Honeynet Virtual Híbrida en el entorno de red de la Universidad Técnica Del Norte de la ciudad de Ibarra

Edgar A. Maya, Tatiana A. Vinueza

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

Se proporciona una solución de seguridad integrada, fusionando las ventajas de la tecnología Honeynet con la de los sistemas de detección de intrusos de red, de modo que, además de contar con una red altamente controlada para contener y analizar ataques en vivo, se monitorice y detecten vulnerabilidades en la red en producción.

***Términos Indexados*—Honeynet, honeywall, honeypot, malware.**

I. INTRODUCCIÓN

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

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

Documento recibido el 7 de noviembre de 2012. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.

E.A. Maya, trabaja en la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador (teléfono: 5936-2955-413; e-mail: eamaya@utn.edu.ec).

T.A. Vinueza, egresada de la Carrera de Ingeniería Electrónica y Redes de Comunicación (teléfono: 5936-2923-025; e-mail: tavinueza@utn.edu.ec).

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

II. CONCEPTOS BÁSICOS

A. Honeypot

Se denomina honeypot (tarro de miel) al recurso de red destinado a ser atacado o comprometido con la finalidad de identificar, evitar y en cierta medida, neutralizar los intentos de secuestrar sistemas y redes de información. [1]

Pueden considerarse como falsos servidores posicionados en lugares estratégicos de una red de prueba, con información que parece ser valiosa para los intrusos. Se los configura de tal manera que se dificulte, pero que no sea imposible romper su seguridad, exponiéndolos deliberadamente y haciéndolos muy atractivos para hackers en busca de un objetivo.

Nivel de Interacción

Se refiere al grado de interacción que se admite que el atacante tenga con un honeypot. Se distinguen: Honeypots de Baja, Media y Alta interacción. [2]

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

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

- **Alta Interacción.-** Constituyen una solución bastante compleja, puesto que implican la utilización de sistemas operativos y aplicaciones implementadas en hardware real, evitando la necesidad de utilizar software de emulación. Proporcionan una gran cantidad de información acerca del modo de actuar de los atacantes, permitiendo que se descubran nuevas herramientas de hacking e identifiquen vulnerabilidades.

Medio de Implementación

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

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

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

Propósito de implementación

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

- **Honeypot de Producción.-** Utilizados para proteger a los entornos operativos en producción y distraer la atención de los atacantes. Se implementan en forma paralela a las redes de datos o infraestructuras de IT, y están sujetas a sufrir constantes ataques.

- **Honeypot de Investigación.-** Tienen como objetivo recolectar información, analizar los tipos y patrones de los ataques existentes en la actualidad. Generalmente, las implementan empresas dedicadas a la seguridad de la información, organismos de investigación como universidades, agencias gubernamentales y militares.

B. *Honeynet*

Una honeynet básicamente es una red de honeypots que tiene como fin el proporcionar información valiosa sobre los métodos y recursos utilizados por la comunidad Blackhat para cometer ataques informáticos. Se las conoce también como honeypots de alta interacción. Reflejan un entorno de red productivo al trabajar con varios sistemas a la vez. Entre ellos Linux, Solaris, Windows, routers Cisco, etc. [3]

Honeynets virtuales

Una honeynet virtual es una solución que permite implementar una honeynet completa en un ambiente virtual. Puede desarrollarse utilizando diversas herramientas de virtualización, tales como: VMware, User Mode Linux y Xen.

Se la puede clasificar en dos tipos:

- **Honeynet Auto contenida.-** Es aquella que emplea únicamente una máquina física para ejecutar toda la honeynet. Cada sistema operativo contenido dentro de ella actúa independientemente. Su mayor ventaja es el ahorro de costes al minimizar la inversión en recursos físicos. La Fig. 1 describe una honeynet auto contenida.

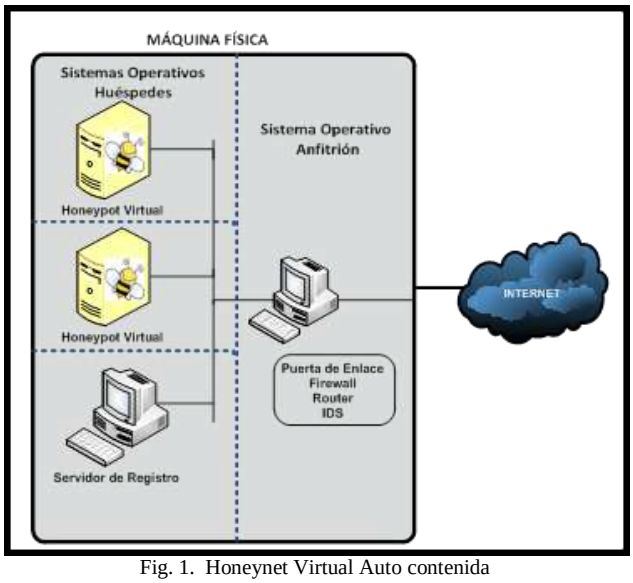

Fig. 1. Honeynet Virtual Auto contenida

- **Honeynet Híbrida.-** Incorpora sistemas reales y virtuales. El Honeywall efectúa el control, captura y el análisis de datos en un sistema aislado, mientras que la virtualización de los Honeypots se realiza en un solo equipo. Este tipo de solución aporta seguridad y flexibilidad. Se presenta en la Fig. 2.

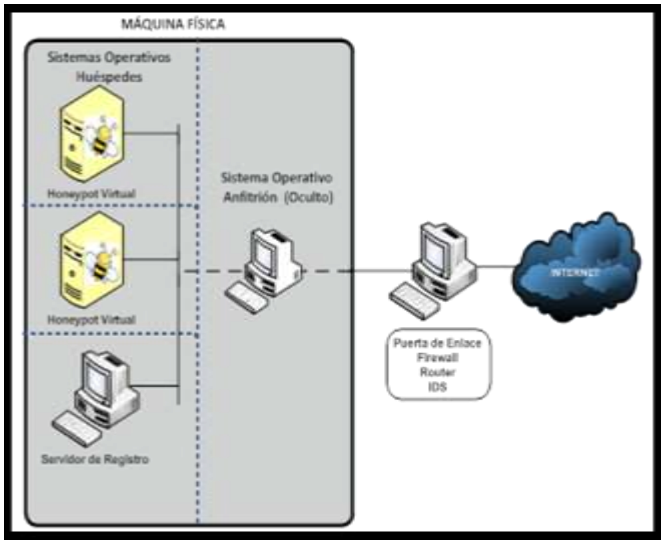

Fig. 2. Honeynet Virtual Híbrida

C. *Sistema de detección de intrusos*

Un sistema de detección de intrusos (IDS, Intrusion Detection System) es uno de los componentes fundamentales de la seguridad actual de los sistemas. Actúa monitoreando el tráfico de la red para alertar al administrador de la presencia de actividades sospechosas. Existen IDS que basan su sistema de detección de alertas en torno a la búsqueda de coincidencias con firmas específicas de amenazas conocidas, de manera similar al comportamiento de un software antivirus; mientras que otros, trabajan a partir de la detección de anomalías en el comportamiento de la red. [4]

Sistema de Detección de Intrusos Basado en Host

Un sistema de detección de intrusiones basado en host (HIDS, Host-Based Intrusion Detection System) tiene como objetivo el monitorear y detectar los ataques lanzados en contra de un equipo determinado. Generalmente, se emplean para proteger la información sensible y significativa almacenada en un host específico.

Sistema de Detección de Intrusos Basado en Red

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

Sistema de Prevención de Intrusos Basado en Red

Un sistema de prevención de intrusos basado en red (NIPS, Network Intrusión Prevention System) es un tipo de mecanismo de seguridad que combina eficientemente las funciones de monitoreo y análisis de los IDS con la respuesta automática activa que proveen los cortafuegos, de manera que no solo detectan la presencia de intrusos, sino que bloquean y mitigan ataques informáticos. La configuración eficaz de un IPS suele convertirse en una tarea bastante complicada, por lo que se recomienda evaluar previamente las necesidades específicas de la red antes de decidirse por esta solución de seguridad. Si la velocidad es un requisito indispensable en la red, esta alternativa puede resultar no conveniente, dado que la respuesta de un IPS no es tan rápida como la de los convencionales cortafuegos e IDS.

En la Fig. 3 se visualiza un esquema de red en el cual se complementa el sistema de seguridad proporcionado por el firewall principal, con la disposición estratégica de varios sistemas de detección de intrusos basados en red y en host, para proteger a la red de posibles ataques, tanto externos como internos.

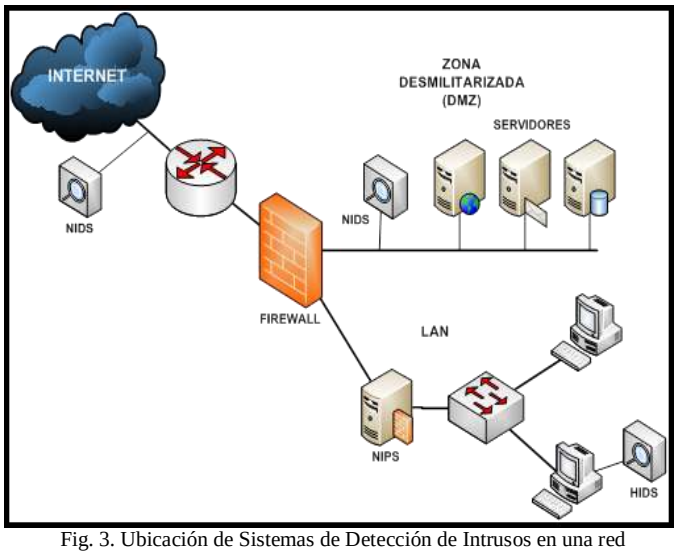

Fig. 3. Ubicación de Sistemas de Detección de Intrusos en una red

III. Diseño e Implementación de la Honeynet

A. *Arquitectura*

La tecnología de las honeynets ha ido evolucionando continuamente desde su aparición hace algunos años. Según el tipo de recursos empleados para proporcionar el modo de captura, control y análisis de datos, se distinguen tres clases de arquitecturas. [2]

La primera generación fue desarrollada por The Honeynet Project en el año 1999. Las actividades de control y captura de datos en esta arquitectura, las realiza un Firewall de capa tres, que actúa a su vez como una puerta de enlace en modo de Traductor de Direcciones de Red (NAT, Network Address Translation). Como desventaja, está el hecho de que puede ser detectada por intrusos con conocimientos avanzados.

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

La tercera generación posee la misma arquitectura que la Gen II, pero experimenta ciertas mejoras en cuanto a la capacidad de gestión y el análisis avanzado de datos. Introduce el concepto de Honeywall Roo, una herramienta open source de fácil implantación que proporciona todos los requerimientos de una honeynet.

Con el propósito de brindar eficientemente estas funciones, se implementa una Honeynet de Producción de Tercera Generación (GEN III). Para minimizar la inversión de recursos económicos y físicos, ofrecer seguridad, flexibilidad y una gestión sencilla de la red, dicha arquitectura se efectúa por medio de una Honeynet Virtual Híbrida, conformada por dos ordenadores; uno que cumple las funciones de Honeywall y el otro que contiene dos máquinas virtuales que constituyen los Honeypots, brindando ventajas semejantes a las proporcionadas por una red completa de dispositivos físicos reales.

Dado que el objetivo del proyecto es el de prevenir y detectar posibles ataques informáticos, además de descubrir las falencias y vulnerabilidades existentes en la seguridad de la red, se opta por localizar a los honeypots en la red de producción. Al situarla después del firewall, se evita el registro de una gran cantidad de ataques y conexiones innecesarias, mostrando únicamente aquellas que comprometan la seguridad de la información.

B. *Modo de Operación*

Como se señaló previamente, la Honeynet Virtual Híbrida de Tercera Generación se ubica en la red Interna de la UTN y emplea únicamente dos máquinas físicas que contienen el honeywall y los honeypots de alta interacción configurados en máquinas virtuales, por medio del software gratuito de virtualización VMware Server 2.0.2. La Fig. 4 expone la topología lógica de red empleada en el diseño de la Honeynet Virtual Híbrida.

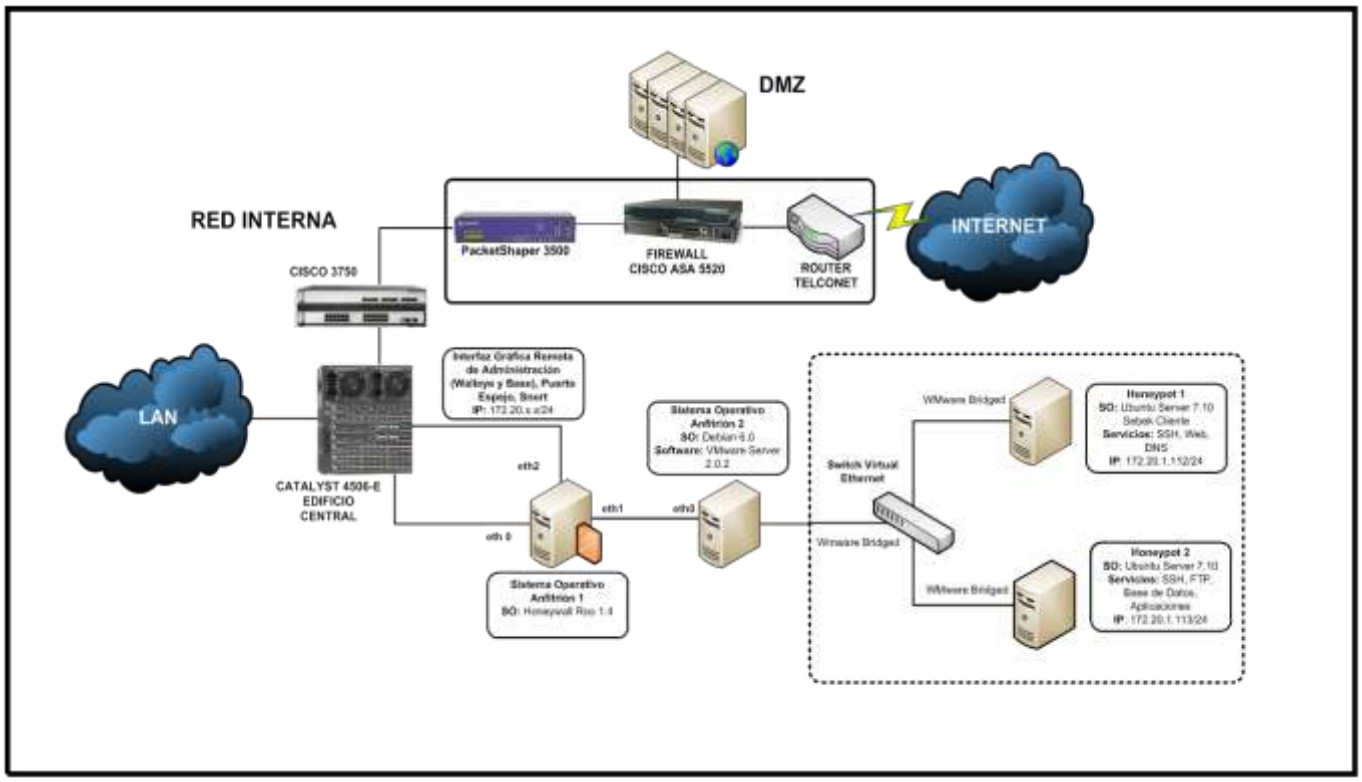

Fig. 4. Topología Lógica de red de la Honeynet Híbrida Virtual de la Universidad Técnica del Norte

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

La captura de datos consiste en el seguimiento y el registro de todas las actividades que amenacen a la honeynet para su posterior análisis. Se requiere recolectar tanta información como sea posible sin que el intruso lo detecte. Contribuye a esta tarea Sebek, una herramienta que opera a nivel del kernel del sistema operativo, capaz de trabajar en canales encriptados, características que la hacen imperceptible para los intrusos. Básicamente, se constituye de dos componentes: el servidor y los clientes. El servidor se configura en el honeywall y tiene como finalidad recolectar las actividades producidas en uno de los honeypots, el cual posee la versión cliente, que envía los datos de las intrusiones hacia el servidor.

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

El control de datos supone la contención controlada de la información y las conexiones. Para evitar que un atacante utilice a una honeynet para lanzar ataques contra la red o comprometa otros sistemas, es necesario asegurar el control de flujo de datos, es decir permitirle cierto grado de libertad para actuar, aunque conlleve un nivel de riesgo mayor. En este proyecto, se realiza mediante la configuración de un cortafuegos basado en iptables que acepta las conexiones entrantes dirigidas hacia los honeypots y limita las salientes.

El análisis de los datos es la capacidad de convertir los datos recogidos en información útil para la detección de tipos y patrones de ataques. Esta actividad se facilita con el uso de las interfaces GUI Web Walleye para examinar las actividades registradas en los honeypots, y BASE con el fin de monitorear las alertas provenientes de la red interna.

Se disponen dos Honeypots virtuales de alta interacción, en los que se configuran los servicios: SSH, FTP, Web, DNS, Base de Datos y Aplicaciones. El sistema operativo para alojarlos es la distribución de Linux Ubuntu Server 7.10, lanzada el 18 de octubre del 2007. Esta versión carece de soporte técnico y actualizaciones de seguridad, incrementando la vulnerabilidad de los Honeypots y convirtiéndolos en un blanco de ataque más atractivo. Como sistema operativo anfitrión de las máquinas virtuales se establece, Debian 6.0, elegido por incorporar el navegador web de código libre Iceweasel, que se deriva de Mozilla Firefox y ofrece total compatibilidad con VMware.

C. Principales Herramientas instaladas

- **Sebek.-** Este software es un fragmento de código alojado en el espacio del Kernel, que registra todas las llamadas de lectura y escritura que se efectúen al sistema. Cuenta con capacidades para detectar pulsaciones de teclado, registro de sesiones encriptadas, captura de contraseñas; entre otras tareas relacionadas con el campo del análisis forense de datos. Se basa en la arquitectura Cliente-Servidor. La versión correspondiente al servidor se instala, generalmente en el gateway y es el encargado de procesar los datos recolectados por el cliente (honeypot 1), permitiendo recrear con precisión las actividades que ocurren en él. [2]

- **Snort.-** es un popular Sistema de Detección de Intrusos basado en Red de código abierto capaz de notificar al administrador de la red acerca de potenciales intentos de intrusiones. Para su funcionamiento emplea detección de firmas y posee un motor pre-procesador que le permite la activación de reglas dinámicas. El proceso de configuración de Snort se lleva a cabo editando el fichero principal "snort.conf". Previamente, se definen los rangos de direccionamiento IP correspondientes a la red y los servidores que serán monitoreados para evitar el disparo de falsos positivos. También se establecen, configuran los módulos preprocesadores y se activan las firmas de seguridad. Posteriormente, se habilita el plugin de salida de datos en formato binario unified que contiene información acerca de las alarmas disparadas por el IDS. Para mejorar el rendimiento de snort, dichos ficheros se procesan por medio de la herramienta barnyard, que a su vez los almacena en una base de datos creada mediante mysql server. [5]

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

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

- **Interfaz Web BASE.-** Para facilitar el monitoreo de las alertas de seguridad en la red interna de la universidad, se implementa la herramienta basada en PHP, BASE (Basic Analysis and Security Engine) versión 1.4.5, que administra los datos de las alarmas almacenadas en la base de datos del IDS y adiciona varias tablas al esquema inicial para que soporte funcionalidades complementarias, entre las que se mencionan: la búsqueda de eventos de acuerdo a la dirección IP de origen, destino, tipo de alerta, tráfico por protocolo, fecha u hora de ocurrencia, la clasificación de las alertas en grupos específicos creados de acuerdo al criterio del administrador y generación de gráficas de tiempo en función de las alertas.

D. Dimensionamiento de Hardware

El dimensionamiento de los recursos de hardware garantiza el correcto funcionamiento y adaptación de los componentes de la Honeynet Virtual Híbrida al entorno de red principal de la UTN.

El análisis de requerimientos se realiza en función de las exigencias técnicas dispuestas por los desarrolladores del software a ejecutarse y a varios factores que afectan el rendimiento de los mismos. Es así, que el equipo fijado para albergar al Honeywall debe poseer suficiente capacidad de memoria, procesamiento y espacio de almacenamiento en la unidad de disco duro para satisfacer la demanda de las herramientas de captura, control y análisis de datos tomando en cuenta dichos aspectos.

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

TABLA I
REQUERIMIENTOS DE HARDWARE PARA LOS EQUIPOS

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

IV. Descripción de Resultados

Se describen las actividades recolectadas por la Honeynet Virtual Híbrida tras un período de implementación de dos meses. La información se organiza en dos secciones principales: la primera detalla el tráfico capturado hacia los honeypots y la segunda se enfoca en las alertas generadas por Snort durante el monitoreo de la red interna.

A. Actividades Recolectadas en los Honeypots

Se han detectado un número significativo de conexiones e intentos de ataques hacia los honeypots desde que éstos se integraron a la red de la UTN. Es importante destacar que todo tráfico dirigido a los señuelos se considera de carácter sospechoso, ya que al no contener información de utilidad para los usuarios de la red, no debería existir ningún tipo de interacción en ellos. De esta manera, se registran un total de 1513 conexiones, de las cuales 823 corresponden al protocolo TCP (54%), 628 pertenecen al protocolo UDP (45%) y únicamente 12 (1%) a ICMP. Se esquematiza en la Fig. 5.

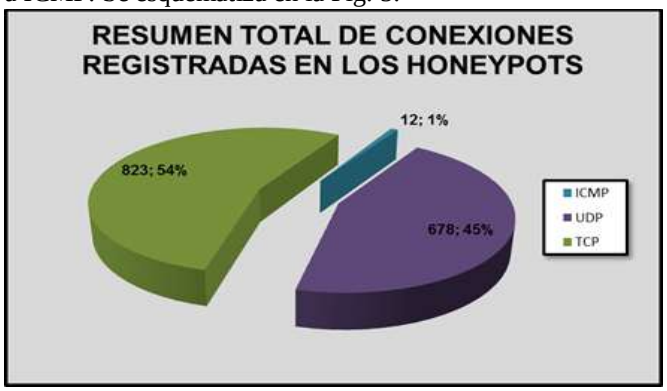

Fig. 5. Resumen total de conexiones registradas en los Honeypots de acuerdo al tipo de protocolo

Según lo obtenido, el puerto de destino más frecuente corresponde al TCP/445 (39%) que hace referencia a Microsoft-DS, un servicio que posibilita el intercambio de archivos y el manejo de recursos compartidos en entornos Windows haciendo uso del protocolo SMB (acrónimo de Server Message Block), en lugar de emplear el sistema básico de entrada y salida (NetBIOS, Network Basic Input/Output System).

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

El tercer puerto destino de mayor ocurrencia en los honeypots (14%) es el TCP/135 conocido como EPMAP (End Point Mapper) que ayuda a determinar el listado de servicios disponibles en equipos remotos. También se asocia con la prestación de servicios de mensajería e intercambio de datos y comunicación entre procesos mediante el procedimiento de llamada remota (RCP, Remote Procedure Call).

El 11% hace mención al puerto UDP/137 perteneciente a NETBIOS que se ocupa de la compartición de recursos y archivos en ambientes Windows. Tanto hackers como malware utilizan este puerto para cometer intrusiones malintencionadas. La vulnerabilidad de este puerto habilitado por defecto se incrementa con la funcionalidad que admite el logueo de usuarios anónimos (null sessions) para mejorar el nivel de compatibilidad y conectividad, razón por la cual es imprescindible mantener activado el firewall de Windows para proteger a los equipos.

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

En la Fig. 6. se observan los puertos destino de las alertas más frecuentes y sus porcentajes.

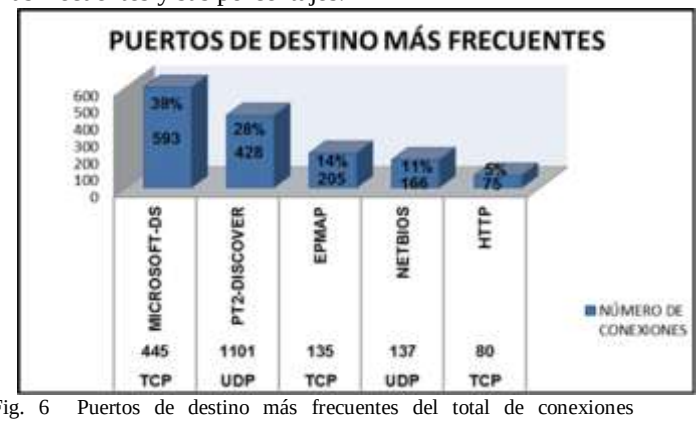

Fig. 6 Puertos de destino más frecuentes del total de conexiones registradas en los honeypots.

B. Actividades recolectadas en la red interna de la universidad

Se sintetizan los resultados obtenidos tras el monitoreo ejecutado por el sistema de detección de intrusos basado en red Snort encargado de sensar permanentemente la red interna de la universidad. Durante este proceso, la interfaz Web BASE ha confirmado ser un instrumento dinámico y confiable, simplificando el tratamiento de los resultados, una tarea que habría resultado bastante tediosa, especialmente por el alto número de alertas detectadas en el tiempo de evaluación de la Honeynet.

Se han registrado un total de 108.744 alertas, distribuidas en 14 categorías principales y correspondientes a 284 alertas únicas, iniciadas desde 12.367 puertos lógicos distintos dirigidos hacia 9014 puertos de destino.

Se aprecia una diferencia importante entre la cantidad de alertas generadas de acuerdo al tipo de protocolo, situándose en primer lugar el protocolo UDP con 82179

equivalente al 75.6% del total, seguido por el protocolo TCP con el 24.3% (26477) y finalmente con el mínimo porcentaje de 0.1% referente al protocolo ICMP. Se ilustran claramente en el gráfico estadístico de la Fig. 7.

Fig. 7. Resumen total de alertas registradas en BASE de acuerdo al tipo de protocolo.

Las alertas disparadas por Snort se han clasificado en 14 grupos diferentes, mismos que se observan en la Fig. 8.

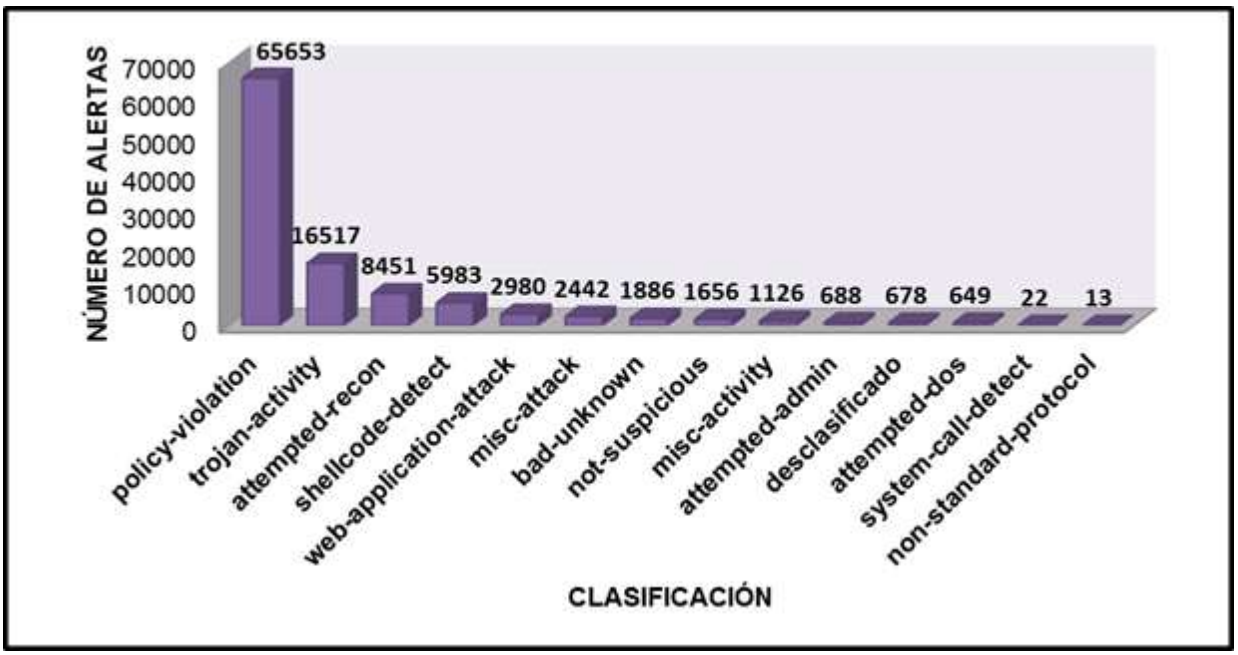

Fig. 8. Gráfico estadístico de la clasificación de alertas registradas en BASE.

V. Conclusiones

Es importante monitorear y medir el tráfico de red para determinar el patrón característico del uso de los recursos y proporcionar información fundamental para efectuar el diseño de la Honeynet Virtual Híbrida y entonces, garantizar su adaptación y correcta funcionalidad.

Durante el diseño de un Sistema de Detección de Intrusos y soluciones de seguridad basadas en la tecnología Honeynet, es primordial establecer estratégicamente la ubicación del sensor en el entorno de la red y planificar la capacidad de hardware de los equipos. De una buena elección dependerá la eficiencia del proyecto para detectar vulnerabilidades y ataques informáticos de acuerdo a su propósito de implementación.

La implementación del Honeywall y Honeypots, utilizando enteramente software de tipo libre y freeware, le proporcionó al proyecto numerosas ventajas, entre las que sobresalen la libertad en la modificación del código fuente de las aplicaciones para adaptarlas a las necesidades específicas de administración, rápida recuperación ante fallos y la eliminación de costos de adquisición y mantenimiento, considerando que se requiere la actualización constante de firmas de seguridad empleadas por el IDS.

La Honeynet comprobó ser efectiva para detectar todos los ataques de seguridad simulados. En este proceso, se demostró que para tomar control total de un sistema objetivo es necesario la ejecución de una serie lógica de intrusiones menores.

Se experimentó dificultad para identificar falsos positivos, debido a la falta de acceso para evaluar las estaciones de trabajo de la red que generan las alertas.

La implementación de la Honeynet Virtual Híbrida permitió determinar una gran cantidad de posibles ataques y vulnerabilidades en la red de la Universidad Técnica del Norte. De su análisis se concluye que, en su mayoría, se originan debido al uso inapropiado de los recursos de red por parte de los usuarios dando lugar a la propagación de diversos tipos de malware y otros tipos de intrusiones.

RECONOCIMIENTOS

Se expresa un especial reconocimiento al Departamento de Informática de la Universidad Técnica del Norte, en especial al Ing. Msc. Fernando Garrido, director del mismo e Ing. Cosme Ortega, por el apoyo y colaboración brindada para desarrollar este trabajo.

REFERENCIAS

[1] Honeynet UTPL (2008). Tecnología honeypot. Recuperado de: http://www.utpl.edu.ec/honeynet/?p=159.

[2] Provos, N., & Holz, T. (2008). Virtual honeypots: From botnet tracking to Intrusion detection. Boston: Pearson Education, Inc.

[3] Inteco. (2010). Honeypots, monitorizando a los atacantes. Recuperado de: http://es.scribd.com/doc/47017021/Honeypots-Monitorizando-a-Los-Atacantes.

[4] Akindeinde, O. (2009). Attack simulation and threat modeling. Lagos, Nigeria.

[5] Alfon. (2009). Seguridad y redes. Snort preprocesadores (I) parte. Recuperado de: http://seguridadyredes.wordpress.com/2009/03/03/snort-preprocesadores-i-parte/.

Edgar A. Maya A.

Nació en Ibarra provincia de Imbabura el 22 de abril de 1980. Ingeniero en Sistemas Computacionales, Universidad Técnica del Norte-Ecuador en 2006. Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador, y cursa la Maestría en Redes de Comunicación (3do Semestre), Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

Tatiana A. Vinueza J.

Nació en Otavalo-Ecuador el 4 de diciembre de 1987. Hija de Wilson Vinueza y Yolanda Jaramillo. Realizó sus estudios primarios en la Escuela Fiscal de Niñas "Gabriela Mistral". En el año 2005 obtuvo su título de Bachiller en Ciencias con especialización Físico Matemático en el I.S.T "República del Ecuador". Actualmente, es egresada de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.