Madrid-España, Honeynets: Aprendiendo del Atacante, https://web.dit.upm.es/~jlopez/publicaciones/mundointernet04.pdf

descubiertas, falsos positivos y falsos negativos pueden hacer el análisis y la determinación de las actividades algo extremadamente difícil.

Las Honeynets resuelven este problema de la sobrecarga de información a través de la simplicidad. Una Honeynet es una red diseñada para ser comprometida, no para ser usada por tráfico productivo. Así, cualquier tráfico entrando o saliendo de nuestra red es sospechoso por definición. Cualquier conexión iniciada desde fuera de la Honeynet hacia dentro de la red es probablemente algún tipo de sondeo, ataque u otra actividad maliciosa. Cualquier conexión iniciada desde dentro de la Honeynet hacia otra red de fuera indica que un sistema fue comprometido. Un agresor ha iniciado una conexión desde su recién atacada computadora y ahora está saliendo a Internet. Este concepto de ningún tráfico productivo simplifica enormemente la captura de datos y el análisis.[61]

2.2.3 Requisitos de una Honeynet

Para construir su Honeynet de forma satisfactoria, hay dos requisitos críticos; Control de Datos y Captura de Datos. Si hay algún fallo en cualquier requisito, entonces hay un fallo en la Honeynet. Las Honeynets pueden construirse y desarrollarse en cantidad de maneras diferentes, de forma que dos Honeynets nunca son iguales.

2.2.3.1 Control de Datos

[61]Eduardo Gallego, 2009, Madrid-España, Honeynets: Aprendiendo del Atacante, https://web.dit.upm.es/~jlopez/publicaciones/mundointernet04.pdf

Es una actividad de contención. Siempre cabe la posibilidad de que la red trampa sea vulnerada por un atacante o incluso que sea utilizada para realizar desde ella otros ataques a mayor escala. Para mitigar en lo posible este riesgo, es necesario llevar a cabo un correcto control sobre los datos de entrada y salida de la honeynet.

Una de las herramientas fundamentales para realizar un correcto control de datos es un cortafuego. En él se deberá definir claramente el tipo y la cantidad de conexiones que se permite en nuestra red, tanto de salida como de entrada. También deberá estar correctamente especificado el tráfico que permitimos de una parte a otra dentro de la propia red, evitando la posibilidad de que el atacante pueda acceder a la parte de administración de la misma o incluso, si existe, a zonas de la red en producción. Todas estas restricciones deberán estar enfocadas a que el atacante disponga de un cierto grado de libertad para interactuar con loshoneypots, de lo contrario la honeynet no podrá cumplir con su objetivo.

2.2.3.2 La Captura de Datos

Es la captura de todas las actividades que realice el atacante. El reto es capturar tantos datos como sea posible, sin que el atacante sospeche que cada acción está siendo capturada. Además, los datos capturados no pueden guardarse localmente en el honeypot. La información guardada localmente puede ser potencialmente detectada por el atacante, alertándole de que el sistema es una Honeynet y los datos guardados pueden ser

también perdidos o destruidos, por ese motivo, es recomendable que la información capturada se envíe de forma segura a un servidor centralizado (forma remota) para su almacenamiento y análisis. De este modo se tendrá tener un mayor control sobre los datos recogidos, se pueden reaprovechar experiencias y se puede obtener una imagen más clara de la evolución de los diferentes ataques que se encuentran presentes en la red.[62]

2.2.4 Cuidados en una HoneyNet

Como se trata de una red normal, cada vez que recibe un ataque hay que detectarlo y ponerle solución. De no hacerlo la red puede quedar por fuera de servicio durante largo tiempo y deja de cumplir sufunción principal. Igualmente,puede ser utilizada como trampolín para otros ataques.

El mantenimiento constante es requerido para mantener la operatividad de la Honeynet. Sus procesos de alerta terminarán, los discos pueden llenarse, los ficheros de configuración corromperse, los registros del sistema necesitarán ser revisados, los firewall necesitan ser actualizados.

2.2.5 Arquitecturas de una Honeynet

2.2.5.1 Generación I

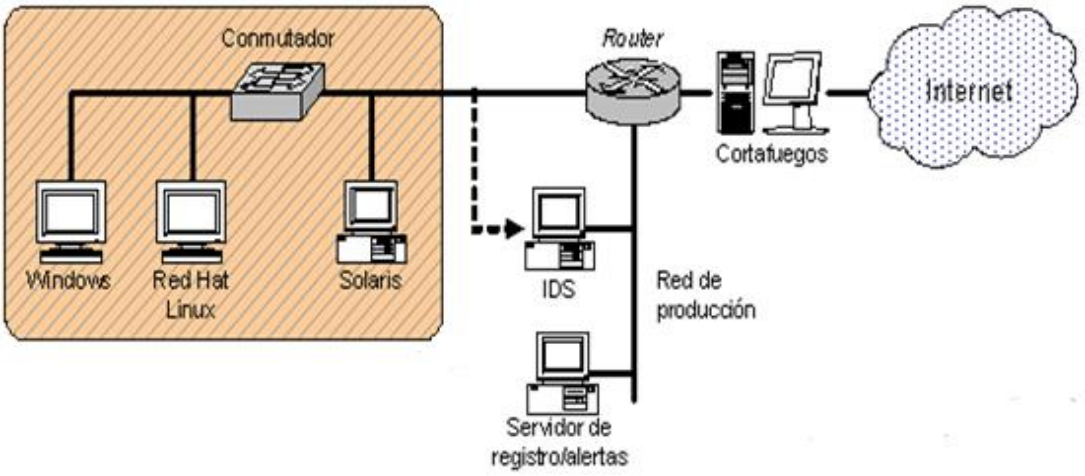
La arquitectura de esta clase de Honeynet se compone de una máquina Gateway (firewall) responsable del control de datos y otra denominada (IDS:

[62]Alberto Segovia, 2010, Honeynets Tareas y Herramientas, http://www.securityartwork.es/2010/07/06/honeynets-iv-tareas-y-herramientas/

Sistema de detección de intrusos) que es responsable de la captura de datos.

Primero se trata de controlar a los agresores, y después capturar sus actividades. El firewall es la principal herramienta para controlar las conexiones entrantes y salientes. El cortafuego se diseña para permitir cualquier conexión entrante, pero controla las conexiones salientes.[63]

Gráfico 10: Arquitectura Honeynet Generación I[64]

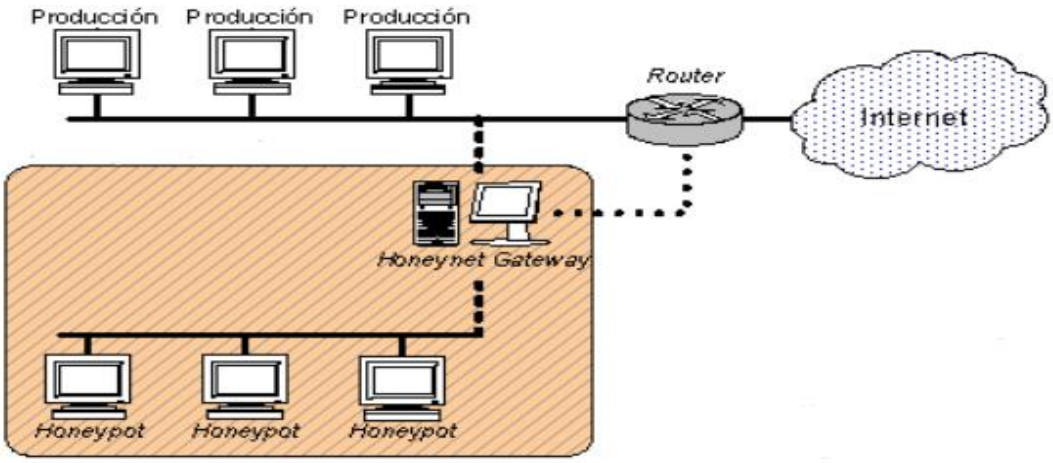


2.2.5.2 Generación II

Con respecto a lastecnologíasGenI, esta arquitectura es más fácil de implementar, más difícil de detectar ytiene un mantenimiento más seguro.[65]

[63]Honeynet Project (http://www.honeynet.org), 2003, Conoce a tu Enemigo: Honeynets, http://his.sourceforge.net/honeynet/papers/honeynet/
[64]**Gráfico 10:** Arquitectura Honeynet Generación I http://www.dgonzalez.net/papers/ids/html/cap04.htm
[65]Honeynet Project (http://www.honeynet.org), 2003, Conoce a tu Enemigo: Honeynets, http://his.sourceforge.net/honeynet/papers/honeynet/

Gráfico 11: Arquitectura HoneynetGeneración II[66]



Como se puede ver en la figura, la primera diferencia con respecto a laarquitectura GEN I es que se utiliza un Honeynet Gateway (Honeywall), que combina los elementos de IDS y cortafuegosque aparecían por separado en la primera generación.El elemento clave de cualquier Honeynet es el gateway (puerta de enlace), que separa los sistemas Honeynet del resto del mundo.Todo el tráfico entrante o saliente de la Honeynet debe pasar a través de este Honeywall. Este elemento es el centro de control de la Honeynet; toda la "magia ocurre aquí.

Las HoneynetsGenII poseen todos los requisitos combinados en un único dispositivo. Esto significa que todo el Control de Datos, Captura y

[66]**Gráfico 11:** Arquitectura HoneynetGeneraciónII, http://www.dgonzalez.net/papers/ids/html/cap04.htm

Recolección se llevará a cabo desde un mismo recurso. Esto hará mucho más fácil el desarrollo y mantenimiento de una Honeynet.[67]

2.2.6 Honeynet Virtuales

Otra área en la que el Honeynet Project está investigando es en el uso de Honeynets virtuales. Las Honeynets Virtuales combinan todos los elementos de una Honeynet en un único sistema físico. No sólo se reúnen los tres requisitos de Control de Datos, Captura de Datos y Recolección de Datos, sino que los propios honeypots se ejecutan en un único sistema. Las Honeynets Virtuales soportan tecnologías GenI y GenII. Ahora los honeypots son realmente sistemas operativos. Nada es emulado.

La aparición de herramientas de emulación y soporte virtual han hecho posible este modelo de implementación de honeynets. Este enfoque consiste en crear una honeynet completa en un sólo equipo físico. Una Honeynet virtual no es una arquitectura, sino una forma de implementarlas; y se puede utilizar para crear tanto, arquitecturas tipo GenI como GenII.

Una Honeynet Virtual coge la tecnología de una Honeynet y la combina en un único sistema. Esto las hace más baratas de construir, más fáciles de implantar, y más simples de mantener. Sin embargo, también tienen desventajas comunes, incluyendo un único punto de fallo y limitaciones con

[67]Federación de Enseñanza de Andalucia, 2009, Honeynet Una desconocida en la Seguridad Informática,http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf

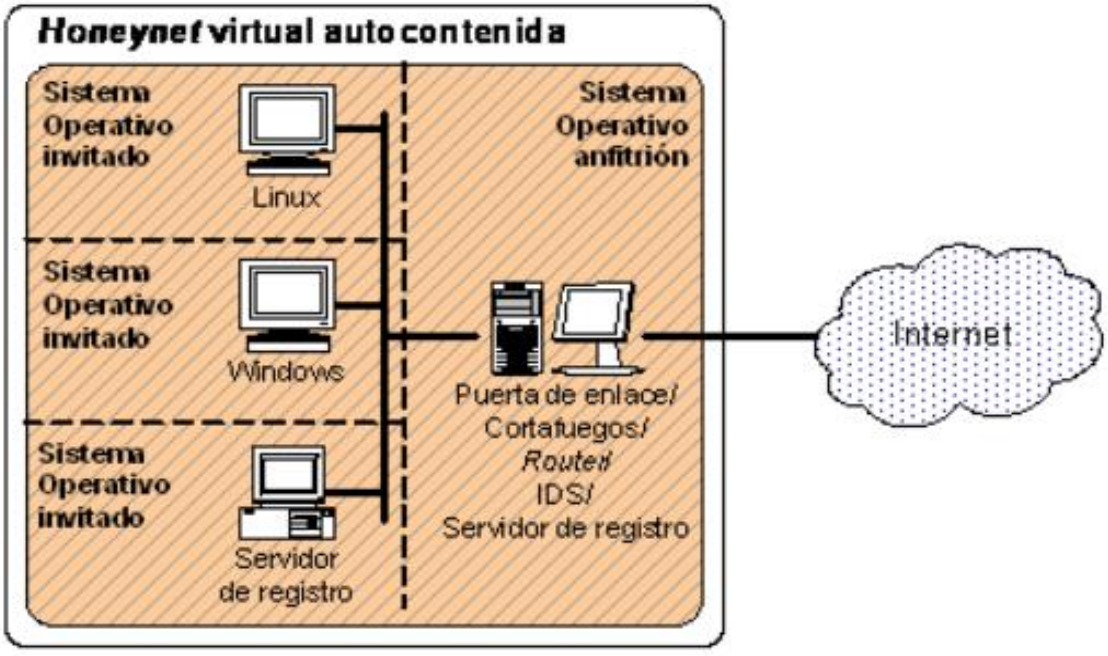
el hardware y el software virtual. Una Honeynet virtual puede ser Auto contenida o Híbrida, como se detallarán a continuación cada una de ellas.[68]

2.2.6.1 Tipos de Honeynet Virtual

2.2.6.1.1 Honeynet Virtual Auto contenida

La honeynet virtual auto contenida engloba a una honeynet en un solo equipo. Lared entera está virtualmente contenida en un único y físico sistema. Una red Honeynettípicamente consiste de un firewall para Control de Datos y Captura de Datos, y loshoneypots dentro de la Honeynet. Un esquema de esta clase de honeynet sería la quemuestra la figura que aparece a continuación.

Gráfico 12: Arquitectura Honeynet Virtual Auto contenida[69]



[68] Honeynet Project (http://www.honeynet.org), 2003, Conoce a tu Enemigo: Definiendo Honeynet Virtuales, http://his.sourceforge.net/honeynet/papers/honeynet/

[69] Gráfico 12: Arquitectura Honeynet Virtual Auto contenida http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf

2.2.6.1.1.1 Las ventajas

- Fácilmente transportable, especialmente si se instala en un portátil.
- Rápida puesta en funcionamiento. Una vez instalada, sólo hay que conectarlaa la red y configurarla en pocos minutos.
- Es barata y ocupa poco espacio. Sólo nos hace falta un ordenador.

2.2.6.1.1.2 Las desventajas

- Si falla el hardware, la Honeynet entera podría dejar de funcionar.
- Necesidad de un ordenador de altas prestaciones. Aunque sólo requiere unordenador, tiene que tener suficiente memoria y capacidad de procesador.
- Seguridad. Como todos los sistemas comparte el mismo hardware, puede queun atacante acceda a otras partes del sistema. Tiene mucha dependencia delsoftware virtual.
- 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 unsistema operativo de cisco en una máquina con un procesador de Intel.[70]

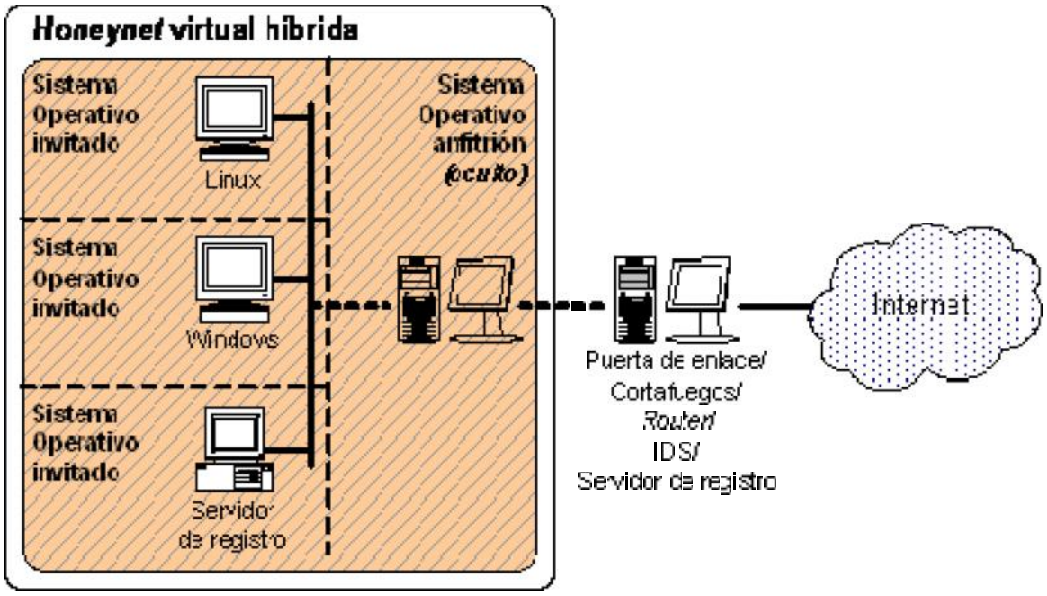
2.2.6.1.2 Honeynet virtual híbrida

Este tipo de Honeynets es una combinación de las Honeynets clásicas y de las de software de virtualización. El honeywall es el responsable de la

[70]Honeynet Project (http://www.honeynet.org), 2003, Conoce a tu Enemigo: Definiendo Honeynet Virtuales, http://his.sourceforge.net/honeynet/papers/honeynet/

captura y control de los datos, siendo éste un sistema separado y aislado, lo que reduce el riesgo de compromiso. Sin embargo todos los honeypots corren sobre una única máquina física

Gráfico 13: Arquitectura Honeynet Virtual Hibrida[71]



2.2.6.1.2.1 Ventajas

- Seguridad: eliminan el punto único de fallo y aíslan los datos yel control en otro dispositivo.
- Flexible: se tiene un dispositivo que contienen diferentes tiposdeHoneypot que son máquinas virtuales, las cuales puedenser de diferentes tipos con diferentes servicios, fáciles decopiar, borrar, duplicar, lo que facilita enormemente en la tareade administración. Si

[71] **Gráfico 13:** Arquitectura Honeynet Virtual Hibrida
http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf

se daña un Honeypot sólo hay quelevantar un duplicado ya pre instalado.

2.2.6.1.2.2 Desventajas

- Se dificulta la movilidad: debido a que tenemos dosdispositivos.
- Costosas: se incrementa el costo por hardware y en espacio.Para cualquier tipo de Honeypot o Honeynet Virtual hay queconsiderar que pueden ser usadas técnicas de fingerprinting(obtención del tipo y versión del sistema operativomediante el envío de paquetes IP específicamenteconstruidos) sobre los Honeypots revelándole al atacante lavirtualización de los sistemas.[72]

2.2.6.2 Ventajas y Desventajas de los Honeynet Virtuales

Las ventajas que presentan este tipo de honeynet virtuales son:

- Fácilmente transportable, especialmente si se instala en un portátil.
- Rápida puesta en funcionamiento. Una vez instalada, sólo hay que conectarla a la red y configurarla en pocos minutos.
- Es barata y ocupa poco espacio. Sólo nos hace falta un ordenador.

Las desventajas que presentan este tipo de honeynet virtuales son:

- Si falla el hardware, la Honeynet entera podría dejar de funcionar.

[72]Federación de Enseñanza de Andalucia, 2009, Honeynet Una desconocida en la Seguridad Informática,http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf

- Necesidad de un ordenador de altas prestaciones. Aunque sólo requiere un ordenador, tiene que tener suficiente memoria y capacidad de procesador.
- Las ventajas son coste reducido y más fácil manejo, ya que todo está combinado en un único sistema. Sin embargo, esta simplicidad también nos cuesta. Primero, estás limitado a qué tipos de sistemas operativos puedes implantar debido al hardware y al programa virtual. Segundo, las Honeynets virtuales traen un riesgo, específicamente que un atacante puede salirse del programa virtual y tomar el sistema Honeynet, saltándose los mecanismos de Control de Datos y de Captura de Datos.
- Seguridad. Como todos los sistemas comparte el mismo hardware, puede que un atacante acceda a otras partes del sistema. Tiene mucha dependencia del software virtual.
- 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.[73]

[73]Federación de Enseñanza de Andalucia, 2009, Honeynet Una desconocida en la Seguridad Informática,http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf

CAPÍTULO III

Situación actual del LTIC

3.1 Introducción

El Laboratorio de Tecnologías de Información y Comunicaciones - LTIC administra los equipos, programas y otras tecnologías relacionadas con tecnologías de información y comunicaciones de la Facultad de Ingeniería.El LTIC, está ubicado en el segundo piso de la Facultad de Ingeniería de la Pontificia Universidad Católica del Ecuador, su horario de atención es de lunes a viernes de 07h00 a 20h00.

El LTIC es un área que dispone de infraestructura tecnológica para satisfacer la demanda de requerimientos de software y de hardware de todas las materias de Ingeniería de Sistemas y parte de las materias de Ingeniería Civil, cuenta con software licenciado y libre a nivel multiplataforma. Las instalaciones del LTIC son independientes de la Dirección de Informática de la PUCE, con la finalidad de realizar todas las prácticas de laboratorios sin afectar a los equipos y servidores que están en ambiente de producción. [74]

3.2 Misión

El LTIC como miembro de la PUCE comparte su misión y visión:

Considera misión propia el contribuir, de un modo riguroso y crítico, a la tutela y desarrollo de la dignidad humana y de la herencia cultural, mediante

[74] Documento "Visión General del Laboratorio TIC"

la investigación, la docencia y los diversos servicios ofrecidos a las comunidades locales, nacionales e internacionales.

En dicha misión, asume el deber de prestar particular atención a las dimensiones éticas de todos los campos del saber y del actuar humano, tanto a nivel individual como social. En este marco propugna el respeto a la dignidad y a los derechos de la persona humana, y a sus valores trascendentes, y apoya y promueve la implantación de la justicia en todos los órdenes de la existencia.

Goza de aquella autonomía institucional que le es necesaria para cumplir sus funciones eficazmente.

Garantiza a sus miembros la libertad académica, salvaguardando los derechos de la persona y de la comunidad dentro de las exigencias de la verdad y del bien común.[75]

Examina a fondo la realidad con los métodos propios de cada disciplina académica, estableciendo después un diálogo entre las diversas disciplinas que las enriquezca mutuamente. Con ello pretende la integración del saber.

Promueve el compromiso de todos los miembros de la comunidad universitaria para la consecución de los fines institucionales, a través del diálogo y la participación.

[75] Documento "Visión General del Laboratorio TIC"

3.3 Visión

En los próximos años, la PUCE, fundamentada en el pensamiento y en las directrices pedagógicas ignacianas, se consolidará como un sistema nacional integrado competitivo y auto sostenible, con infraestructura tecnológica de vanguardia.Será reconocida por su gestión ética en servicio de la comunidad, y por su estructura académica moderna para la formación de profesionales con responsabilidad social.

Será también reconocida por los resultados de la investigación científica desarrollada en sus unidades académicas, por realizar su gestión con el apoyo de un sistema técnico, innovador y efectivo, con procesos eficientes y recursos humanos capacitados y comprometidos con la misión institucional.[76]

3.4 Estructura Orgánica

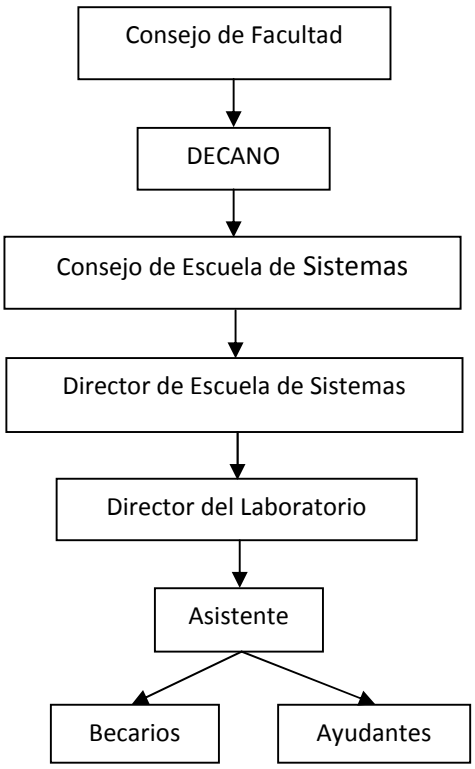
El Laboratorio de Tecnologías de Información y Comunicaciones (LTIC), es una unidad de servicio de la Facultad de Ingeniería de la PUCE.

- Asiste al cuerpo docente y estudiantado en la actividad académica práctica.
- Desarrollar investigación y apoyar el desarrollo de las asignaturas relacionadas con la práctica tecnológica y científica de la Informática, los Sistemas y la Computación.

[76] Documento "Visión General del Laboratorio TIC"

- Procurar la capacitación técnica en diferentes ámbitos relacionados con tecnologías de información y comunicaciones a docentes, administrativos, becarios, ayudantes y estudiantes de pregrado y postgrado de la Facultad de Ingeniería.
- Ofertar servicio y asesoría a otras Unidades Académicas de la PUCE en lo concerniente a prácticas y técnicas de laboratorio en informática, sistemas y computación.
- Brindar servicios a terceros bajo los requisitos legales y demás normativa de la PUCE.

Gráfico 14: Organigrama - LTIC[77]



[77] Gráfico 14: Documento "Visión General del Laboratorio TIC"

3.5 Situación Actual del LTIC

La actual administración del semestre 2014–2015, ha estado reformulando la normativa interna del LTIC, la cual se encuentran mitigando problemas existentes en todas las áreas del Laboratorio.

Existe un instructivo interno de seguridad en el cual se indica el acceso físico al Laboratorio, más no las seguridades que deberían implementarse en los servidores. Deberían establecerse normas generales con la implementación de las mejores prácticas de seguridad sobre los servidores con los que cuenta LTIC. [78]

En cada inicio de semestre, se da un mantenimiento a todos los equipos correspondientes al LTIC y se actualiza las últimas versiones de todo el software.

Se tiene un inventario actualizado al día sobre el hardware y software del LTIC. No existe un diagrama de conectividad.

3.6 Servicios

El LTIC ofrece a profesores y estudiantes infraestructura tecnológica para cumplir con el proceso de enseñanza - aprendizaje. Cuenta con aulas equipadas con hardware y software necesario para el desarrollo y formación de estudiantes de ingeniería en sistemas e ingeniería civil. Actualmente se

[78] Documento "Visión General del Laboratorio TIC"

brinda acceso al internet con una velocidad de 70 Megas, lo que permite que los estudiantes puedan hacer tareas de investigación sin ningún problema.[79]

3.7 Seguridad

3.7.1 Física

Las instalaciones del LTIC cumplen los siguientes procedimientos por seguridad:

- Bloqueo del ascensor izquierdo para el segundo piso
- Una puerta de acceso principal ubicada frente al ascensor.
- Puertas con tarjetas de acceso y llave en cada aula y sala.
- Puertas internas para el Data Center y área de mantenimiento.
- El Laboratorio cuenta con cámaras de seguridad
- Existen detectores de movimiento y de humo en cada sala del LTIC.

Son áreas restringidas:

- Estación de registro en el ingreso del Laboratorio.
- Oficina de Becarios.
- Oficinas Administrativas (Director, Asistente, Mantenimiento).
- Data Center.

Toda área restringida, permanecerá cerrada por razones de seguridad.[80]

- El acceso a estas áreas será autorizados por los administrativos del Laboratorio.

[79] Documento "Visión General del Laboratorio TIC"
[80] Documento "Visión General del Laboratorio TIC

- No se permite ninguna persona en calidad de acompañante en la estación de registro, en la oficina de becarios ni en la sala de mantenimiento.

3.7.2 Lógica

En el punto anterior, se mencionó brevemente la mayoría de seguridades físicas con las que cuenta el LTIC, la cual hace referencia a la protección del LTIC frente a accesos no autorizados y ataques físicosa los ordenadores, instalaciones, personal, documentación física, etc. Sin embargo, para salvaguardar en mayor porcentaje los bienes del LTIC, esta debe contar con seguridades lógicas ya que, ambas seguridades tanto físicas como lógicas son complementarias. De nada sirve controlar los accesos físicos a las instalaciones para no sufrir percances y mantener a salvo los bienes, si un individuo puede acceder a la información confidencial del LTIC cómodamente desde otro ordenador conectado a la red.

Para tener una idea más clara de las vulnerabilidades lógicas del LTIC, se realizó un escaneo de toda la red para conocer si existe puertos abiertos o servicios vulnerables la cual puedan ser comprometidos por cualquier intruso informático. Además, se usó la herramienta wireshark para capturar y analizar los paquetes de circulan por la red, permitiendo ver a un nivel bajo y detallado que está pasando en la red.

Mediante las pruebas realizadas en la red del LTIC, no se encontró servicios vulnerables ni actividades maliciosas en la red. Sin embargo, esto no quiere

decir que el LTIC, está libre de cualquier ataque, ya que los intrusos informáticos están dispuestos a atacar cuando menos se lo espera.

Un tema importante que debemos recalcar es que muchas veces, el punto más débil de un sistema informático son las personasrelacionadasen mayor o menor medida con él, dando la posibilidad de ataquescomo:

- Ingeniería social:En relación al LTIC, los usuarios que a diario o semanal usan las computadoras, pueden abusar de la ingenuidad o confianza de los ayudantes o becarios, para obtener información que pueda ser utilizada para tener acceso a la información de las claves o computadoras no autorizadas.
- ShoulderSurfing: En relación al LTIC, los usuarios pueden espiar físicamente a los ayudantes o becarios para obtener generalmente claves de acceso al sistema.
- Basureo: En relación al LTIC, un ayudante al momento de hacer algún mantenimiento en cualquier equipo, puede olvidada información importante relacionada al sistemas, dando la posibilidad a cualquier usuario obtener dicha información.
- Atacante interno: En relación al LTIC, las amenaza pueden proceder de personas que han realizado ayudantías y han tenido acceso a los sistemas y claves.

CAPÍTULO IV

Diseño del prototipo de seguridad para LTIC

4.1 Propuesta de un prototipo de seguridad con honeynet

Las redes y sus aplicaciones, y en particular Internet, han introducido nuevas formas de manejo de información que también implican riesgos. Éstos surgen a partir de las vulnerabilidades que poseen los sistemas de información. La existencia de vulnerabilidades implica amenazas, cuya concreción son los ataques.

Para prevenir o mitigar 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.

Ante una carencia de herramienta deseguridad que permita mantener protegidos los sistemas de información delLaboratorio de Tecnologías de la Información y Comunicación –LTIC,se hacen necesaria la propuesta de la Implementación de un prototipo de seguridad con Honeynet Virtuales.

4.1.1 Objetivo de la propuesta

Implementar de un prototipo de seguridad con honeynet virtuales para descubrir patrones de ataques y analizar el comportamiento y las condiciones de los intrusos, aplicado en el Laboratorio de Tecnologías de la Información y Comunicación - ITIC.

4.1.2 Justificación de la propuesta

Actualmente, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Por tal motivo, es necesario utilizar técnicas proactivas de defensa orientadas a la seguridad de redes como son los honeynet.

La idea principal de la tecnología de los honeynet es mostrar a los atacantes un sistema virtual que parezca el sistema real, cuya intención es atraer a los atacantes simulando ser sistemas débiles o con fallas de seguridad, evidentes, o no del todo, pero si lo suficiente para atraerlos y ser un reto para sus habilidades de intrusión, de esa manera los ataques se efectuarán sobre esesistema sin causar ningún daño al sistema real.

Con la presente propuesta, el Laboratorio de Tecnologías de la Información y Comunicación – LTIC, podrá realizar un mejor aseguramiento de los servidores de la red, siendo la herramienta de los honeynets punto de distracción de los sistemas reales ante cualquier ataque oatacante, salvaguardando la información.

Con la implementación de esta herramienta se podrá contar con elementospara el análisis de situaciones anómalas o ataques, teniendo la informaciónnecesaria para poder evitar y realizar correcciones o un mejor aseguramiento enlos componentes externos para cerrar las posibles entradas que pudiese tener unatacante y de la misma forma se podrá contar con elementos para estudiar cual es elcomportamiento de los ataques.

4.1.3 Importancia y beneficios

En la actualidad, las compañías pueden ser infectadas conmalware y están expuestas a la pérdidade datos. Es por ello, que todaorganización debe estar a la vanguardia de estos procesos yestar preparada para afrontar tales situaciones, identificandolos posibles riesgos informáticos y tomando medidas queaseguren su integridad.Muchos sistemas están expuestos a "agujeros" de seguridad que son explotadospara acceder a archivos, obtener privilegios o realizar sabotaje.

Por tal razón es muy importante la propuesta que los sistemas Honeynetpresentan, ya que estos sistemas, en vez de repeler las acciones de los atacantes, utilizan técnicaspara monitorizarlas y registrarlas

La implementación de unprototipo de Honeynet en el entorno de red del LTIC, constituye un componente de seguridadindispensable. Los Honeypots al constituirse como equiposdestinados a ser atacados y comprometidos, desvían la atención de cualquier atacante. De esta manera, se evita que se involucren losrecursos principales de información, permitiendo aún más,conocer las vulnerabilidades y agujeros de seguridadexistentes.

Estos sistemas trampa están diseñados para imitar el comportamiento de aquellossistemas que puedan ser de interés para un intruso.

Suelen contar con mecanismos de protección para que un atacante con éxito nopueda acceder a la totalidad de la red, naturalmente, si un intruso consigue entraren un sistema trampa, no debe percatarse de que está siendo monitorizado oengañado.

La propuesta beneficiara directamente al Laboratorio de Tecnología de la Información y Comunicaciones – LTIC.,la cual es designada para garantizar y velar por un óptimo funcionamiento de las estructurasde cómputo, telecomunicaciones y servicios que brinda a los estudiantes de la Facultad de Ingeniería.

4.1.4 Alcance de la propuesta

El presente proyecto de disertación de grado, culminará con la entrega de un documento que contenga el prototipo de seguridad de una honeynet virtual como recurso de investigación y estudio del tráfico que circula por la red, definiendo mecanismos y tendencias de ataques para definir medidas necesarias preventivas a nivel de las redes de datos, en el Laboratorio de Tecnologías de la Información y Comunicación, de la Facultad de Ingeniería de la PUCE.

4.2 Definición de requerimientos funcionales y técnicos

4.2.1 Requerimientos Funcionales

Estos requerimientos definen el tipo de servicio esperado de la propuesta.

- La honeynetestá diseñada y compuesta por un conjunto de sistemas dispuestos a ser sondeados, atacados y comprometidos por un intruso informático.
- La honeynet actuara como una pecera ya que tendrá la capacidad de observar, monitorear, analizary capturar el ataque.
- Con un posterior análisis del ataque capturado por la honeynet, es posible aprender las tácticas y determinar los patrones de ataques que emplean los intrusos para comprometer los sistemas.
- La Honeynet tendrá la capacidad de engañar a posibles ataques mediante simulaciones falsas creadas en los honeypots

Requerimientos Técnicos

4.2.1.1 Requerimientos de Hardware

Los Requerimientos mínimos para el funcionamiento de la Honeynet Virtual es un ordenador de las siguientes:

Tabla 1: Especificaciones TécnicasMínimas[81]

ESPECIFICACIONES TÉCNICAS MINIMAS	
Procesador	Intel Core 2 Duo
Memoria RAM	3 GB
Disco Duro	250 GB
Tarjeta de Red	Fast Ethernet 10/100 Mbps

Para un Mejor funcionamiento se recomendaría características superiores ya que en la misma correrán máquinas virtuales (Honeywall,Honeypots, etc).

La Máquina adquirida en el LTIC para la implementación del Honeynet tiene las siguientes características:

Tabla 2: Especificaciones Técnicasde la Honeynet Virtual[82]

ESPECIFICACIONES TÉCNICAS	
Procesador	Intel® Core™ i7 ; 3.40 GHz
Memoria RAM	6 GB
Disco Duro	250 GB
Tarjeta de Red	Fast Ethernet 10/100/1000 Mbps

[81]Tabla 1: Especificaciones Técnicas Mínimas para la Honeynet Virtual, Realizado por: Jhonny Vaca
[82]Tabla 2: Especificaciones Técnicas de Honeynet Virtual, Realizado por: Jhonny Vaca

4.2.1.2 Requerimientos de Software

4.2.1.2.1 Software de Virtualización VMWARE PLAYER

VMware Player, es una potente herramienta gratuita, desarrollada especialmente para la virtualización. Con VMware Player, se puede crear y ejecutar máquinas virtuales en nuestro sistema, con la posibilidad de instalar en éstas el sistema operativo que queramos, por ejemplo cualquier versión de Windows, Linux, Mac OS X, Chrome OS, etc. Además una de las principales características del programa, es que podemos ejecutar múltiples sistemas operativos o programas, sin que se modifique nuestro sistema operativo actual. También podremos instalar y probar programas aisladamente de una forma segura, ya que no modificará nuestro sistema operativo actual.[83]

La versión que se utilizara para las máquinas virtuales de la honeynet será la versión **VMware Player 6.0.2 build-1744117**.

4.2.1.2.2 Herramientas de Captura de la Honeynet (Honeywall)

Esta herramienta será un Honeywall, esuna distribución de Linux roo-1.4.hw-20090425114542 basada en Centos. Esta herramienta incluye varios componentes claves para la honeynet.

[83] (2011), VMware Player, http://www.softzone.es/2011/10/06/vmware-player-4-0-0-crea-y-ejecuta-maquinas-virtuales-con-vmware-player/

Tabla 3: Componentes de la Honeywall[84]

Componente	Descripción
Snort	Sistema de detección de intrusosbasadoenreglas,capazderealizarel análisis deltráficodelaredentiemporeal y también registrar
Snort_inline	Es una versión modificada del Snortquetomadecisionessobreeltráfico saliente siempre y cuandotengaataquesconocidos.
SessionLimit	Controldelímitedesesiones.
Sebek	Es una herramienta de captura de datos diseñada para capturar al ataques sobre las actividades de una honeypot
Walleye	Proporciona al administradorherramientasdeanálisisdedatosdemanera remota. Losadministradorespuedenaccederatodoslosdatos capturadosporSnort_inlineySebek, estosdatosincluyenladirecciónIP, datostransferidosyaccionesdelos atacantesenlosHoneypots.Walleyeseejecutasobreunservidor
Pcap	Interfaz de captura de datos delkerneldeLinux.
Iptables	Firewall de Linux integrado en elkernel, usadoparalimitarlospaquetesenelcontroldedatosypara registrar losdatosenlacapturadedatos.
Swatch	Herramientaque comunicaaladministradorpormediodeuncorreoelectrónicotan
Argus + Hflow	Información de flujos de tráfico yrelaciones.
Menu	Una interfaz gráfica usadaparamantenimientoycontrolde la Honeynet
Mysql	Unservidordebasededatosutilizadoparaalmacenar y relacionar el contenidocapturado.

[84]Tabla 3: Componentes de la Honeywall, Realizado por: Jhonny Vaca

4.2.1.2.3 BackTrack Linux 5.1 R1

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

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.[85]

4.2.1.2.4 Windows Xp

Windows XP es una versión de Windows, lanzada en octubre de 2001. Su nombre en clave durante la fase de desarrollo fue Whistler, mientras que su denominación oficial proviene del término inglés eXPerience.

Microsoft ha proporcionado soporte técnico a Windows XP durante los últimos 12 años. Pero tanto para nosotros como para nuestros socios de hardware y software ha llegado el momento de invertir nuestros recursos en apoyar tecnologías más recientes para que podamos seguir proporcionando nuevas experiencias de primera calidad. Por consiguiente, la asistencia técnica para Windows XP ya no está disponible, incluidas las actualizaciones automáticas que ayudan a proteger tu PC.[86]

[85] http://www.backtrack-linux.org/forums/showthread.php?t=24468
[86] http://windows.microsoft.com/es-es/windows/end-support-help

4.2.1.2.5 VALHALA HONEYPOT

Valhalla fue desarrollado por Marcos FlávioAssunção trae es una herramienta que permite ejecutar el concepto de honeypot para ajustar al gusto y las necesidades de la red que administran. Cuenta con los siguientes servicios para identificar atacantes: WEB, FTP, TFTP, POP3, ECHO, DAYTIME, SMTP, FINGER e PORT FORWARDING. Simula puertos de troyanos bien conocidos (Como el NetBus, SubSeven, etc) y también permite utilizar puertos adicionales, es un software para sistemas operativosWindows de Libre distribución. Se puede descargar el proyecto de http://sourceforge.net/projects/valhalahoneypot/.[87]

4.2.1.2.6 SEBEK

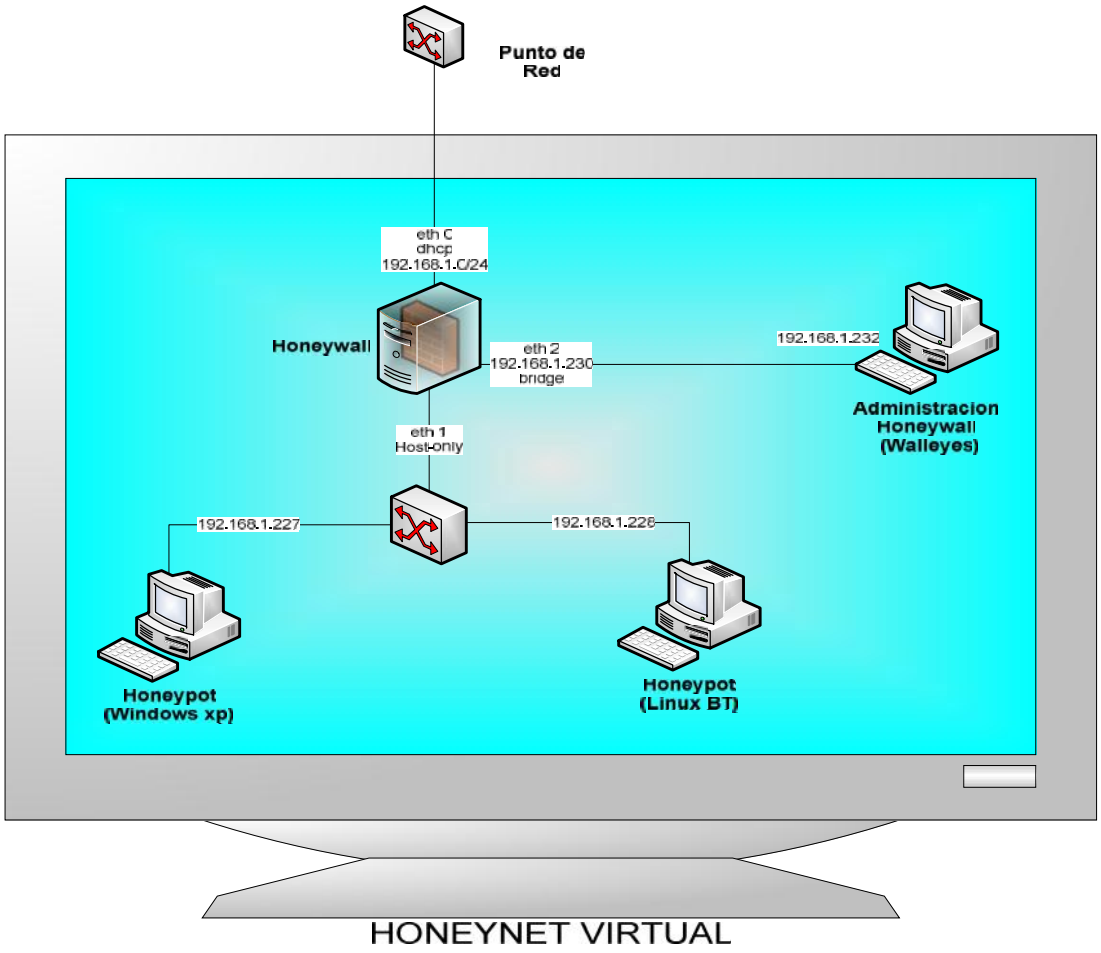
Sebekha sido desarrollado por Edward Balas, miembro del Honeynet Project, es una herramienta de captura de datos diseñada para capturar la actividad de los atacantes en los Honeypots. Básicamente Sebek es una solución formada por dos componentes, un cliente y un servidor. El Sebek cliente es instalado y ejecutado en los Honeypots y se encarga de capturar todas las actividades de los atacantes, estos datos recogidos no son almacenados localmente debido a que esto revelaría al atacante que su actividad es monitoreada. Los datos son enviados de manera oculta hacia el servidor Sebek, encargado de

[87] 2011, ValhallaHoneypot, http://www.binaryti.com/2012/02/valhalla-honeypot.html

recoger los datos y almacenarlos en un repositorio central. El servidor Sebek puede estar localizado en el mismo Honeywall o en un servidor remoto. Esta herramienta de seguridad se puede ejecutar en plataformas Linux yWindows, y se lo puede descargar desde la web desde la siguiente ubicación: https://projects.honeynet.org/sebek/.[88]

4.3 Esquema genérico o estándar de la propuesta

Gráfico 15: Esquema de la Honeynet[89]



[88] http://his.sourceforge.net/proy_his/papers/tut_sebek/
[89] Gráfico 15: Esquema de la Honeynet, Realizado por: Jhonny Vaca

4.4 Descripción de la propuesta

4.4.1 Instalación de Honeynet Virtual

4.4.1.1 Instalación de Honeywall en MVWARE

La Honeywall tendrá 3 interfaces o tarjetas de red, dos en modos “Bridge” y una en modo “Host-only”.

Bridge: Al configurar la Máquina Virtual con esta opción, usa una dirección IP desde la red física y tiene acceso completo a los recursos de red. Significa que puede acceder a Internet, al servidor DHCP de la LAN, a losarchivos compartidos entre otras cosas. Es como tener un computadorseparado en la propia red.

Host-Only:Con esta opción,la Máquina Virtual que está conectada a nuestroequipo real es invisible a otros dispositivos en la LAN. Es decirse crea una red aislada a la de la LAN real.

Tabla 4: Interfaces de Red de la Honeywall[90]

INTERFACES DE RED	
Interface de Red 1 (Host-only)	El Honeywall se comunicara con los honeypots
Interface de Red 2 (Bridge)	El Honeywall se comunicara con la maquina anfitrión (Red Externa)
Interface de Red 3 (Bridge)	Para la administración del honeywall

[90]Tabla 4: Interfaces de Red de la honeywall, Realizado por: Jhonny Vaca

Gráfico 16: Nueva Máquina Virtual Honeywall (Firewall)[91]

Gráfico 17: Linux distribución Centos[92]

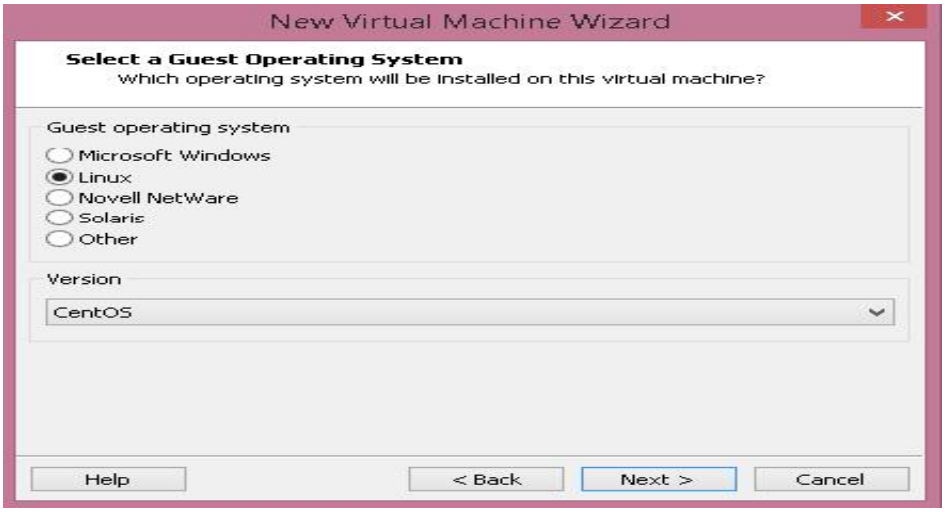
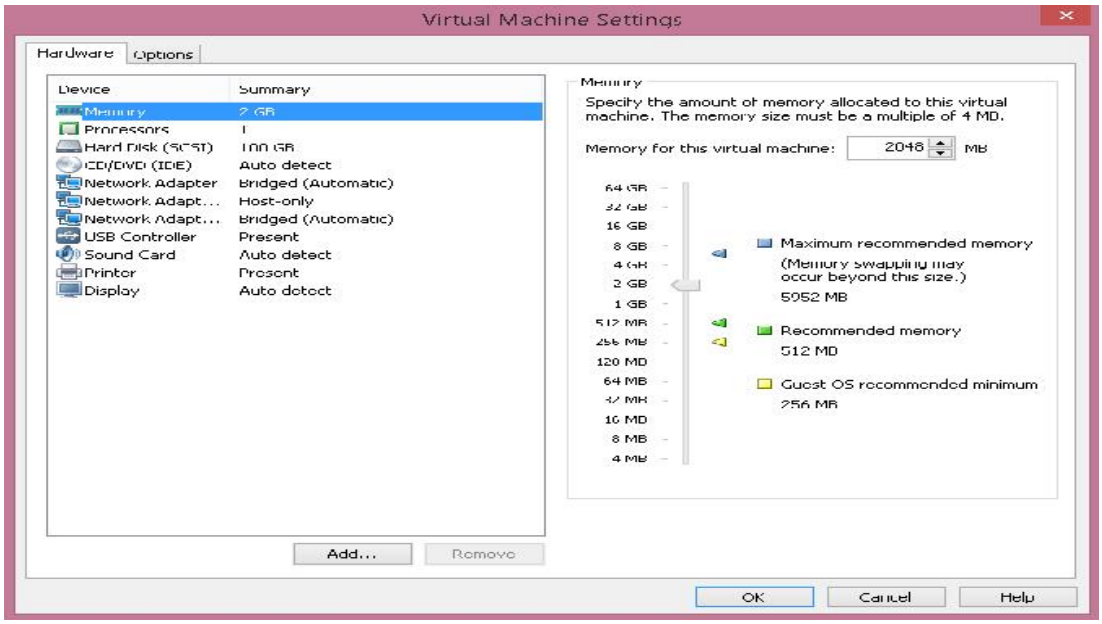


Gráfico 18: Características Máquina Virtual (Honeywall)[93]



[91]Gráfico 16: Nueva Máquina Virtual Honeywall (Firewall), Realizado por: Jhonny Vaca
[92] Gráfico 17: Linux distribución Centos, Realizado por: Jhonny Vaca
[93]Gráfico 18: Características Máquina Virtual (Honeywall), Realizado por: Jhonny Vaca

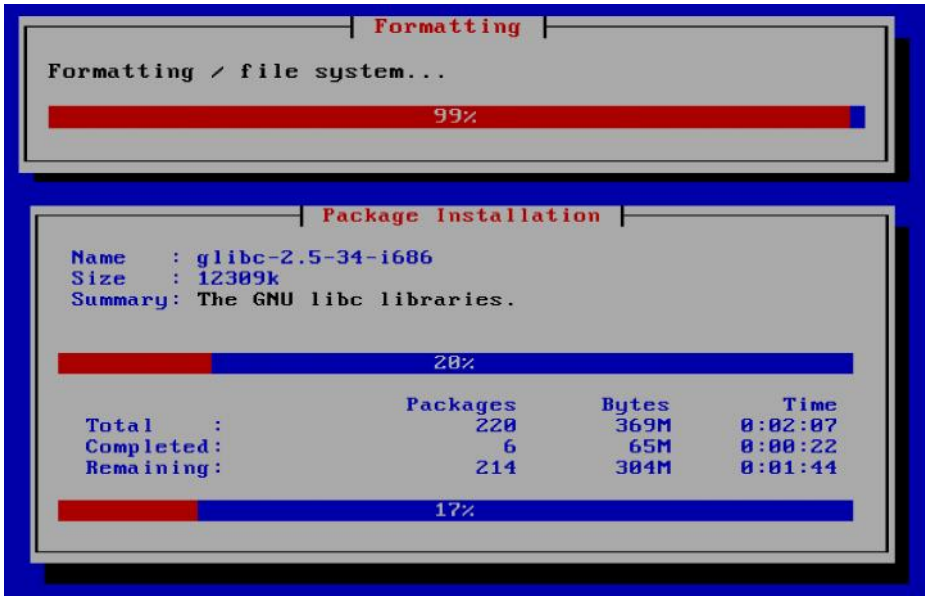
4.4.1.2 Configuración del Honeywall

4.4.1.2.1 Al encender la nueva máquina virtual, esta será la pantalla de bienvenida del Honeywall, indica que todos los datos del disco duro serán borrados tras su instalación, presionarenter

Gráfico 19: Pantalla de Bienvenida del Honeywall[94]

4.4.1.2.2 El sistema formateara el disco duro e instalara el Honeywall

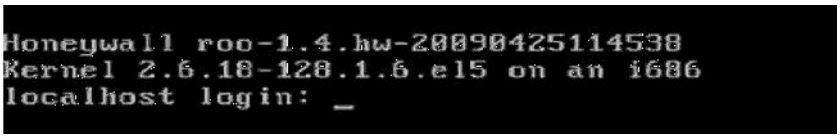
Gráfico20: Instalación del Honeywall[95]



[94]Gráfico 19: Pantalla de Bienvenida del Honeywall, Realizado por: Jhonny Vaca
[95]Gráfico 20: Instalación del Honeywall, Realizado por: Jhonny Vaca

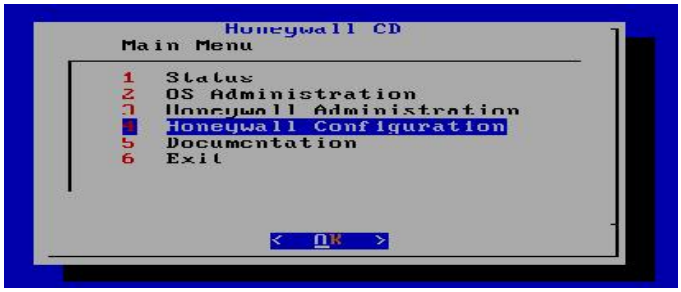
4.4.1.2.3 Al terminar la instalación mostrara la pantalla de ingreso, el usuario por defecto “roo” y el password “honey”. Después, ingresar el comando “su -” y el password “honey”, presionar enter.

Gráfico 21: Pantalla de Ingreso del Honeywall[96]



4.4.1.2.4 Seleccionar “HoneywallConfiguration”

Gráfico 22: Pantalla deMenu del Honeywall[97]



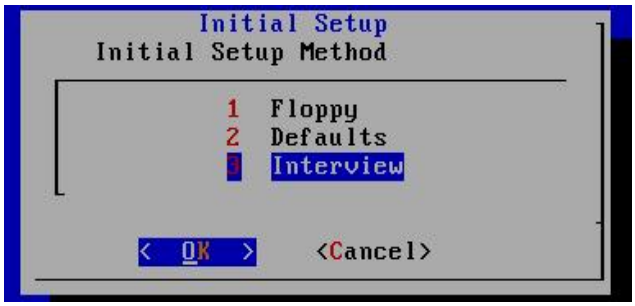
4.4.1.2.5 En el método de configuración inicial tiene 3 opciones:

Floppy: Permite cargar configuraciones existentes en el disco

Defaults: Cargara las configuraciones por defecto.

Interview: Cando se configura por primera vez.

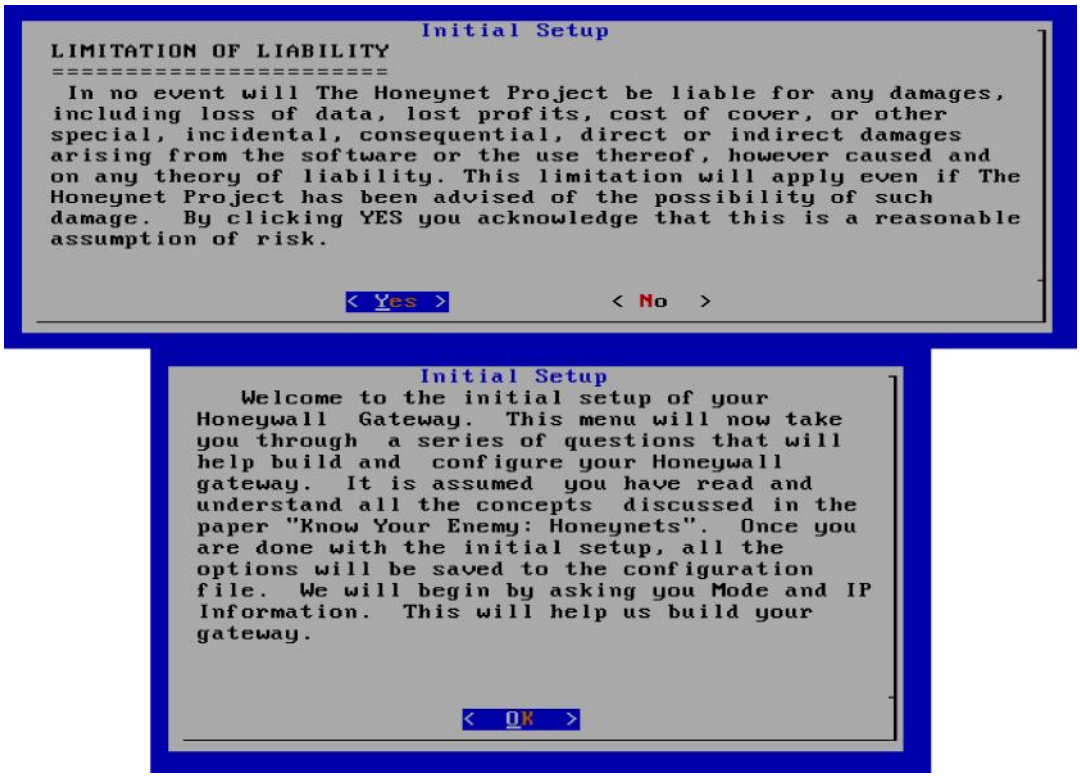
Gráfico 23: Pantalla método de configuración del Honeywall[98]



[96]Gráfico 21: Pantalla de Ingreso del Honeywall, Realizado por: Jhonny Vaca
[97]Gráfico 22: Pantalla de Menu del Honeywall, Realizado por: Jhonny Vaca
[98]Gráfico 23: Pantalla método de configuración del Honeywall, Realizado por: Jhonny Vaca

4.4.1.2.6 Aceptar el acuerdo

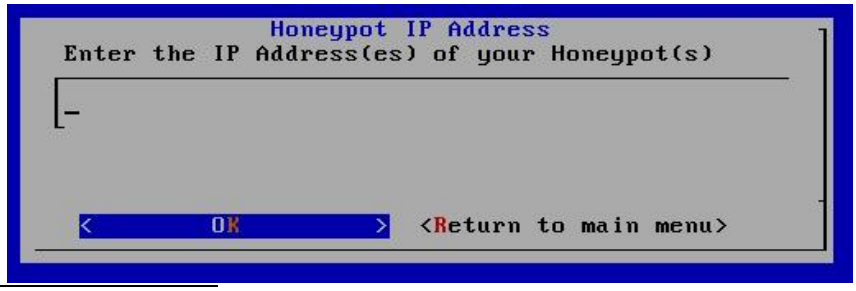
Gráfico24: Pantalla de Bienvenida y Acuerdo del Honeywall[99]



4.4.1.2.7 Ingresar las direcciones IP de los honeypots, si hay más de dos direcciones separar por espacio.

192.168.1.227 192.168.1.228

Gráfico 25: Pantalla de IPs de los honeypots[100]

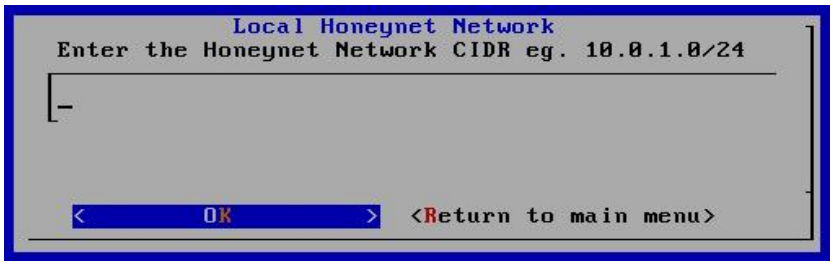


[99]Gráfico 24: Pantalla de Bienvenida y Acuerdo del Honeywall, Realizado por Jhonny Vaca
[100]Gráfico 25: Pantalla de IPs de los honeypots, Realizado por Jhonny Vaca

4.4.1.2.8 Ingresar la dirección de red en formato CIDR

192.168.1.0/24

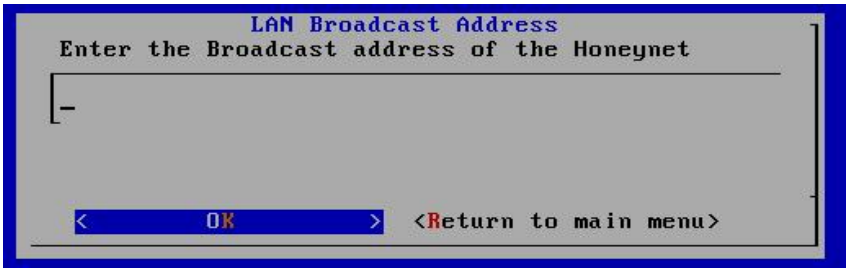
Gráfico 26: Pantalla de dirección CIDR de la Red[101]



4.4.1.2.9 Ingresar dirección broadcast de la red

192.168.1.255

Gráfico 27: Pantalla de dirección Broadcast de la red[102]



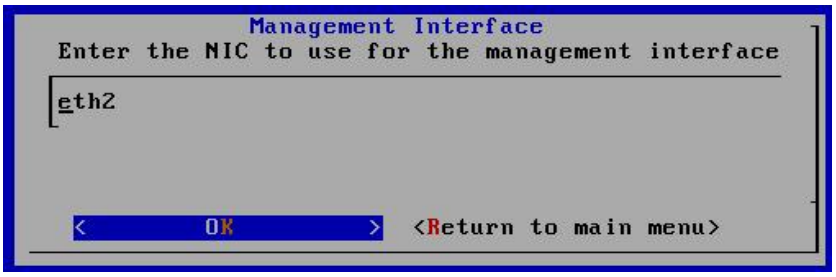
4.4.1.2.10 Indica que la primera parte de la configuración ha terminado. Aceptar

Gráfico28: Pantalla de Primera configuración terminada[103]

[101]Gráfico 26: Pantalla de dirección CIDR de la Red, Realizado por: Jhonny Vaca
[102]Gráfico 27: Pantalla de dirección Broadcast de la red, Realizado por: Jhonny Vaca
[103]Gráfico 28: Pantalla de Primera configuración terminada, Realizado por: Jhonny Vaca

4.4.1.2.11 Tarjeta de red que conectara a la administración remota

Gráfico 29: Pantalla de tarjeta de red para administración remota[104]

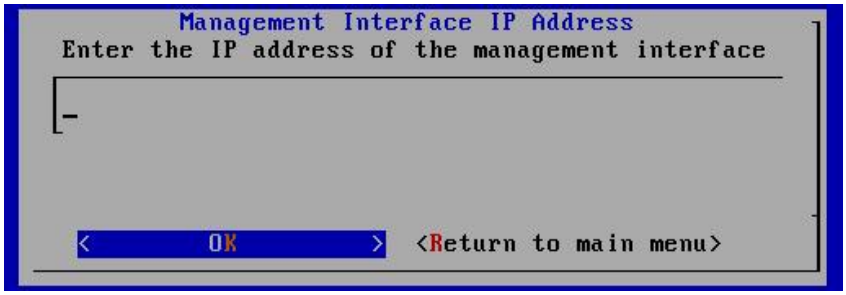


4.4.1.2.12 Pregunta si se quiere configurar la interface de administración remota. **Yes**

Gráfico 30: Pantalla para aceptar la configuración remota[105]

4.4.1.2.13 Ingresar la dirección IP que se usara para la administración remota **192.168.1.230**

Gráfico 31: Pantalla de IP de administración remota[106]



[104] Gráfico 29: Pantalla de tarjeta de red para administración remota, Realizado por: Jhonny Vaca
[105] Gráfico 30: Pantalla para aceptar la configuración remota, Realizado por: Jhonny Vaca
[106] Gráfico 31: Pantalla de IP de administración remota, Realizado por: Jhonny Vaca

4.4.1.2.14 Ingresar la Máscara de Red para la IP de administración remota

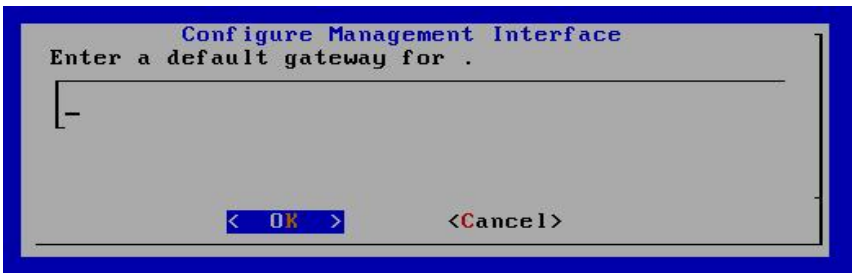
255.255.255.0

Gráfico 32: Pantalla de la máscara de red para administración Remota[107]

4.4.1.2.15 Ingresar el Gateway para la IP de administración remota

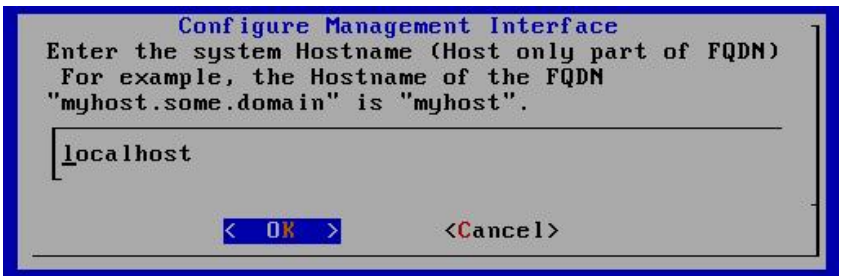
192.168.1.1

Gráfico 33: Pantalla Gateway de la IP de administración remota[108]



4.4.1.2.16 Elegir un nombre para el sistema,lorecomendable seríaponerunnombreficticio**roo-server**

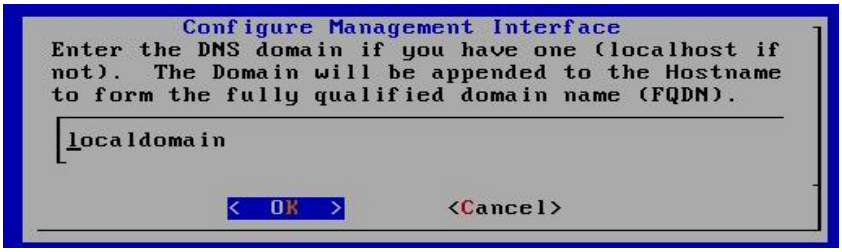
Gráfico 34: Pantalla Hostmane del honeywall[109]



[107] Gráfico 32: Pantalla de la máscara de red para administración Remota, Realizado por: Jhonny Vaca
[108] Gráfico 33: Pantalla Gateway de la IP de administración remota, Realizado por: Jhonny Vaca
[109] Gráfico 34: Pantalla Hostmane del honeywall, Realizado por: Jhonny Vaca

4.4.1.2.17 Ingresareldominio de la Honeywall, o por defaul"localdomain".

Gráfico 35: Pantalla Dominio del Honeywall[110]



4.4.1.2.18 Ingresar los servidores DNS, separar por espacio

172.16.0.1 192.168.1.11

Gráfico36: Pantalla DNS del Honeywall[111]

4.4.1.2.19 Confirmar la activación de la interface de administración.

Gráfico 37: Pantalla de Activación de interfaz de administración remota[112]

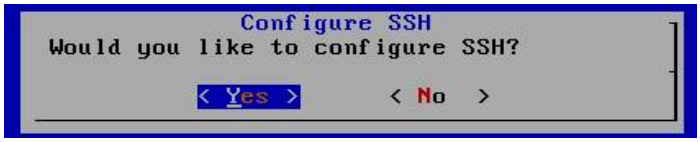
4.4.1.2.20 Preguntaparaactivarla interfazdesdeenelpróximoboot.

Gráfico 38: Pantalla Activación administración remota en próximo boot[113]

[110] Gráfico 35: Pantalla Dominio del Honeywall, Realizado por: Jhonny Vaca
[111] Gráfico 36: Pantalla DNS del Honeywall, Realizado por: Jhonny Vaca
[112] Gráfico 37: Pantalla de Activación interfaz de administración remota, Realizado por: Jhonny Vaca
[113] Gráfico 38: Pantalla Activación administración remota en próximo boot, Realizado por: Jhonny Vaca

4.4.1.2.21 Confirmar la configuración SSH.

Gráfico39: Pantalla Configuración de SHH del Honeywall[114]



4.4.1.2.22 Preguntaparaqueelusuariorootpuedalogarseremotamente

Gráfico 40: Pantalla Acceso al usuario root para SSH[115]

4.4.1.2.23 Cambiardepasswordparaelusuarioroo

Gráfico 41: Pantalla Cambio de password usuario roo[116]

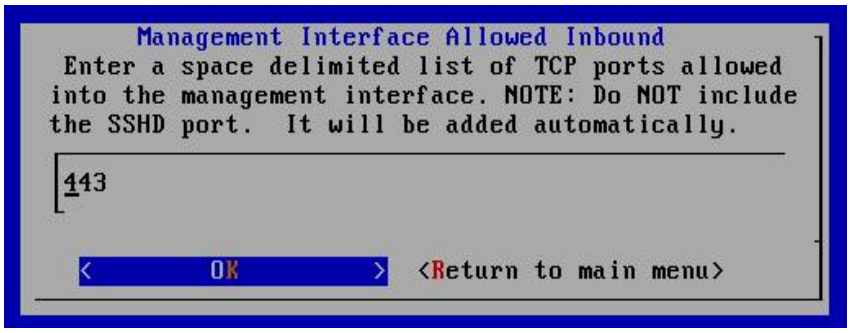
4.4.1.2.24 Cambiar password para usuario root

Gráfico 42: Pantalla Cambio de password usuario root[117]

[114] Gráfico 39: Pantalla Configuración de SHH del Honeywall, Realizado por: Jhonny Vaca
[115] Gráfico 40: Pantalla Acceso al usuario root para SSH, Realizado por: Jhonny Vaca
[116] Gráfico 41: Pantalla Cambio de password usuario roo, Realizado por: Jhonny Vaca
[117] Gráfico 42: Pantalla Cambio de password usuario root, Realizado por: Jhonny Vaca

4.4.1.2.25 Puerto permitido para la interface de administración. Por defecto

Gráfico 43: Pantalla Puerto permitido para administración remota[118]



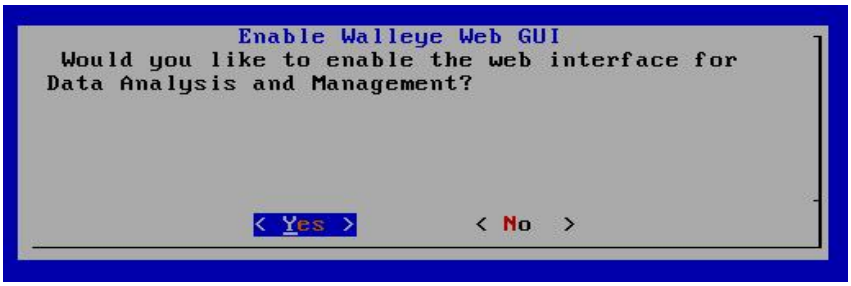
4.4.1.2.26 Ingresar direcciones IPs permitidas para administrar el Honeywall, de lo contrario ingresar **any**

Gráfico 44: Pantalla Puerto permitido para administración remota[119]

4.4.1.2.27 Pregunta para habilitar interface web de administración remota

Yes

Gráfico 45: Pantalla Habilitar interface web[120]



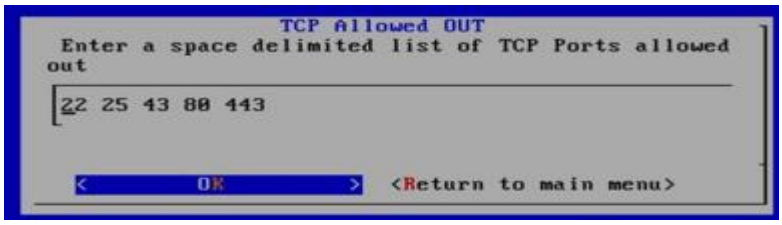
[118] Gráfico 43: Pantalla Puerto permitido para administración remota
[119] Gráfico 44: Pantalla Puerto permitido para administración remota
[120] Gráfico 45: Pantalla Habilitar interface web

4.4.1.2.28 Confirmar restricciones de firewall salientes

Gráfico 46: Pantalla confirmar restricciones de firewall[121]

4.4.1.2.29 Especificar puertos TCP de salida.

Gráfico 47: Pantalla Puertos TCP de salida[122]

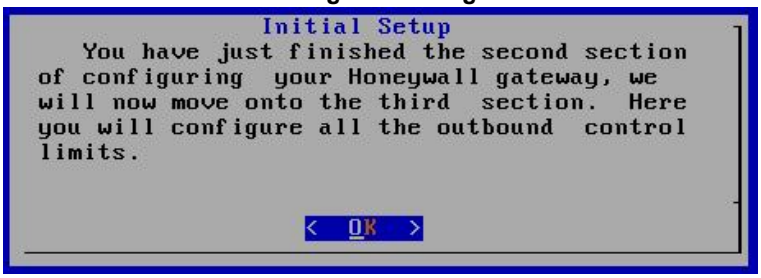


4.4.1.2.30 Especificar puertos UDP de salida.

Gráfico 48: Pantalla Puertos UDP de salida[123]

4.4.1.2.31 Indica que la segunda parte de la configuración ha terminado.

Gráfico 49: Pantalla de Segunda configuración terminada[124]



[121] Gráfico 46: Pantalla confirmar restricciones de firewall, Realizado por: Jhonny Vaca
[122] Gráfico 47: Pantalla Puertos TCP de salida, Realizado por: Jhonny Vaca
[123] Gráfico 48: Pantalla Puertos UDP de salida, Realizado por: Jhonny Vaca
[124] Gráfico 49: Pantalla de Segunda configuración terminada, Realizado por: Jhonny Vaca

4.4.1.2.32 Ingresar la escala de tiempo para la recolección de datos.

Gráfico 50: Pantalla Escala de tiempo[125]

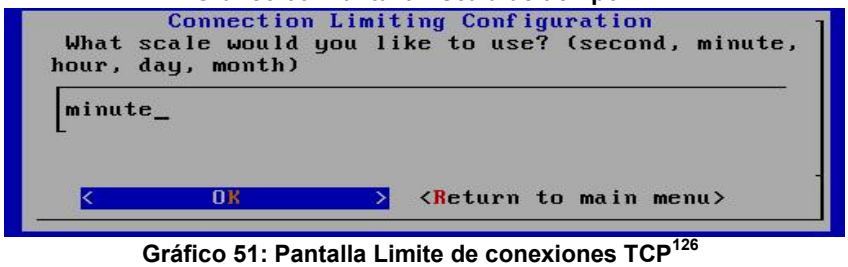


Gráfico 51: Pantalla Limite de conexiones TCP[126]

Gráfico 52: Pantalla Limite de conexiones UDP[127]

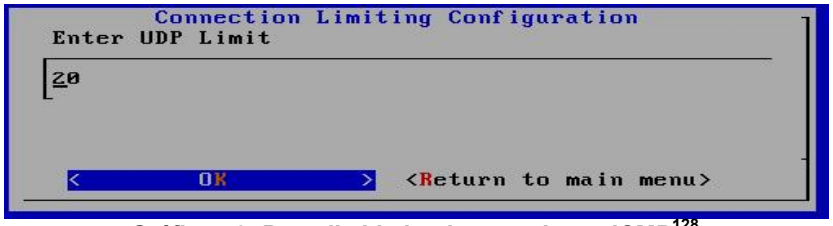


Gráfico 53: Pantalla Limite de conexiones ICMP[128]

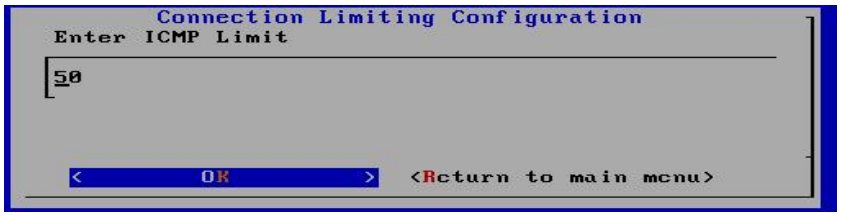
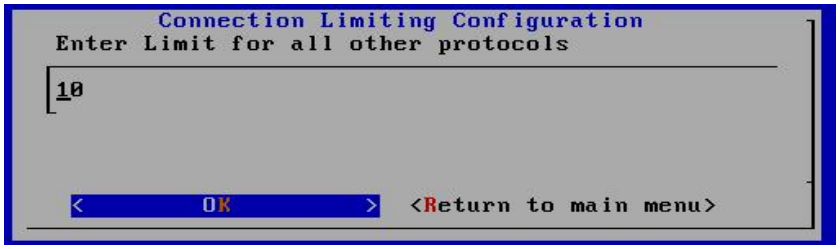


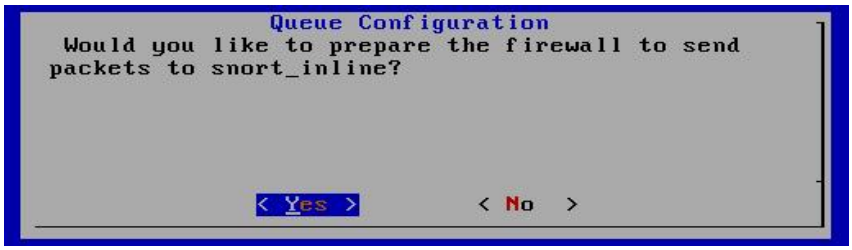
Gráfico 54: Pantalla Limite de conexiones para los demás protocolos[129]



[125] Gráfico 50: Pantalla Escala de tiempo, Realizado por: Jhonny Vaca
[126] Gráfico 51: Pantalla Limite de conexiones TCP, Realizado por: Jhonny Vaca
[127] Gráfico 52: Pantalla Limite de conexiones UDP, Realizado por: Jhonny Vaca
[128] Gráfico 53: Pantalla Limite de conexiones ICMP, Realizado por: Jhonny Vaca
[129] Gráfico 54: Pantalla Limite de conexiones para los demás protocolos, Realizado por: Jhonny Vaca

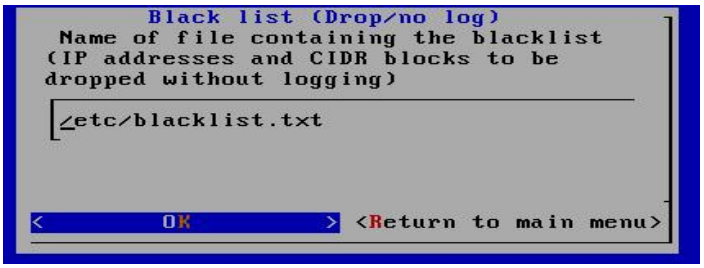
4.4.1.2.33 Habilitar la aplicación snort_inline. **Yes**

Gráfico 55: Pantalla Habilitar snort_inline[130]



4.4.1.2.34 Indicar el archivo de la lista negra (blacklist)

Gráfico 56: Pantalla Archivo Blacklist[131]

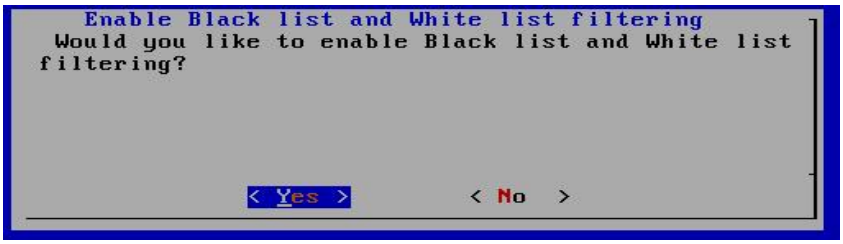


4.4.1.2.35 Indicar el archivo (whitelist), obtendrá las IPs de confianza.

Gráfico 57: Pantalla Archivo Blacklist[132]

4.4.1.2.36 Habilitar filtrado para lista (Black y White)

Gráfico 58: Pantalla Filtrado Black - White[133]



[130] Gráfico 55: Pantalla Habilitar snort_inline, Realizado por: Jhonny Vaca
[131] Gráfico 56: Pantalla Archivo Blacklist, Realizado por: Jhonny Vaca
[132] Gráfico 57: Pantalla Archivo Blacklist, Realizado por: Jhonny Vaca
[133] Gráfico 58: Pantalla Filtrado Black - White, Realizado por: Jhonny Vaca

4.4.1.2.37 Habilitar filtrado seguro durante la captura de paquetes

Gráfico 59: Pantalla Filtrado Seguro[134]

4.4.1.2.38 Ingresar ruta de archivo fencelist

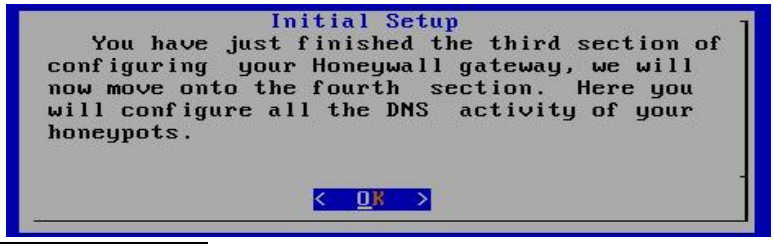
Gráfico 60: Pantalla Ingreso de archivo fencelist[135]

4.4.1.2.39 Pregunta para activar el modo (Roach Motel). Seleccionar **No**

Gráfico 61: Pantalla Modo Roach Motel[136]

4.4.1.2.40 Indica que la tercera parte de la configuración ha terminado.

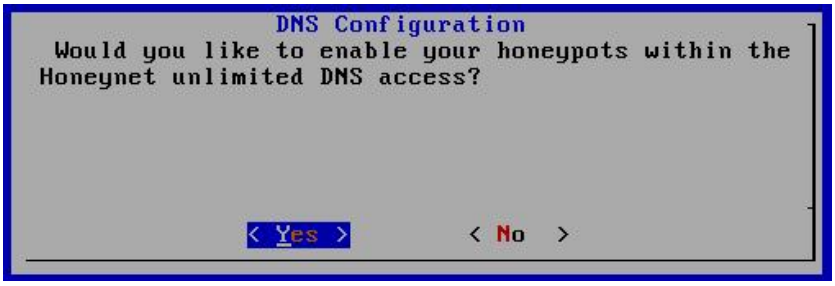
Gráfico 62: Pantalla de Tercera configuración terminada[137]



[134] Gráfico 59: Pantalla Filtrado Seguro, Realizado por: Jhonny Vaca
[135] Gráfico 60: Pantalla Ingreso de archivo fencelist, Realizado por: Jhonny Vaca
[136] Gráfico 61: Pantalla Modo Roach Motel, Realizado por: Jhonny Vaca
[137] Gráfico 62: Pantalla de Tercera configuración terminada< Realizado por Jhonny Vaca

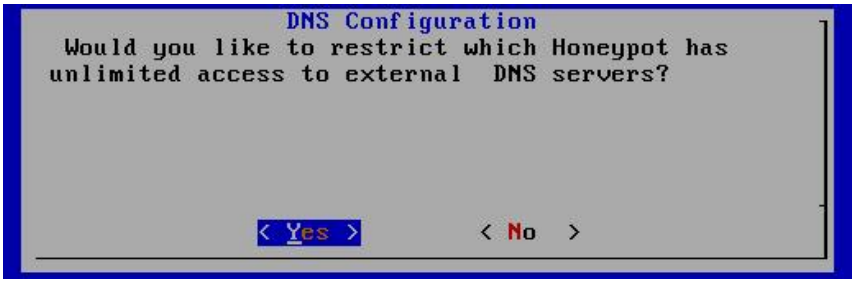
4.4.1.2.41 Permite la utilización del servidor DNS por parte de los honeypots

Gráfico 63: Pantalla Servidor DNS Honeypots[138]



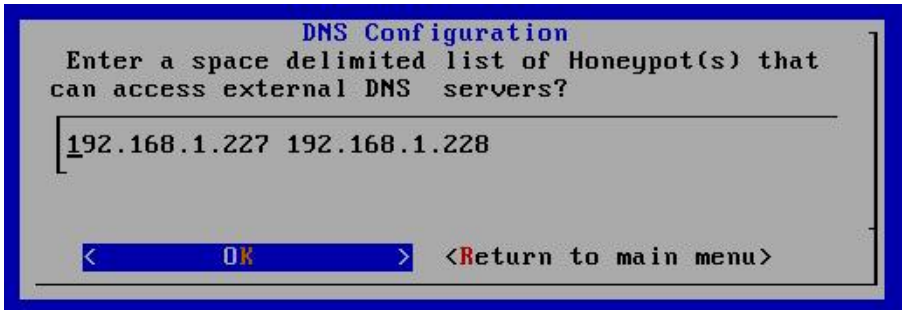
4.4.1.2.42 Habilitar la restricción de accesos ilimitados de los Honeypots hacia servidores DNS externos.

Gráfico 64: Pantalla de Restricción Servidores DNS externos[139]



4.4.1.2.43 Ingresar las IPs de los honeypots que accederán al servidor DNS externos

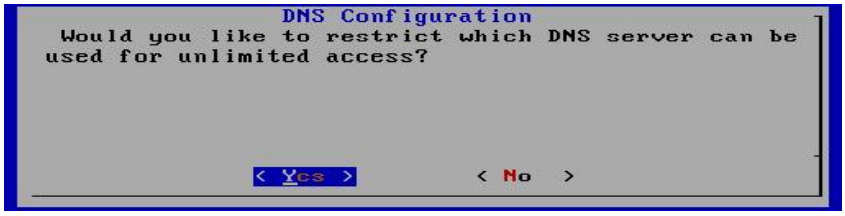
Gráfico 65: Pantalla de Honeypots DNS externos[140]



[138]Gráfico 63: Pantalla Servidor DNS Honeypots, Realizado por: Jhonny Vaca
[139]Gráfico 64: Pantalla de Restricción Servidores DNS externos, Realizado por: Jhonny Vaca
[140]Gráfico 65: Pantalla de Honeypots DNS externos, Realizado por: Jhonny Vaca

4.4.1.2.44 Habilitar la restricción del servidor DNS a ser utilizado para accesos ilimitados.

Gráfico 66: Pantalla de Restricción Servidores DNS acceso ilimitado[141]



4.4.1.2.45 Indica que la cuarta parte de la configuración ha terminado.

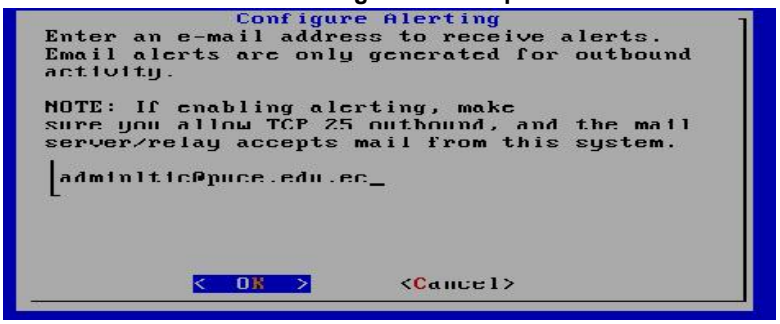
Gráfico 67: Pantalla de Cuarta configuración terminada[142]

4.4.1.2.46 Configurar Email para alertas

Gráfico 68: Pantalla Configurar Email[143]

4.4.1.2.47 Ingresar Email para alertas

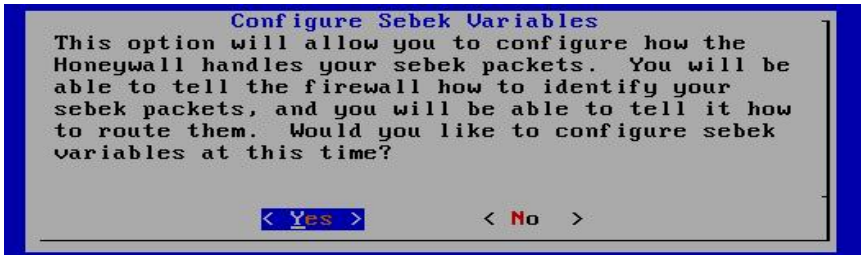
Gráfico 69: Pantalla Ingresar Email para Alertas[144]



[141] Gráfico 66: Pantalla de Restricción Servidores DNS acceso ilimitado, Realizado por: Jhonny Vaca
[142] Gráfico 67: Pantalla de Cuarta configuración terminada, Realizado por: Jhonny Vaca
[143] Gráfico 68: Pantalla Configurar Email, Realizado por: Jhonny Vaca
[144] Gráfico 69: Pantalla Ingresar Email para Alertas, Realizado por: Jhonny Vaca

4.4.1.2.48 Configurar opcionesSebek, para recibir datos de los honeypots

Gráfico 70: Pantalla Configurar Sebek[145]



4.4.1.2.49 Ingresar la IP que escuchara los paquetes Sebek de los honeypots

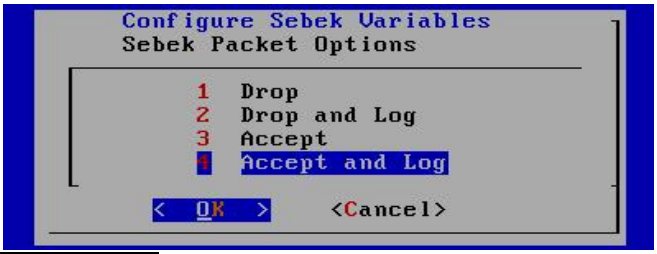
Gráfico 71: Pantalla Ingresar IP Sebek[146]

4.4.1.2.50 Ingresar puerto UDP del destino de los paquetes Sebek

Gráfico 72: Pantalla Ingresar Puerto UDP destino Sebek[147]

4.4.1.2.51 Configurar Sebek para log de todo el tráfico de los honeypots

Gráfico 73: Pantalla Configurar log Sebek[148]



[145] Gráfico 70: Pantalla Configurar Sebek, Realizado por: Jhonny Vaca
[146] Gráfico 71: Pantalla Ingresar IP Sebek, Realizado por: Jhonny Vaca
[147] Gráfico 72: Pantalla Ingresar Puerto UDP destino Sebek, Realizado por: Jhonny Vaca
[148] Gráfico 73: Pantalla Configurar log Sebek, Realizado por: Jhonny Vaca

4.4.1.2.52Finalización de la configuración del Honeywall

Gráfico 74: Pantalla Finalización Configuración Honeywall[149]

4.4.1.3 Instalación y configuración de Sebek

Al descargar, Sebek-Win32-3.0.5 para Windows se puede instalar y configurar en el respectivo honeypot.

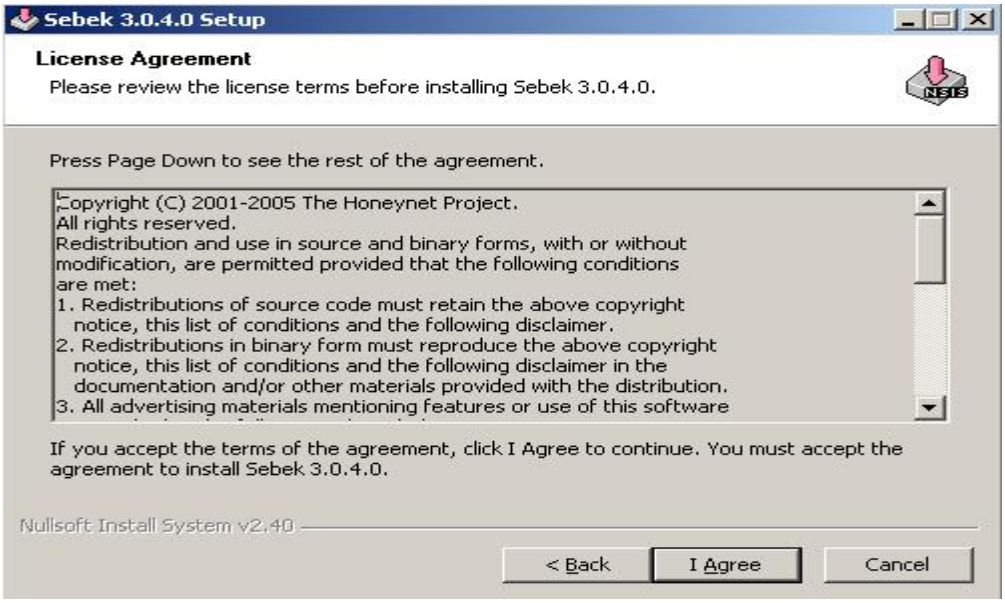
4.4.1.3.1 Ejecutar el instalador Setup.exe. Click en Next.

Gráfico 75: Pantalla de Bienvenida a Configuración Sebek[150]

[149]Gráfico 74: Pantalla Finalización Configuración Honeywall, Realizado por: Jhonny Vaca
[150]Gráfico 75: Pantalla de Bienvenida a Configuración Sebek, Realizado por: Jhonny Vaca

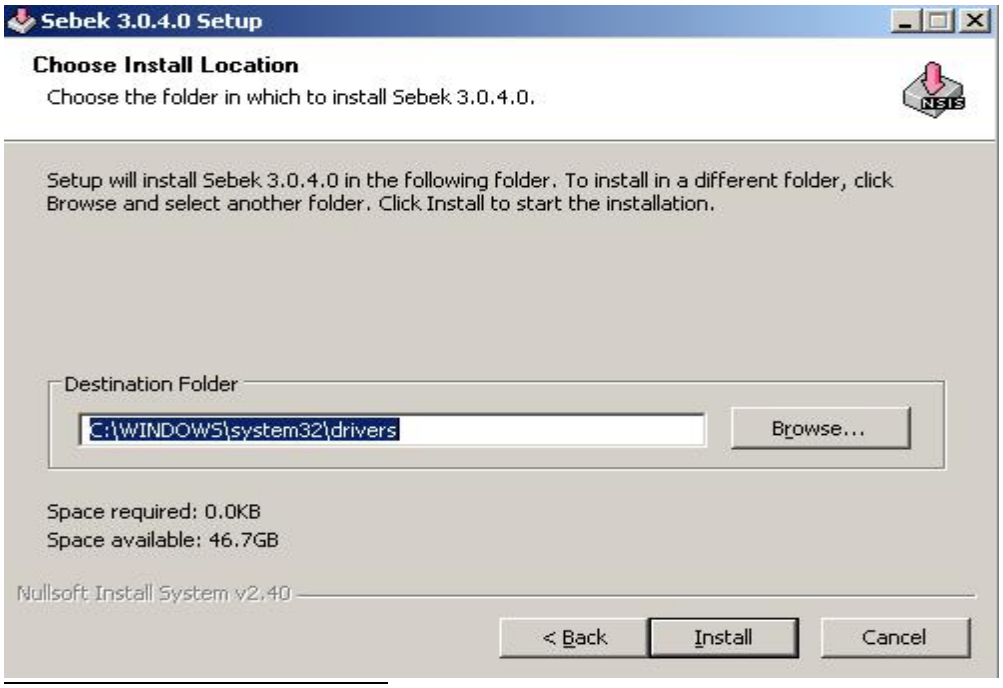
4.4.1.3.2 Aceptar Acuerdo de licencia.

Gráfico 76: Pantalla Acuerdo de Licencia[151]



4.4.1.3.3 Escoger la dirección de instalación.

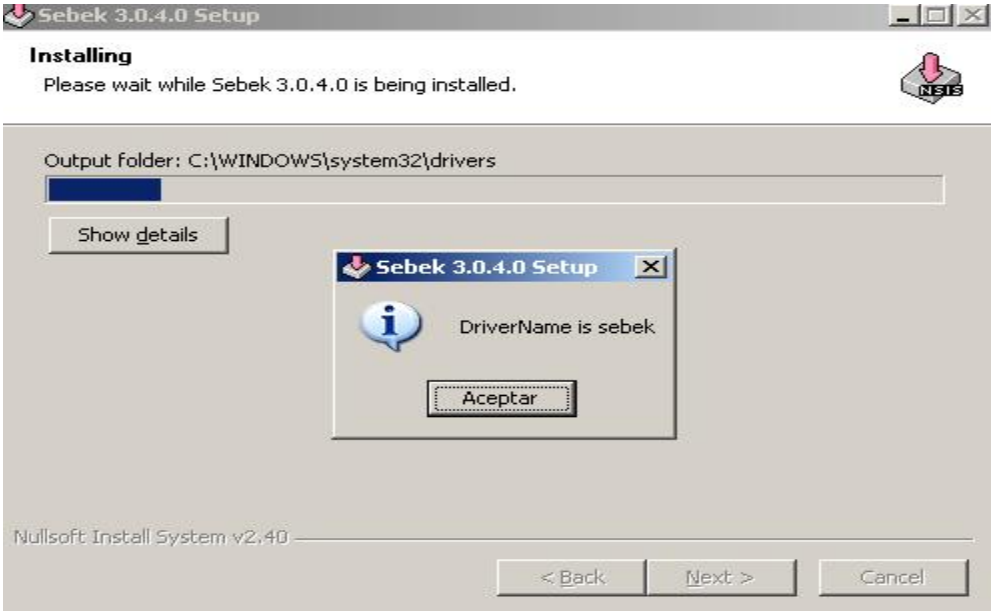
Gráfico 77: Pantalla Dirección de Instalación[152]



[151]Gráfico 76: Pantalla Acuerdo de Licencia, Realizado por: Jhonny Vaca
[152]Gráfico 77: Pantalla Dirección de Instalación, Realizado por: Jhonny Vaca

4.4.1.3.4 Instalación de Archivos Drivers.

Gráfico 78: PantallaInstalación de Archivos[153]



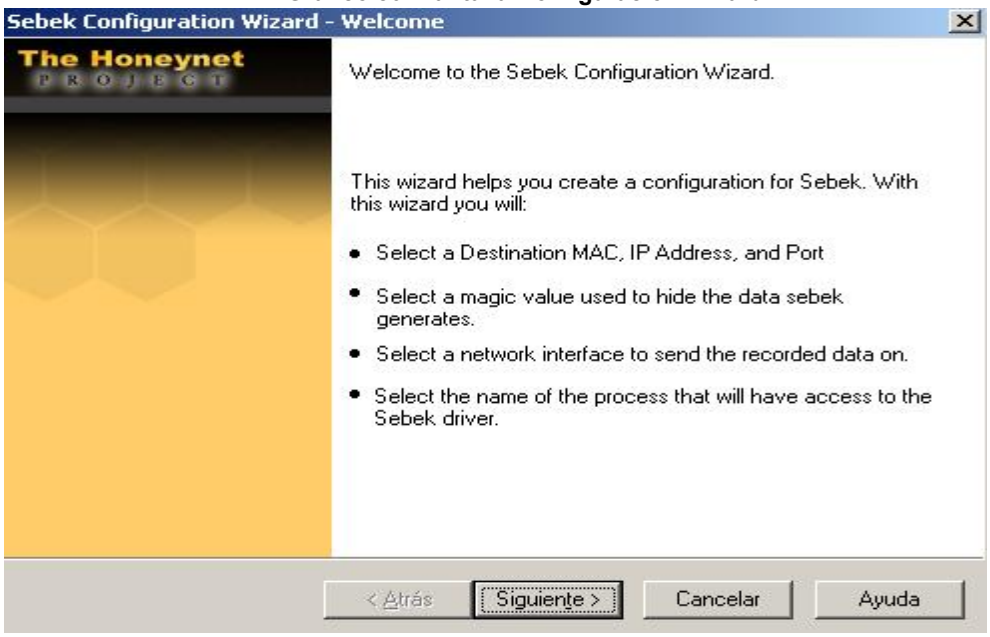
4.4.1.3.5 Finalizar instalación de archivos driver

Gráfico 79: Pantalla Instalación Driver completada[154]

[153]Gráfico 78: Pantalla Instalación de Archivos, Realizado por: Jhonny Vaca
[154]Gráfico 79: Pantalla Instalación Driver completada, Realizado por: Jhonny Vaca

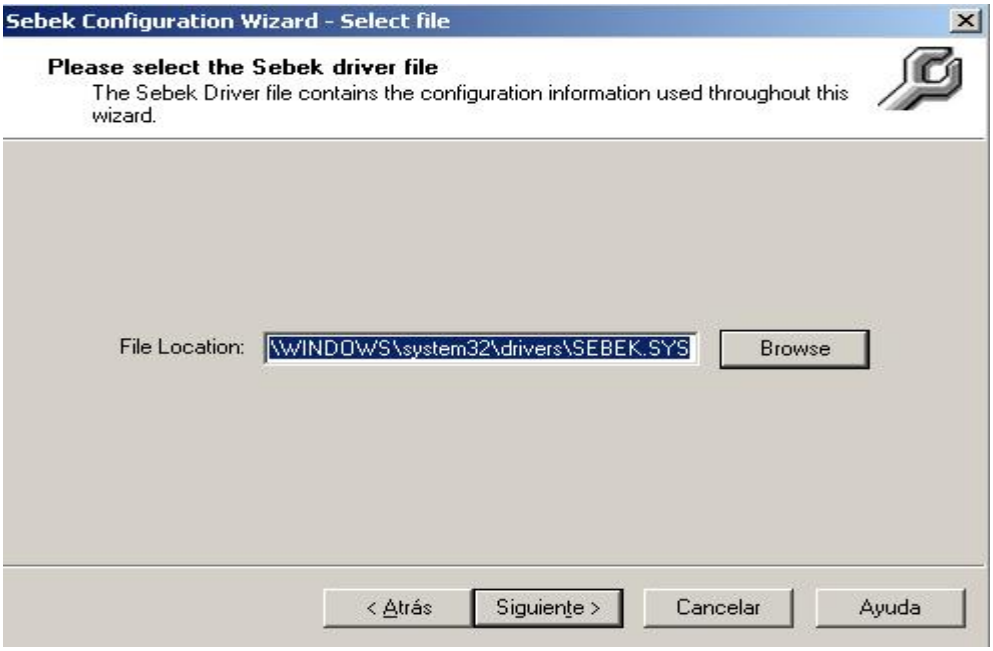
4.4.1.3.6 Ejecutar“Configuration Wizard.exe”

Gráfico 80: Pantalla Configuración Wizard[155]



4.4.1.3.7 Ubicar los Driver Instalados

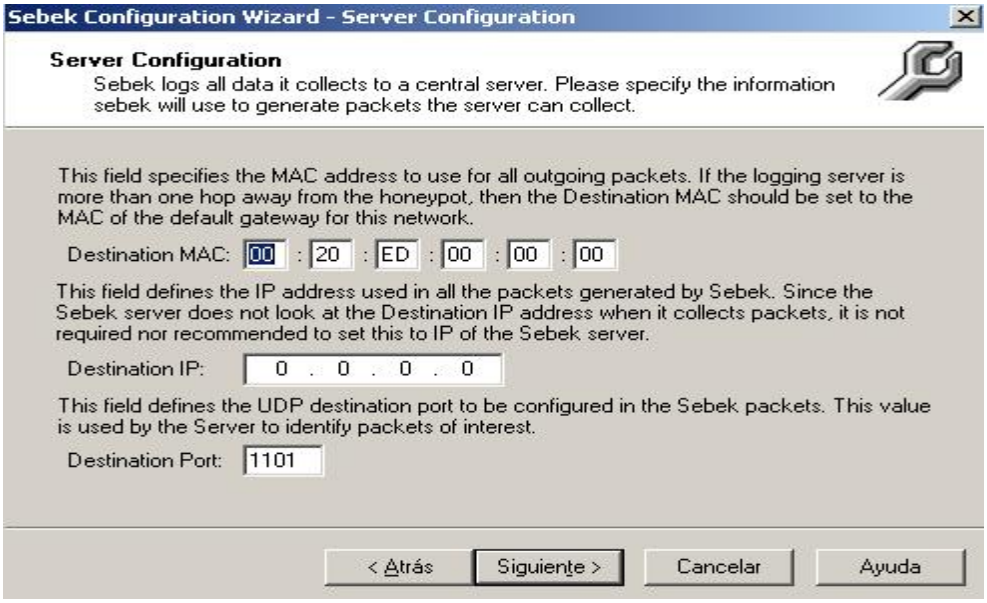
Gráfico 81: PantallaUbicación Driver[156]



[155]Gráfico 80: Pantalla Configuración Wizard, Realizado por: Jhonny Vaca
[156]Gráfico 81: Pantalla Ubicación Driver, Realizado por: Jhonny Vaca

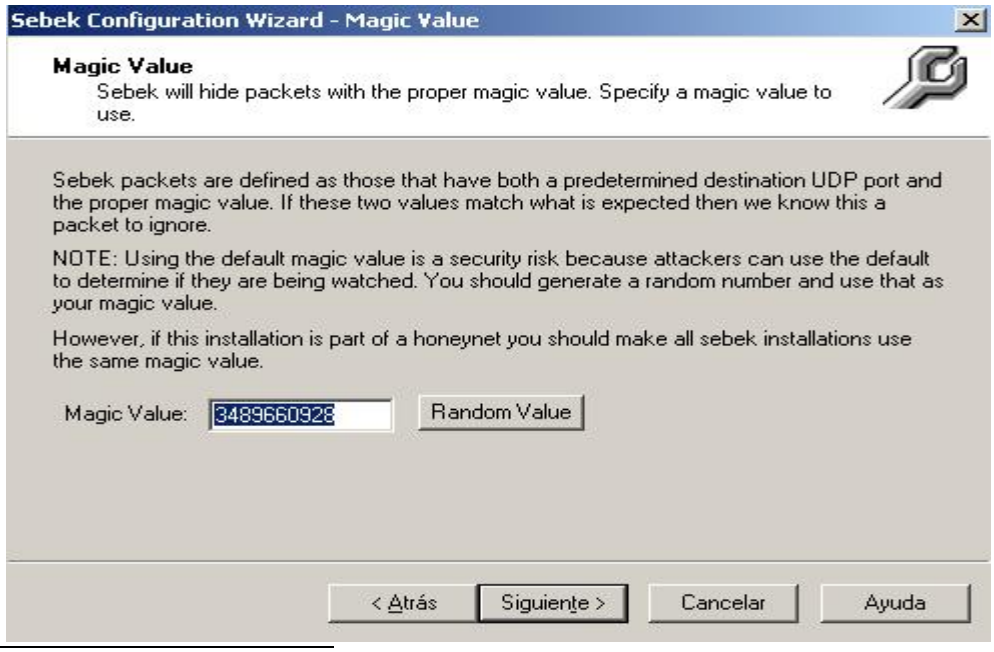
4.4.1.3.8 Configurar IP, Dirección MAC y Puerto destino de la honeywall

Gráfico 82: PantallaIP, MAC Puerto Destino[157]



4.4.1.3.9 Elegir el Valor Randomico

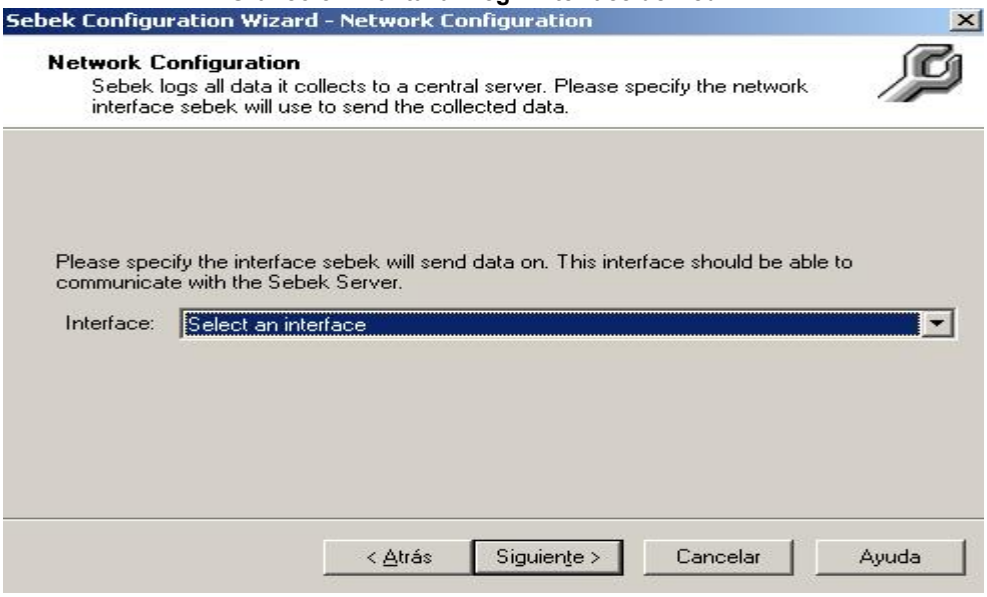
Gráfico 83: PantallaValorRandomico[158]



[157]Gráfico 82: Pantalla IP, MAC Puerto Destino, Realizado por: Jhonny Vaca
[158]Gráfico 83: Pantalla Valor Randomico, Realizado por: Jhonny Vaca

4.4.1.3.10Elegir Interface de Red que se comunicará con el servidor Sebek

Gráfico 84: Pantalla Elegir Interface de Red[159]



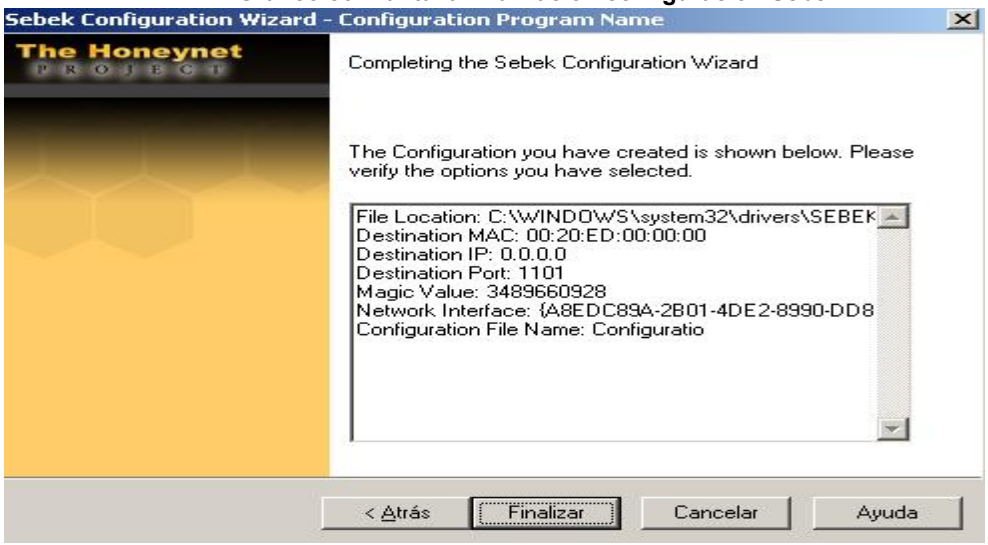
4.4.1.3.11Elegir el programa por defecto

Gráfico 85: PantallaPrograma por defecto[160]

[159]Gráfico 84: Pantalla Elegir Interface de Red, Realizado por: Jhonny Vaca
[160]Gráfico 85: Pantalla Programa por defecto, Realizado por: Jhonny Vaca

4.4.1.3.12Finalización de la configuración Sebek

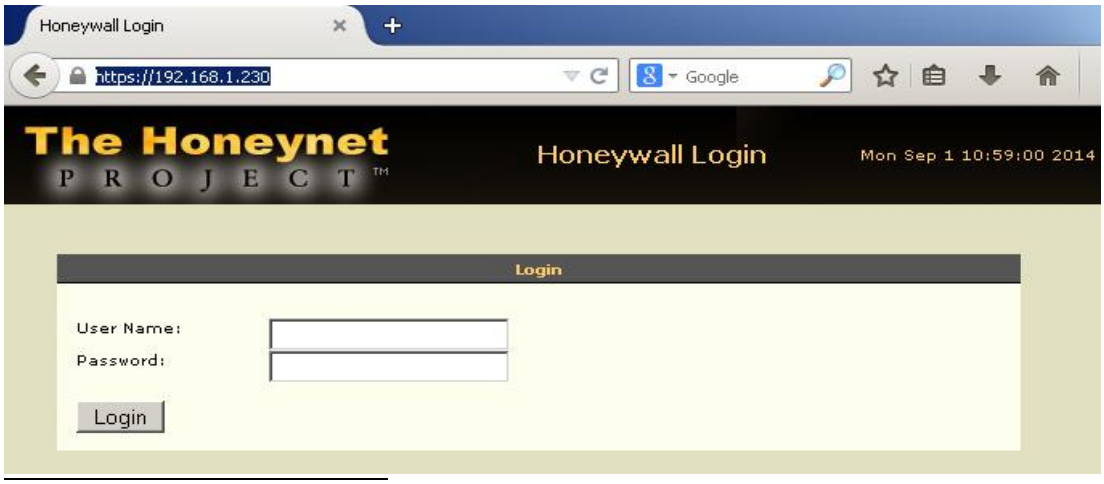
Gráfico 86: PantallaFinalización configuración Sebek[161]



4.4.1.4 Interface Web Walleye

4.4.1.4.1 Para Ingresar a la interface, iniciar un navegador desde el equipo o máquina virtual instalado Sebek. Ubicar la dirección IP de administración del honeywall, utilizar ssl.

Gráfico 87: PantallaIngresoInterface Web Walleyes[162]

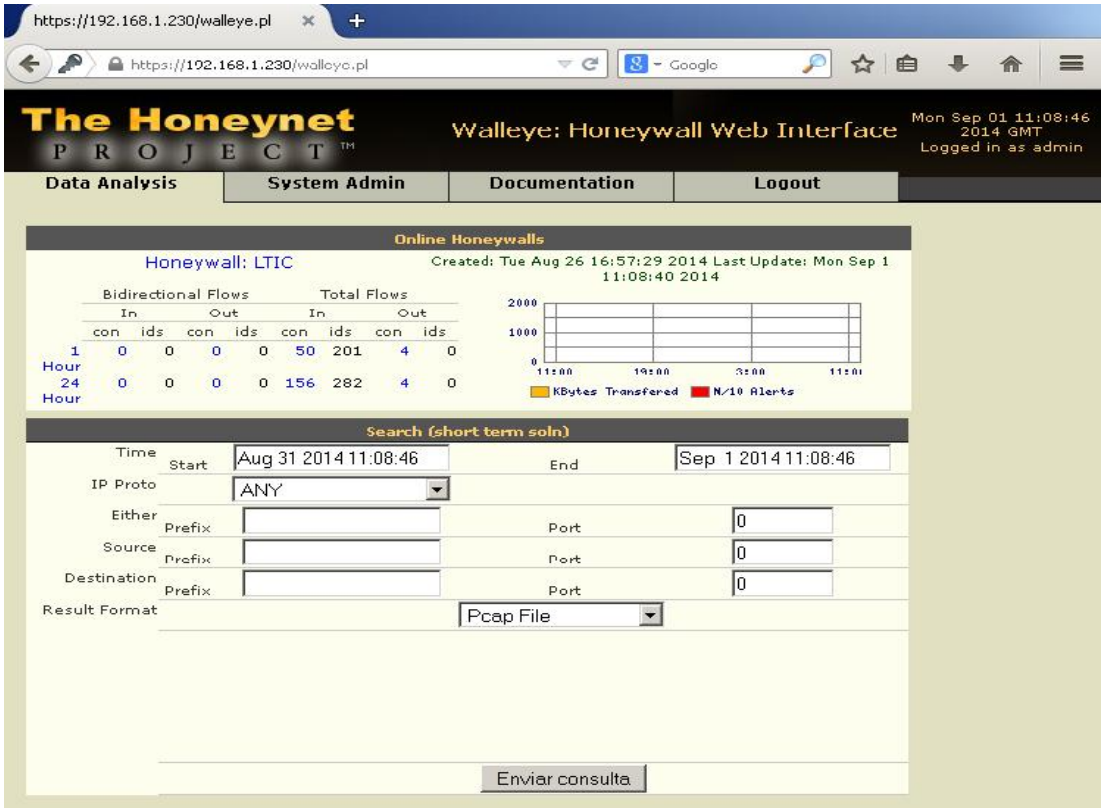


[161]Gráfico 86: Pantalla Finalización configuración Sebek, Realizado por: Jhonny Vaca
[162]Gráfico 87: Pantalla Ingreso Interface Web Walleyes, Realizado por: Jhonny Vaca

4.4.1.4.2 Cuando se ingresa por primera vez el usuario y el password por defecto son: **UserName:**roo ; **Password:** honey. Después dará la opción de cambiar el password.

4.4.1.4.3 Una vez registrado correctamente se puede ingresar a la interface Web Walleyes, lo cual podemos ver el monitoreo y análisis gráficamente.

Gráfico 88: Pantalla Interface Web Walleyes[163]



[163]Gráfico 88: Pantalla Interface Web Walleyes, Realizado por: Jhonny Vaca

4.4.1.5 Configuración del Honeypot

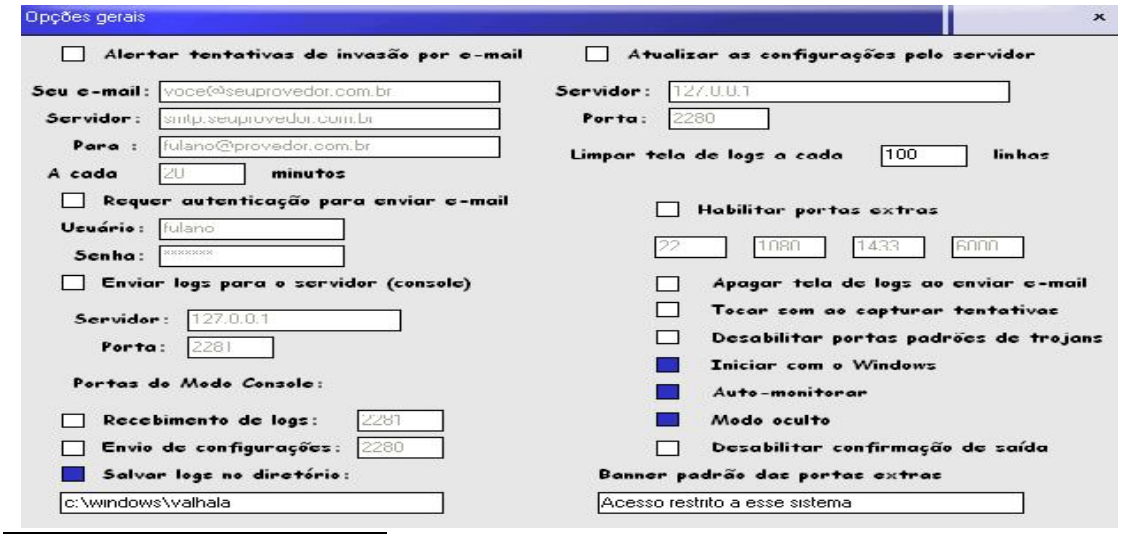
Se ha escogido el proyecto Valhala Honeypot 1.8 para Windows, este es un Honeypot de baja interacción, sin embargo incrementamos su interacción al conectarlo con el Honeywall.

4.4.1.5.1 Ejecutar el honeypot como administrador.

Gráfico 89: Pantalla Valhala Honeypot 1.8[164]

4.4.1.5.2 Seleccionar opciones y activar “Salvar logs no directorio”, “Iniciar con Windows”, “Auto-monitorear” y “Modo Oculto”

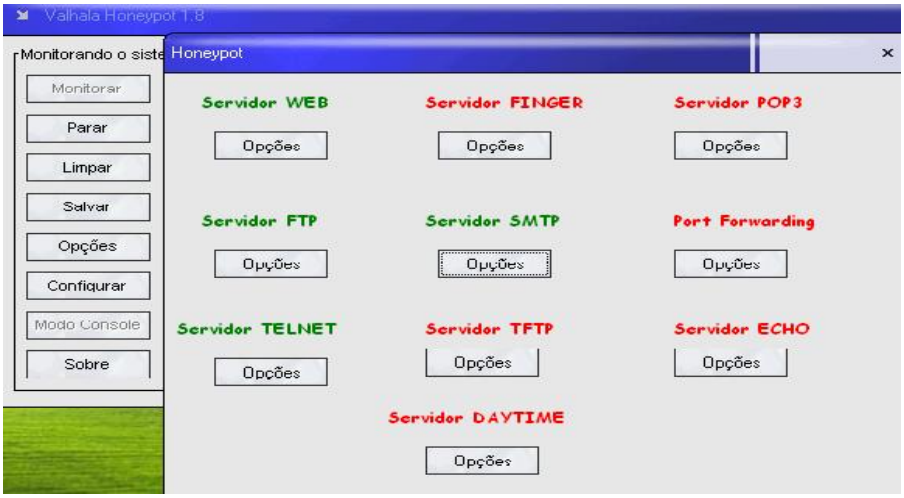
Gráfico 90: Pantalla Opciones Valhala Honeypot 1.8[165]



[164]Gráfico 89: Pantalla Valhala Honeypot 1.8, Realizado por: Jhonny Vaca
[165]Gráfico 90: Pantalla Opciones Valhala Honeypot 1.8, Realizado por: Jhonny Vaca

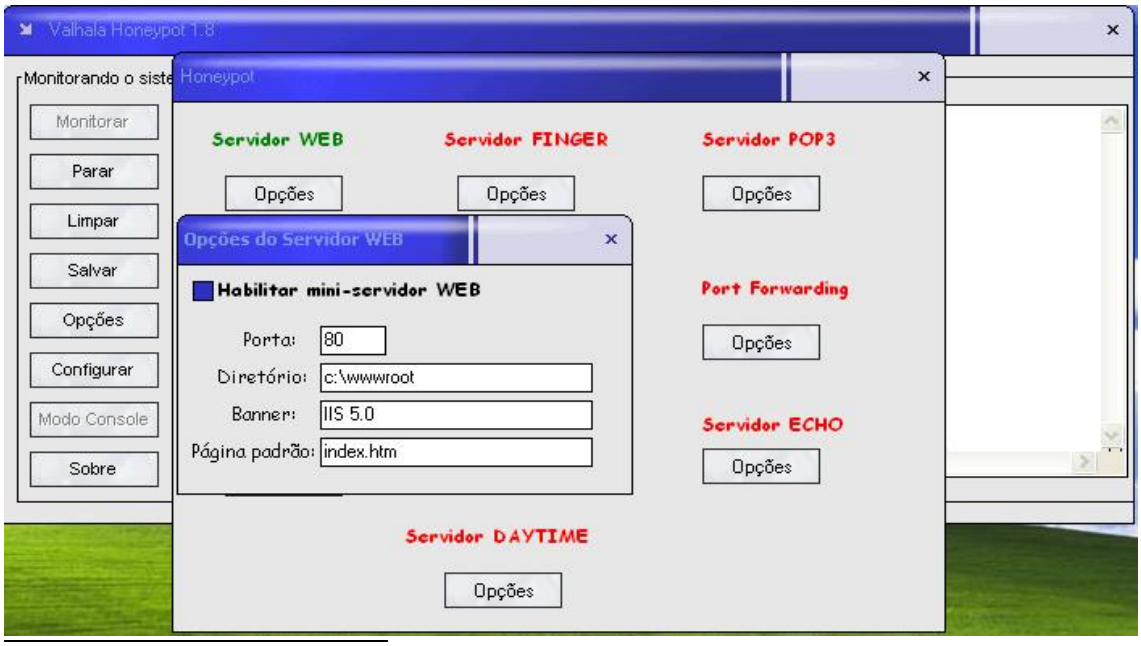
4.4.1.5.3 En el Botón Configurar se configura los servicios que se emularan con el honeypot.

Gráfico 91: Pantalla Opciones Valhala Honeypot 1.8[166]



4.4.1.5.4 En la opción Servidor Web, escoger el puerto, directorio y nombre de la página web. Es Necesario crear la carpeta y la página .htm

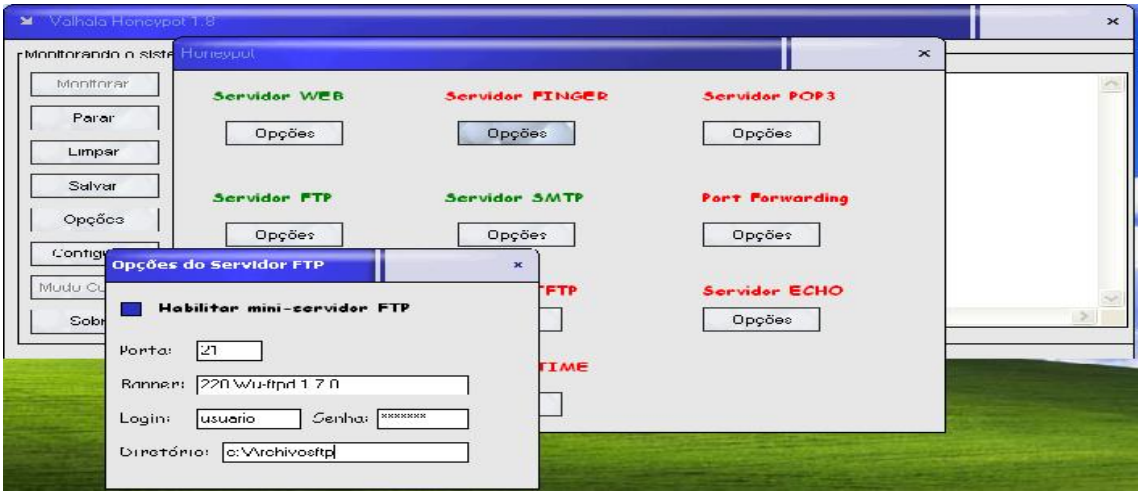
Gráfico 92: Pantalla Opciones Servidor Web[167]



[166]Gráfico 91: Pantalla Opciones Valhala Honeypot 1.8, Realizado por: Jhonny Vaca
[167]Gráfico 92: Pantalla Opciones Servidor Web, Realizado por: Jhonny Vaca

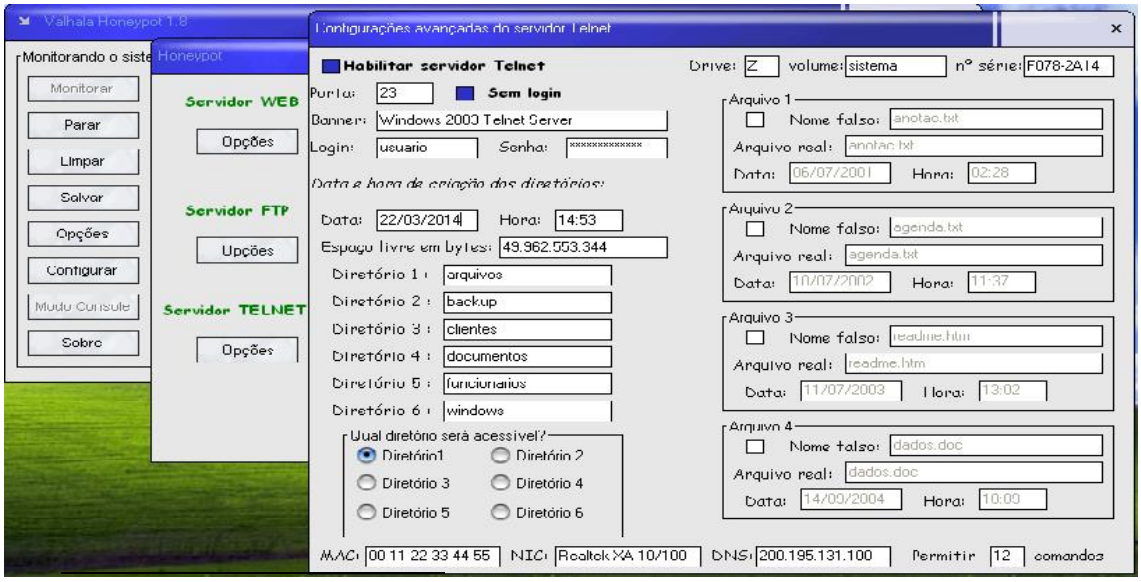
4.4.1.5.5 En la opción Servidor ftp, escoger el puerto, banner, usuario, password y carpeta que permitirá el ingreso.

Gráfico 93: Pantalla Opciones Servidor ftp[168]



4.4.1.5.6 En la opción Servidor TELNET, escoger el Banner, usuario, password, directorios falsos a los que se permiten ingresar, MAC, DNS de la víctima, volumen del sistema.

Gráfico 94: Pantalla Opciones Valhala Honeypot 1.8[169]



[168]Gráfico 93: Pantalla Opciones Servidor ftp, Realizado por: Jhonny Vaca
[169]Gráfico 94: Pantalla Opciones Valhala Honeypot 1.8, Realizado por: Jhonny Vaca

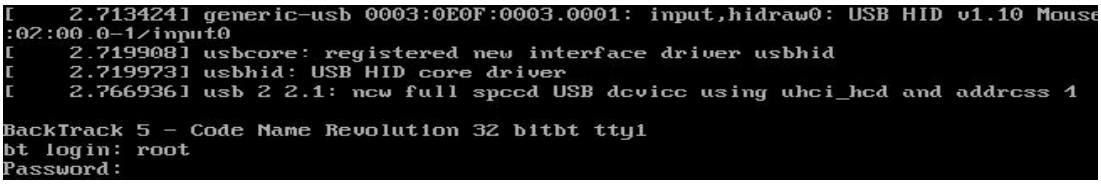
4.4.1.6 Herramienta utilizada para el ataque (BackTrack)

Esta herramienta de distribución GNU/Linux en formato LiveCD puede ser descargada de la siguiente ruta: http://www.backtrack-linux.org/downloads/

4.4.1.6.1 Una vez instalado, el usuario y password por defecto es:

Usuario: root ; **Password:** toor

Gráfico 95: Pantalla Ingreso 1BackTrack[170]



4.4.1.6.2 Para poder ingresar a la interface gráfica escribir:**startx.** Al estar en la consola grafica se puede comenzar los ataques.

Gráfico 96: Pantalla Ingreso 2BackTrack[171]

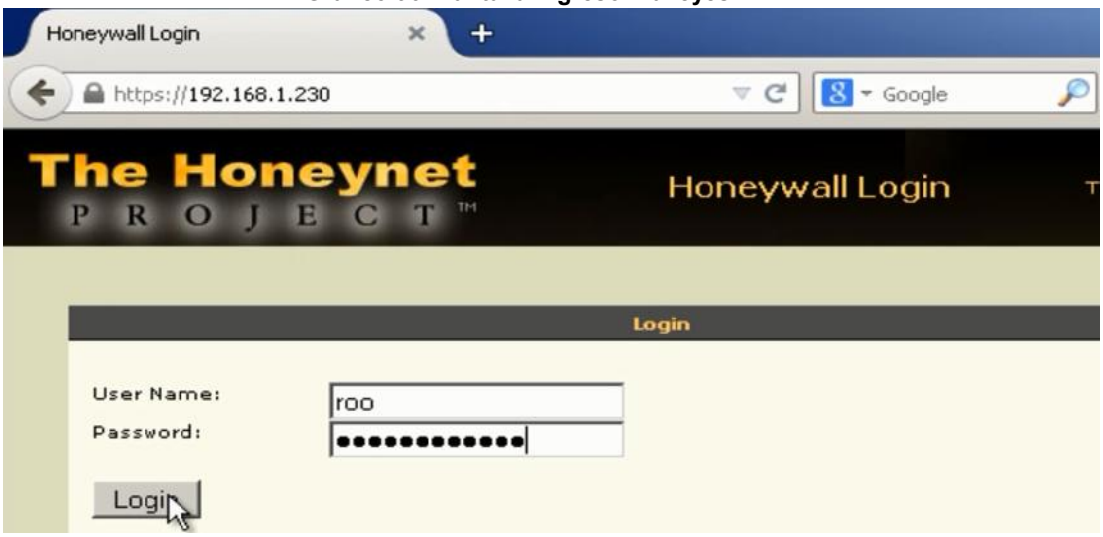
[170]Gráfico 95: Pantalla Ingreso 1BackTrack, Realizado por: Jhonny Vaca
[171]Gráfico 96: Pantalla Ingreso 2BackTrack, Realizado por: Jhonny Vaca

4.4.2 Pruebas de Funcionamiento de la Honeynet

Para la realización de las pruebas de funcionamiento de la honeynet, se realizó ataques simulados utilizaran la herramienta BackTrack, y en cada ataque se procederá a revisar los datos capturados en el honeywall.

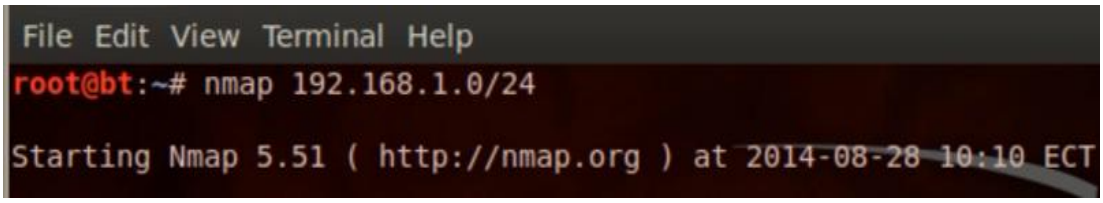
4.4.2.1 Abrir la interface (Walleye), con el usuario y claves definidos anteriormente.

Gráfico 96: Pantalla Ingreso Walleyes[172]



4.4.2.2 Con la herramienta BackTrack, se realiza el primer ataque simulado, la cual será un escaneo de la red a través del comando**Nmap**.

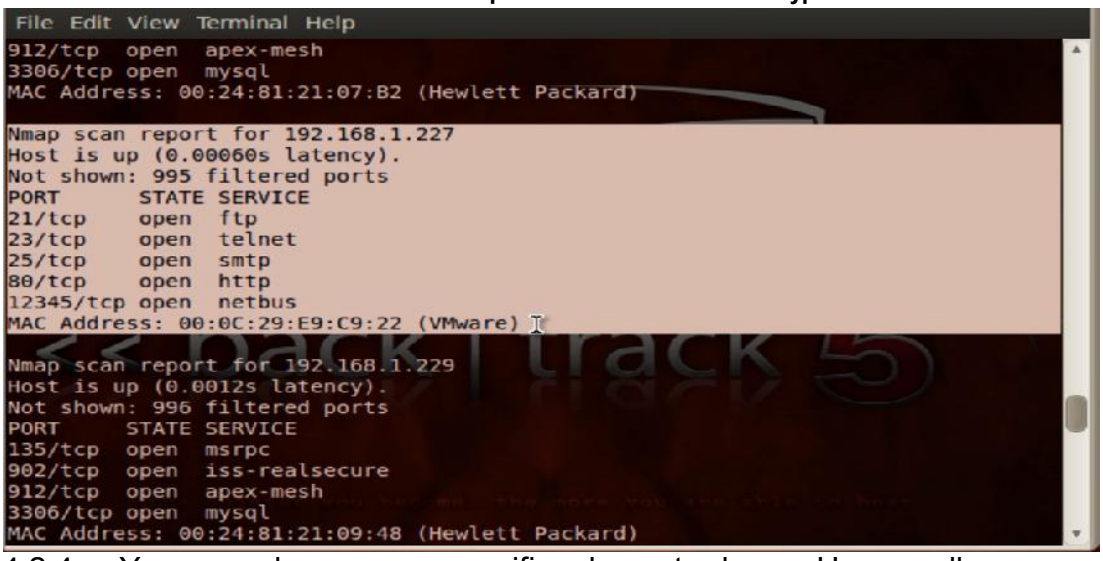
Gráfico 97: Comando Nmap[173]



[172] Gráfico 96: Pantalla IngresoWalleyes, Realizado por: Jhonny Vaca
[173] Gráfico 97: Comando Nmap, Realizado por: Jhonny Vaca

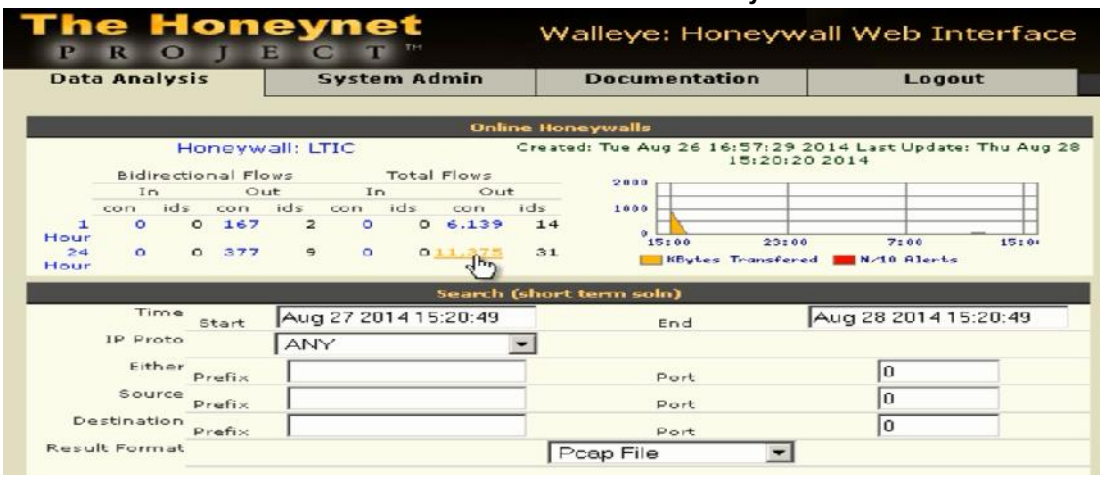
4.4.2.3 El comando Nmap, verifica los servicios y puertos que se encuentran abiertos en la red. Se observa que el escaneo ha detectado el honeypot de la honeynet, el cual se dejó intencionalmente los puertos abiertos.

Gráfico 98: Verificación de puertos abierto en el honeypot[174]



4.4.2.4 Ya se puede empezar a verificar las entradas en Honeywall

Gráfico 99: Verificación de entradas en la honeywall[175]



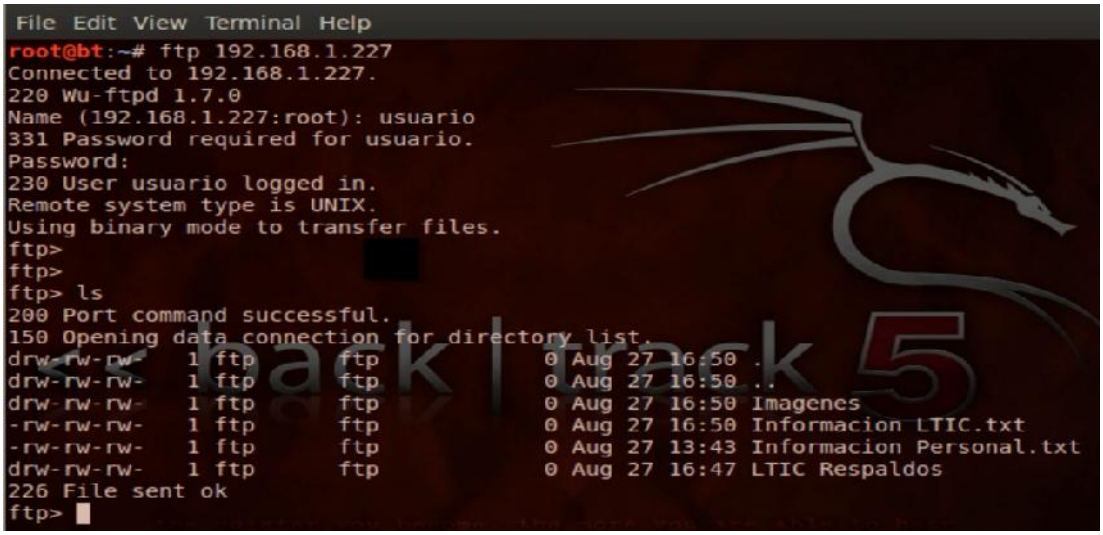
[174]Gráfico 98: Verificación de puertos abierto en el honeypot, Realizado por Jhonny Vaca
[175]Gráfico 99: Verificación de entradas en la honeywall, Realizado por Jhonny Vaca

4.4.2.5 Como se observa en el gráfico, se ha identificado un patrón en el tráfico generado del honeywall, el cual corresponde a al escaneo realizado por NMAP

Gráfico 100: Patrón NMAP en el tráfico generado[176]

4.4.2.6 Después que el atacante ha logrado identificar los objetivos vulnerables, tratara de acceder a los servicios que corren en dichos puertos abiertos, lo cual la honeywall capturará las actividades que realice dicho atacante.

Gráfico 101: Patrón NMAP en el tráfico generado[177]



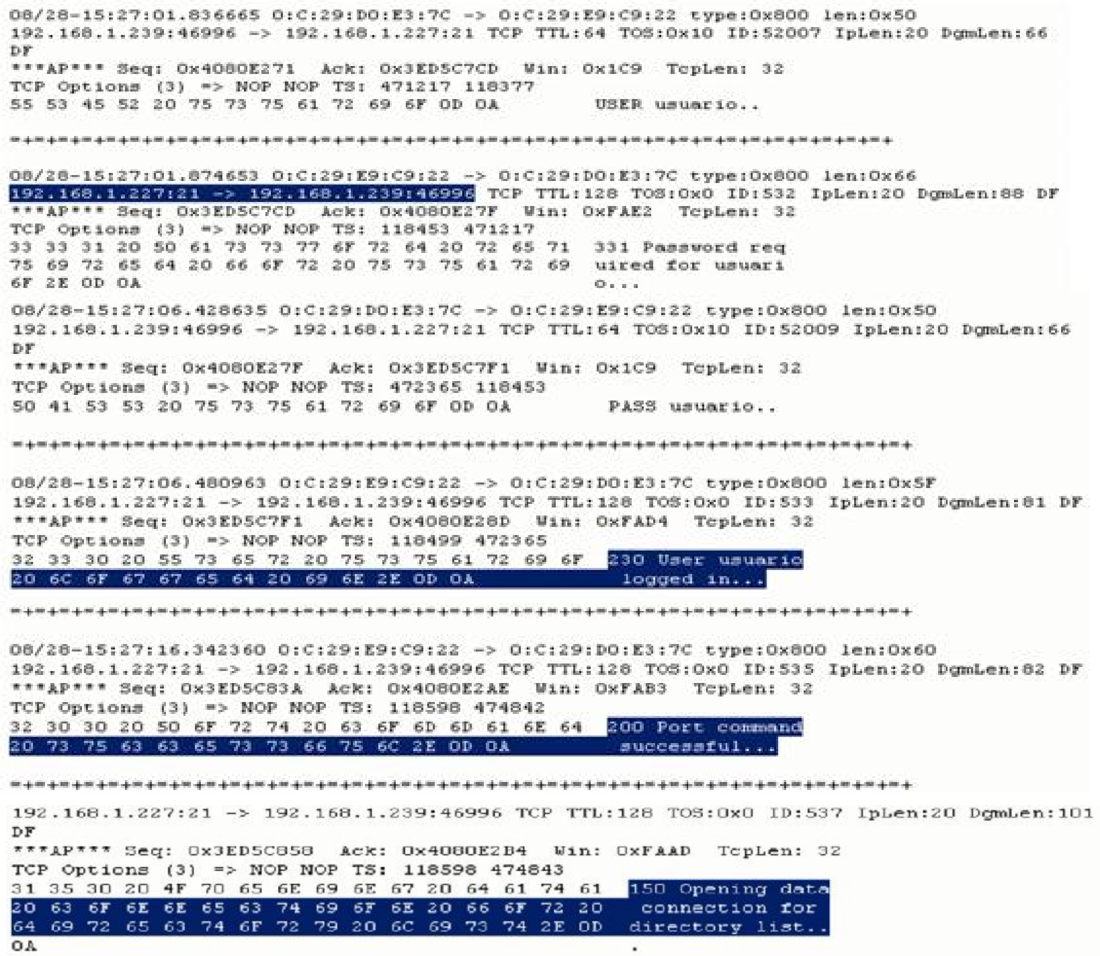
[176]Gráfico 100: Patrón NMAP en el tráfico generado, Realizado por Jhonny Vaca
[177]Gráfico 101: Patrón NMAP en el tráfico generado, Realizado por Jhonny Vaca

4.4.2.7 Se observa una captura de actividad ftp en el honeywall

Gráfico 102: Conexión ftp detectada en el honeywall[178]

4.4.2.8 Una vez que la actividad ftp ha sido capturada por el honeywall, es posible realizar un análisis más detallado.

Gráfico 103: Análisis en detalle de actividad ftp[179]

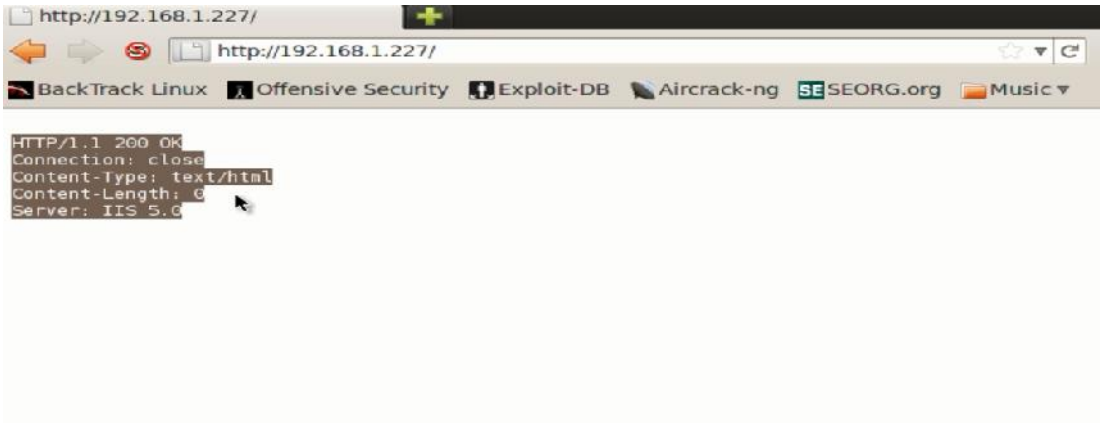


```
08/28-15:27:01.836665 0:C:29:D0:E3:7C -> 0:C:29:E9:C9:22 type:0x800 len:0x50
192.168.1.239:46996 -> 192.168.1.227:21 TCP TTL:64 TOS:0x10 ID:52007 IpLen:20 DgmLen:66
DF
***AP*** Seq: 0x4080E271  Ack: 0x3ED5C7CD  Win: 0x1C9  TcpLen: 32
TCP Options (3) => NOP NOP TS: 471217 118377
55 53 45 52 20 75 73 75 61 72 69 6F 0D 0A        USER usuario..

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

08/28-15:27:01.874653 0:C:29:E9:C9:22 -> 0:C:29:D0:E3:7C type:0x800 len:0x66
192.168.1.227:21 -> 192.168.1.239:46996 TCP TTL:128 TOS:0x0 ID:532 IpLen:20 DgmLen:88 DF
***AP*** Seq: 0x3ED5C7CD  Ack: 0x4080E27F  Win: 0xFAE2  TcpLen: 32
TCP Options (3) => NOP NOP TS: 118453 471217
33 33 31 20 50 61 73 73 77 6F 72 64 20 72 65 71  331 Password req
75 69 72 65 64 20 66 6F 72 20 75 73 75 61 72 69  uired for usuari
6F 2E 0D 0A                                      o...
08/28-15:27:06.428635 0:C:29:D0:E3:7C -> 0:C:29:E9:C9:22 type:0x800 len:0x50
192.168.1.239:46996 -> 192.168.1.227:21 TCP TTL:64 TOS:0x10 ID:52009 IpLen:20 DgmLen:66
DF
***AP*** Seq: 0x4080E27F  Ack: 0x3ED5C7F1  Win: 0x1C9  TcpLen: 32
TCP Options (3) => NOP NOP TS: 472365 118453
50 41 53 53 20 75 73 75 61 72 69 6F 0D 0A        PASS usuario..

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

08/28-15:27:06.480963 0:C:29:E9:C9:22 -> 0:C:29:D0:E3:7C type:0x800 len:0x5F
192.168.1.227:21 -> 192.168.1.239:46996 TCP TTL:128 TOS:0x0 ID:533 IpLen:20 DgmLen:81 DF
***AP*** Seq: 0x3ED5C7F1  Ack: 0x4080E28D  Win: 0xFAD4  TcpLen: 32
TCP Options (3) => NOP NOP TS: 118499 472365
32 33 30 20 55 73 65 72 20 75 73 75 61 72 69 6F  230 User usuario
20 6C 6F 67 67 65 64 20 69 6E 2E 0D 0A            logged in...

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

08/28-15:27:16.342360 0:C:29:E9:C9:22 -> 0:C:29:D0:E3:7C type:0x800 len:0x60
192.168.1.227:21 -> 192.168.1.239:46996 TCP TTL:128 TOS:0x0 ID:535 IpLen:20 DgmLen:82 DF
***AP*** Seq: 0x3ED5C83A  Ack: 0x4080E2AE  Win: 0xFAB3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 118598 474842
32 30 30 20 50 6F 72 74 20 63 6F 6D 6D 61 6E 64  200 Port command
20 73 75 63 63 65 73 73 66 75 6C 2E 0D 0A         successful...

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

192.168.1.227:21 -> 192.168.1.239:46996 TCP TTL:128 TOS:0x0 ID:537 IpLen:20 DgmLen:101
DF
***AP*** Seq: 0x3ED5C858  Ack: 0x4080E2B4  Win: 0xFAAD  TcpLen: 32
TCP Options (3) => NOP NOP TS: 118598 474843
31 35 30 20 4F 70 65 6E 69 6E 67 20 64 61 74 61  150 Opening data
20 63 6F 6E 6E 65 63 74 69 6F 6E 20 66 6F 72 20   connection for
64 69 72 65 63 74 6F 72 79 20 6C 69 73 74 2E 0D  directory list..
0A                                               .
```

[178] Gráfico 102: Conexión ftp detectada en el honeywall, Realizado por Jhonny Vaca
[179] Gráfico 103: Análisis en detalle de actividad ftp, Realizado por Jhonny Vaca

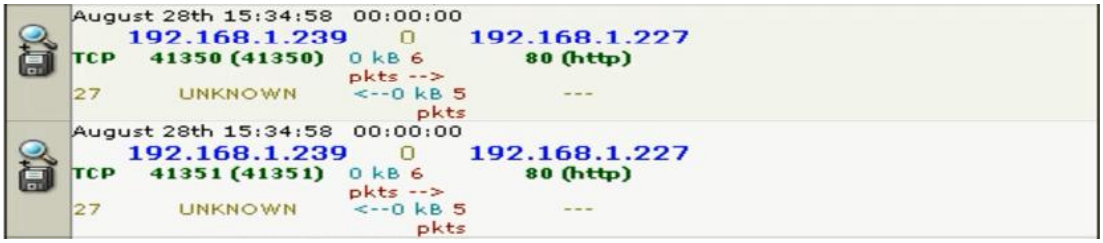
4.4.2.9 Ingreso a la página web falsa, creada por la honeypot previamente

Gráfico 104: Pagina web falsa[180]



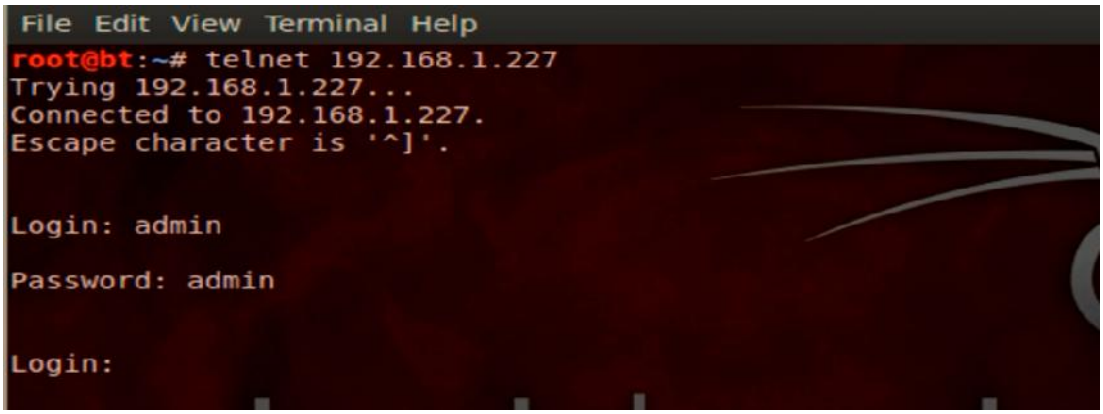
4.4.2.10 Se observa una captura de actividad http (80) en el honeywall

Gráfico 105: Captura de actividad http[181]



4.4.2.11 Comando de verificación del servicio telnet

Gráfico 106: Servicio Telnet[182]



[180]Gráfico 104: Pagina web falsa, Realizado por Jhonny Vaca
[181]Gráfico 105: Captura de actividad http, Realizado por Jhonny Vaca
[182]Gráfico 105: Servicio Telnet, Realizado por Jhonny Vaca

4.4.2.12 Se observa una captura de actividad Telnet (23) en la honeywall

Gráfico 107: Captura de actividad Telnet[183]

4.4.2.13 Una vez que la actividad Telnet ha sido detectada y capturada por el honeywall, es posible realizar un análisis más detallado

Gráfico 108: Análisis en detalle de actividad Telnet[184]

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

08/28-15:39:24.151802 0:C:29:D0:E3:7C -> 0:C:29:E9:C9:22 type:0x800 len:0x42
192.168.1.239:47434 -> 192.168.1.227:23 TCP TTL:64 TOS:0x10 ID:18788 IpLen:20 DgmLen:52
DF
***A**** Seq: 0xFCAE4CF6  Ack: 0xDE27EF3F  Win: 0x1C9  TcpLen: 32
TCP Options (3) => NOP NOP TS: 656775 125875

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

08/28-15:39:30.398628 0:C:29:D0:E3:7C -> 0:C:29:E9:C9:22 type:0x800 len:0x49
192.168.1.239:47434 -> 192.168.1.227:23 TCP TTL:64 TOS:0x10 ID:18789 IpLen:20 DgmLen:59
DF
***AP*** Seq: 0xFCAE4CF6  Ack: 0xDE27EF3F  Win: 0x1C9  TcpLen: 32
TCP Options (3) => NOP NOP TS: 658337 125875
61 64 6D 69 6E 0D 0A                                  admin..

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

08/28-15:39:30.403298 0:C:29:E9:C9:22 -> 0:C:29:D0:E3:7C type:0x800 len:0x44
192.168.1.227:23 -> 192.168.1.239:47434 TCP TTL:128 TOS:0x0 ID:578 IpLen:20 DgmLen:54 DF
***AP*** Seq: 0xDE27EF3F  Ack: 0xFCAE4CFD  Win: 0xFACE  TcpLen: 32
TCP Options (3) => NOP NOP TS: 125937 658337
0D 0A                                                 ..

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

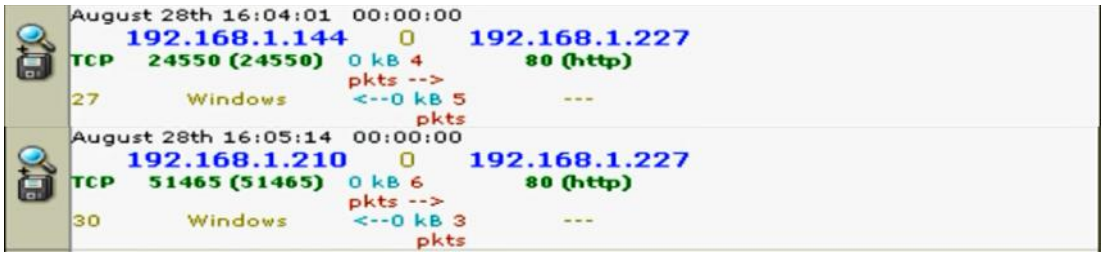
4.4.2.14 También se puede obtener un mínimo de detalle de las actividades maliciosas, directo del honeypot.

Gráfico 109: Resultados de la actividad telnet en honeypot[185]

[183]Gráfico 107: Captura de actividad Telnet, Realizado por Jhonny Vaca
[184]Gráfico 108: Análisis en detalle de actividad Telnet, Realizado por Jhonny Vaca
[185]Gráfico 109: Resultados de la actividad telnet en honeypot, Realizado por Jhonny Vaca

4.4.2.15 Durante las pruebas existió una actividad de http, de dos IPs diferentes, a la utilizada para simular los ataques.

Gráfico 110: Actividad http de IPs diferentes[186]



4.4.2.16 Actividad http de IPs diferentes, en honeypot

Gráfico 111: Actividad http de IPs diferentes en honeypot[187]

[186]Gráfico 110: Actividad http de IPs diferentes, Realizado por Jhonny Vaca
[187]Gráfico 111: Actividad http de IPs diferentes en honeypot, Realizado por Jhonny Vaca

CAPÍTULO V

Conclusiones y Recomendaciones

5.1 Conclusiones

1. A diferencia de los IDS o Firewalls tradicionales que generan demasiadas megas de ficheros logs con todo tipo de información que muchas veces no es necesaria; las Honeynets, generan un volumen pequeño de datos de altísimo valor.
2. Los datos que proporciona la Honeynet pueden ser analizados detenidamente, dando la posibilidad de aprender las tácticas más utilizadas por los atacantes, conocer las vulnerabilidades de la red y determinar los patrones de ataques que emplean los intrusos para comprometer los sistemas.
3. Con el debido estudio y conocimiento, las herramientas que se utilizan para implementar una honeynet son relativamente fácilesy rápidas de configurar. Su administración se vuelve sencilla a través de la interface gráfica (Walleyes).
4. La Honeynet es capaz de atraer la atención de un intruso mediante señuelos conformados por sistemas aparentemente vulnerables, ya sean reales o simulados, situados en un entorno controlado diseñado para vigilar las acciones de los intrusos.

5. Sin duda la honeynet, representa una alternativa de seguridad de bajo costo, ya que a través de los datos capturados en la misma, permite tomar decisiones y establecer políticas de seguridad en la red, además permite facilidad de movimiento, ahorro de espacio y hardware.
6. Mediante las pruebas realizadas y el análisis de los resultados obtenidos, el sistema ha funcionado correctamente, detectando los diferentes ataques que se ha llevado acabo, generando las respectivas alertas.
7. El Laboratorio de Tecnología de la Información y Comunicación – LTIC, no cuenta con ningún Sistema de Detección de Intrusos (IDS), lo cual puede representar unadesventaja de seguridad para los equipos de la red.

5.2 Recomendaciones

1. Se debe monitorear constantemente la honeynet para estar al tanto del tráfico que circule por ella y tomar la mejor decisión frente a los datos capturados.
2. Ubicar la honeynet en una zona donde no comprometa ningún sistema y evite que la red sufra daños.
3. Se recomienda utilizar la Honeynet no solo como medida de seguridad sino como herramienta de investigación para los estudiantes ya que constituye un recurso educativo ya que se puede aprender patrones de ataque y amenazas de todo tipo.
4. Una vez que los resultados de la honeynet sean analizados, se recomienda la planificación y ejecución de una política de seguridad que permita gestionar y reparar dichas vulnerabilidades informáticas.
5. El equipo anfitrión (host), donde se va a implementar la honeynetvirtual,debe ser de altas características, capaz de soportar las máquinas virtuales sin problemas de rendimiento. Además, se recomienda que los discos duros de la máquina donde se ha instalado la honeynet virtual tengan la suficiente capacidad de almacenamiento y procesamiento, debido a la cantidad de información que genera la misma.
6. Se debe tener un respaldo de seguridad de toda la información, en el caso de la honeynet auto contenida, tener respaldos de las máquinas

virtuales, con el fin de poder restablecer la Honeynet en caso de daños.

7. Se recomienda realizar el plan estratégico del LTIC, analizando el FODA y definiendo objetivos estratégicos para mejorar sus servicios y su seguridad.
8. Se recomienda que la Honeynet implementada en el LTIC, se mantenga en ejecución, ya sea para producción (para monitorear, analizar y recolectar información en ambiente real de la red del LTIC) o para investigación (no con la finalidad de proteger la red, sino proporcionar recursos educativos de naturaleza demostrativa y de investigación, para estudiar patrones de ataques).

ANEXOS DEL PROYECTO
ANEXO A

Casos de Delitos InformáticosImportantes a través de la Historia

- **Caso 1**

NOMBRE: WladimirLevin

DELITOS: Robo de más de US$ 10’000.000, de cuentas corporativas del Citibank-Rusia

SENTENCIA: 3 años de prisión. El Servicio Secreto de EUA, recuperó $240.000. El resto no ha sido recuperado

- **Caso 2**

NOMBRE: Kevin Mitnick, Alias —El Cóndor.

DELITOS: Ingresos a servidores, robo de información, y publicación en Internet de miles de números de tarjetas de crédito.

AFECTADOS: Visa, Motorola, Nokia, Novell, FBI, Pentágono.

SENTENCIA: Fue sentenciado a pasar 46 meses en una prisión federal y a pagar 4.125 dólares por daños.Salió de la cárcel en enero del 2000 y con la prohibición expresa de tocar un ordenador o dispositivo que le permita conectarse a Internet durante tres años a partir de su puesta en libertad.

- **Caso 3**

NOMBRE: Robert Tampan Morris, hijo de Robert Morris quien colaboro con el desarrollo del Internet.

DELITOS: Difundió el primer Virus - Gusano a través de ARPANET,

logrando infectar 6,000 terminales conectadas a la red.

SENTENCIA: 4 años de prisión y el pago de US $ 10,000 de multa y 400 horas de servicio comunitario. Su ataque inicio la conciencia de la inseguridad en la red.

- **Caso 4**

NOMBRE: Kevin Poulson, conocido pirata telefónico o phreker.

DELITOS: Interceptación de Comunicaciones, Fraude Informático

AFECTADOS: Logro intervenir la central de conmutación para que su línea telefónica sea seleccionada como la ganadora en multitud de concursos y ofertas telefónicas, mientras bloqueaba las de otros usuarios.

BENEFICIOS ILÍCITOS: Consiguió ganar 2 automóviles deportivos Porsche, 2 viajes a Hawai, y más de 22.000 dólares en efectivo.

- **Caso 5**

NOMBRE: Albert González, alias Jaguarll, Segvec, y Soupnazi

DELITOS: Acceso no autorizado a ordenadores, de cometer fraude en relación con éstos, de dañarlos y de conspiración para cometer fraude informático. Robo de información de tarjetas de Crédito y Débito.

AFECTADOS: Bancos y Tarjetas de Crédito, con un perjuicio de más de 130 millones de dólares, podría llegar a 263 millones de dólares.

SENTENCIA: Sentenciado a 70 años de Prisión. El 18 de marzo del 2010[188]

[188]Dr. Santiago Acurio Del Pino. 2010. Pontificia Universidad Católica del Ecuador. Los Delitos Informáticos en el Ecuador

ANEXO B

1. Del correcto uso del LTIC en general

a. Hacer buen uso de la infraestructura física, equipos, programas y otros implementos que están en el LTIC.
b. No está permitido fumar, ingerir alimentos, ni ingresar con mascotas a las instalaciones del LTIC.
c. La infraestructura física, los equipos, las aplicaciones y otros implementos del LTIC son exclusivamente para uso académico.
d. Toda persona sin excepción debe registrarse en la ventanilla de atención e indicar el propósito de su presencia.
e. El documento válido para ingresar al LTIC es el carné de la Universidad, en caso de que no se tuviere este documento se requiere autorización expresa del director del LTIC.
f. El horario de atención del LTIC es de 07:00 a 20:00 de Lunes a Viernes en los días laborables de la Universidad.
g. El horario de asignación y disponibilidad de aulas del Laboratorio se publicará oportunamente en la cartelera, debiendo los estudiantes, docentes y administrativos respetar de manera estricta dicho horario.
h. Las instalaciones sanitarias están identificadas y son de uso exclusivo de los usuarios del laboratorio.

2. Del correcto uso de las AULAS.

a. Las AULAS están equipadas con diez y seis (16) computadoras personales conectadas en red. Está permitido utilizar las computadoras portátiles de los estudiantes en las horas de clase.

b. Las AULAS del LTIC son exclusivamente para sesiones prácticas de las cátedras o cursos que demanden uso de computadoras. La Dirección de Informática, tiene aulas que pueden ser reservadas para proyecciones o para la utilización de herramientas de ofimática.

c. Los ***docenteso instructores***, deben hacer uso de las aulas asignadas de acuerdo al horario establecido en cada semestre o a la reserva confirmada de la misma, de acuerdo al siguiente procedimiento:

- El docente o instructor debe retirar la llave del aula asignada, en la oficina de Becarios, en el instante que va a iniciar su clase y entregar una identificación para registro.
- El docente o instructor puede solicitar un proyector, si fuera del caso, el mismo que está sujeto a la disponibilidad de equipos en el LTIC.
- Los estudiantes no pueden ingresar al aula de clase sin presencia del docente o instructor respectivo.
- Durante el uso del aula, el docente o instructor, es el responsable directo de todos los equipos y de hacer cumplir las normas internas del Laboratorio.

- El docente o instructor debe notificar de inmediato cualquier novedad a los ayudantes en lo que respecta al correcto funcionamiento de los equipos del aula.
- Una vez terminada la clase todos los alumnos deben salir del aula, apagando los equipos utilizados, incluye apagar el monitor.
- Al final de la clase, el docente deberá devolver la llave del aula y el proyector en caso de haberlo solicitado, en la oficina de becarios y retirará su identificación.

d. El becario o ayudante de turno debe verificar el estado de entrega o recepción del aula y cualquier novedad informará al Director o Asistente.

e. La reservación de un aula solo la puede hacer un docente, indicando fecha, horario, cátedra, curso y paralelo, con un mínimo de 24 horas de anticipación, enviando un correo electrónico al Director y Asistente. La confirmación de la reserva se hará por este medio.

f. La reserva de aulas se sujetará a la disponibilidad de horario, así como al software y hardware existentes en cada aula.

g. Se dispondrá del aula, si el docente no asiste en los veinte minutos iniciales de cada reserva.

h. Si el docente no va a utilizar el aula reservada debe notificar de este particular a los administrativos del LTIC.

3. Del correcto uso de Computadoras Personales.

a. Las computadoras personales del LTIC, son de **uso educativo exclusivamente**, cualquier otro tipo de utilización debe ser autorizado por el Director.

b. Para utilizar un computador, es necesario contar con su respectivo usuario y contraseña. En caso de no tenerlos, debe solicitar su creación al Becario de turno, previo la verificación de estar matriculado actualmente en la Facultad de Ingeniería o con la autorización del Director.

c. Toda persona que desea utilizar una computadora, deberá registrarse en la ventanilla de atención, allí se le asignará un computador en función de la disponibilidad de los mismos.

d. El registro de usuarios, determinará la responsabilidad en caso de detectarse daños en los equipos. Consecuentemente el daño se imputará al usuario registrado, sin facultad para transferir su utilización a terceros.

e. El usuario que encuentre algún daño o des configuración en la computadora, deberá informar del particular inmediatamente al ayudante de turno, quien registrará la novedad.

f. Es responsabilidad del usuario devolver la computadora en perfectas condiciones luego de su utilización.

g. El límite máximo de personas por computadora es de dos (2), no se permiten acompañantes adicionales.

h. No está permitido el movimiento de computadoras, ni de sus componentes como son teclado, mouse o monitor.

i. No está permitido abrir las computadoras o desconectarlas de la red.

4. Del correcto uso del acceso a Internet.

a. El acceso al Internet del LTIC, es de **uso educativo exclusivamente**, cualquier otro tipo de utilización debe ser autorizado por el Director.

b. Los usuarios se sujetarán a las restricciones de seguridad y velocidades de acceso definidas por los administrativos del LTIC.

c. Está prohibido la navegación a sitios con contenido: pornográfico, videos, música, Chat, juegos.

d. No están permitidas las descargas en general (software de prueba, componentes, videos, entre otros), y en caso de ser necesario se debe solicitar al becario de turno el requerimiento, el mismo que tendrá autorización del Director para efectuarla y entregarla.

5. Del correcto uso del Software en general

a. Todo software (programa) que se instala en el Laboratorio, cumple con los lineamientos establecidos por la Universidad, respetando las leyes de propiedad intelectual, uso GNU o licencias demostrativas.

b. No está permitido instalar y/o utilizar software no autorizado por los administrativos del Laboratorio.

c. No está permitido cambiar la configuración o cambio de parámetros establecidos en el software instalado.
d. El listado actualizado del software disponible se encuentra publicado en la Intranet de la Facultad.
e. Los ayudantes o becarios, pueden entregar una copia únicamente del software permitido, licencias Software Libre o trials demostrativos.
f. El software licenciado no se puede transferir a terceras personas, son uso exclusivo del Laboratorio.
g. La actualización del software dependerá de la disponibilidad del LTIC para adquirir nuevas versiones. En especial si se trata de software licenciado.

6. De las sanciones

a. Para quienes incumplan con lo establecido en esta normativa, se aplicará lo contemplado en el Art.7 del Reglamento del Laboratorio de la Facultad de Ingeniería.

   Además se contempla las siguientes sanciones para los siguientes casos:

b. Cualquier estudiante que se encuentre jugando dentro del Laboratorio tendrá como primera sanción la prohibición de uso de cualquier computadora por un día.
c. En caso de reincidir se prohibirá su ingreso durante una semana.

d. En caso de ser nuevamente encontrado jugando se le prohibirá el acceso definitivo al Laboratorio el tiempo que reste del semestre que este cursando.
e. Un estudiante sancionado, solo podrá ingresar a sus horas de clases prácticas y a exámenes.

GLOSARIO DE TERMINOS

A

AppleTalk:es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes.

ATM: El Modo de Transferencia Asíncrona(Asynchronous Transfer Mode)

B

BIOS: El Sistema Básico de Entrada/Salida (Basic Input-Output System)

C

CAN: Red de Campus Area / Controller Area Network / Cluster

D

DAN: DeskArea Networks

DNS: Sistema de Nombres de Dominio (DomainNameSystem)

DOS: Ataque de denegación de servicio (Denial of Service)

E

Ethernet: Define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

F

FDDI: Interfaz de Datos Distribuida por Fibra (FiberDistributed Data Interface)

Firewall o Cortafuego: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

FrameRelay: La técnica FrameRelay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

FTP: Protocolo de Transferencia de Archivos (File Transfer Protocol)

G

GIF: Graphic Interchange Format

H

HDLC:(High-Level Data Link Control, control de enlace de datos de alto nivel)

I

ITSEM - Information Technology Security Evaluation Manual

IDS: Un sistema de detección de intrusos (IntrusionDetectionSystem)

IEC: International Electro technicalCommission

IP: InternetProtocol (Protocolo de Internet')

IPv6: El Internet Protocoloversión 6 (IPv6) /Protocolo de Internet versión 6, es una versión del protocolo Internet Protocolo(IP), diseñada para reemplazar a Internet Protocoloversión 4, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

IPX:(Internet Packet Exchange - Intercambio de Paquetes interred). Protocolo para el intercambio de paquetes entre aplicaciones dentro de una red Netware. Actualmente este protocolo está en desuso y sólo se utiliza para juegos en red antiguos.

IRC (Internet Relay Chat): es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior.

ISO/IEC 27001: Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005

ISO: International Organization for Standardization

L

LAN: Local Area Networks

LOG: Aarchivoqueguardalainformacióndeloqueserealizaenel sistema.

M

MALWARE: Tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

MAN: Red de área metropolitana (MetropolitanArea Network)

MS-DOS: MS-DOS (siglas de MicroSoft Disk OperatingSystem, Sistema operativo de disco de Microsoft) es un sistema operativo para computadoras basados en x86. Fue el miembro más popular de la familia de sistemas operativos DOS de Microsoft, y el principal sistema para computadoras personales compatible con IBM PC en la década de 1980 y mediados de

1990, hasta que fue sustituida gradualmente por sistemas operativos que ofrecían una interfaz gráfica de usuario, en particular por varias generaciones de Microsoft Windows.

N

NetBEUI: NetBEUI (NetBIOS Extended User Interface, en español Interfaz extendida de usuario de NetBIOS), es un protocolo de nivel de red sin encaminamiento y bastante sencillo utilizado como una de las capas en las primeras redes de Microsoft. NetBIOS sobre NetBEUI es utilizado por muchos sistemas operativos desarrollados en 1990, como LAN Manager, LAN Server, Windows 3.x, Windows 95 y Windows NT.

NetBIOS: Es un protocolo de aplicación para compartir recursos en red. Se encarga de establecer la sesión y mantener las conexiones. Pero este protocolo debe transportarse entre máquinas a través de otros protocolos; debido a que por sí mismo no es suficiente para transportar los datos en redes LAN como WAN, para lo cual debe usar otro mecanismo de transporte

P

PAN: Personal Area Networks

PPP: Point-to-pointProtocolo (en español Protocolo punto a punto)

R

RST: Resetear Conexión: Al haber algún error o pérdida de paquetes de envío se establece envío de Flags RST:

S

SAN: Red del Sistema de Área / Area Network Server / Pequeñas redes de área

SGSI: Sistema de Gestión de la Seguridad de la Información.

SMTP: Simple Mail Transfer Protocolo

SQL:SQL corresponde a la expresión inglesa StructuredQueryLanguage (entendida en español como Lenguaje de Consulta Estructurado), la cual identifica a un tipo de lenguaje vinculado con la gestión de bases de datos de carácter relacional que permite la especificación de distintas clases de operaciones entre éstas.

SSH:(Secure Shell): este fue desarrollado con el fin de mejorar la seguridad en las comunicaciones de internet. Para lograr esto el SSH elimina el envío de aquellas contraseñas que no son cifradas y codificando toda la información transferida

STP: SpanningTreeProtocolo) es un protocolo de red de nivel 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El STP es un protocolo de prevención de bucles físicos en la LAN. El STP permite que los switches se comuniquen para descubrir loops (bucles) físicos en lared y eliminarlos.

T

TCP (Transmision Control Protocolo)

TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet

Telnet: Telnet es el acrónimo de Telecommunication Network. Se trata del nombre de un protocolo de red que se utiliza para acceder a una computadora y manejarla de forma remota.

TheHoneynet Project: Es una organización de investigación no lucrativa dedicada al aprendizaje de las herramientas, tácticas y motivos de la comunidad blackhat y a compartir las lecciones aprendidas.

TI: Tecnología de la Información.

U

UDP (UserDatagramProtocolo) / Protocolo de Datagrama de Usuario

V

VPN – Red Privada Virtual / Virtual Private Network

W

WAN: Redes de área amplia (Wide Area Network)

Wi-Fi: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

WLAN: Red de área local inalámbrica (Wireless Local Area Network)

X

X.25: Puede usarse como protocolo de WAN para establecer comunicaciones con socios comerciales, otras organizaciones, proveedores y clientes, tanto a nivel nacional como internacional

XML:eXtensibleMarkupLanguage / Lenguaje de Marcas eXtensible') Es un sistema estándar de codificación de información. Los programas que utilizan el formato XML pueden intercambiar fácilmente sus datos, ya que responden a una misma lógica interna.