Captura y análisis de los ataques informáticos que sufren las redes de datos de la ESPOL, implantando una honeynet con miras a mejorar la seguridad informática en redes de datos del Ecuador

Pazmiño, Mayra; Avilés, Jorge; Abad, Cristina Ms.Sc.
Grupo de Visualización Científica y Sistemas Distribuidos
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
{mpazmino,iaviles,cabad}@fiec.espol.edu.ec

Resumen

Es un hecho que en la actualidad las redes de computadoras son atacadas y vulneradas, cada año se incrementa la velocidad de propagación, la facilidad de ejecución y el daño que producen estos ataques, por lo tanto, es muy importante el estudio y la elaboración de estrategias que permitan tener un grado adecuado para protegerse. Para poder tener una red segura se debe considerar lo que se debe proteger y de quién, luego definir las políticas de seguridad adecuada e implementarlas, pero para poder realizar esta tarea es necesario conocer cuáles son los patrones de ataques sufridos. Los sistemas de alertas de intruso utilizados generalmente una gran cantidad de datos lo que hace casi imposible un análisis efectivo, las honeynets proveen el mecanismo de registro y alerta sin la necesidad de manejar todo el trafico real y sin comprometer la integridad de sus sistemas y servicios. En este documento se plantea la solución de implementar una honeynet en las redes de datos de la ESPOL para estudiar determinar los patrones de ataques.

Palabras claves: *ataques, honeypots, honeynets, dirección IP, MAC, arquitecturas, redes de datos*

Abstract

It is a fact that computers[s networks are attacked and wounded currently, each year increase the velocity of propagation, the facility of execution and the damage that produce these attacks, therefore, is very important the study the elaboration of strategies that permit to have an adequate degree to be protected. To be able to have a sure network should be considered what should be protected and whose, then to define the politics of adequate security and to implement them, but for be able to carry out this task is necessary to know which are the bosses of attacks suffered. In this document the solution to implement be planted a honeynet in the ESPOL networks to study, to determine the bosses of attacks.

1. Introducción

La seguridad en una red de computadores depende de las vulnerabilidades en el software y hardware en los equipos que la conforman y de los tipos de ataques internos o externos que sufren.

Se debe conocer las vulnerabilidades del software para poder aplicar medidas que eviten la explotación de las mismas, así mismo saber los posibles ataques en los servicios de red para implementar medidas para bloquearlos usando dispositivos de detección y bloqueos de ataques en la red.

Existen mecanismos que sirven de defensa para las redes de computadoras como firewalls, sistemas de detección de intrusos (IDS), redes privadas virtuales (VPNs), listas de control de acceso, etc. Los problemas de estos mecanismos de seguridades se producen cuando no están correctamente configurados, y pueden dar una falsa sensación de seguridad. Para plantear las reglas correctas en firewalls, IDSs y ACLs, es imprescindible que el administrador de la red tenga una visión detallada y realista de los tipos de ataques a los que su red es susceptible. El uso de una tecnología llamada Honeypots permite conocer en mejor detalle los ataques y vulnerabilidades de las redes.

Un Honeypots o "tarro de miel" en el campo de la seguridad en redes de información se define como un recurso de la red que se encuentra voluntariamente vulnerable para que el atacante pueda examinarla, atacarla. [1] Directamente no es solución a ningún problema; su función principal es recoger información importante sobre el atacante que permita prevenir estas incursiones dentro del ámbito de la red real en casos futuros.

El presente trabajo consiste en implementar un tipo especial de Honeypot "Honeynet", en las redes de datos en la ESPOL, que nos permitirá capturar y analizar los patrones de ataques a dichas redes.

2. Motivación

Las redes de comunicación dentro del Campus universitario Gustavo Galindo de Guayaquil cuentan con enlaces a la red Internet, y son parte de diversos ambientes que brindan servicios a estudiantes, académicos, personal administrativo, investigadores e incluso la sociedad en general. Además algunas instalaciones cuentan con infraestructuras inalámbricas, por lo cual debemos tener en consideración que dispositivos como portátiles, teléfonos celulares, entre otros usan el servicio de conectividad, y en muchas ocasiones aplicar una política restrictiva en el uso de la red puede representar un problema.

Dentro del arsenal de defensa de las redes de Campus, podemos encontrar una gran gama de mecanismos, como firewalls, sistemas de detección de intrusos (IDS), redes privadas virtuales (VPNs), listas de control de acceso, etc, los cuales trabajan como parte de un todo que ayuda a incrementar la seguridad de los sistemas. Sin embargo, todas estas medidas son de pura defensa de recursos, dejando a un lado la capacidad pro-activa que puede ayudar en un grado muy considerable.

También tenemos que considerar que en la actualidad el aumento del ancho de banda disponible y el fácil acceso a la red, ha contribuido a una evolución en las técnicas de ataques existentes, teniendo cambios en los escenarios típicos generadores de amenazas para cualquier sistema conectado a Internet.

Tener una información detallada acerca de las actividades de intrusos que entran a nuestras redes es crucial, porque nos ayudará a tomar medidas sobre el ataque sufrido y actualizar las políticas para evitar réplicas o ataques con patrones similares, también nos proporcionará información detallada sobre vulnerabilidades de sistemas que podríamos considerar en otras redes que aún no han sido afectadas.

El enfoque generalmente utilizado para obtener información sobre los rastros de los intrusos en nuestras redes es el uso de las mismas herramientas de seguridad de la red. Lastimosamente, este enfoque tiene dos problemas principales : (1) Si el sistema afectado es un servicio de vital importancia, no puede ser desconectado (por ejemplo, un servidor de correos) por lo cual el análisis de datos deberá ser realizado con el servicio encendido mientras sigue proveyendo sus servicios productivos, limitando la habilidad de obtener suficiente información de lo sucedido, cuánto daño ocasionó e incluso si el atacante accedió a otros sistemas de la red; y, (2) en el caso hipotético de que sea factible apagar el servicio afectado (servidor de correos), se obtendría mucha polución de datos, debido a que los datos buscados que corresponden al ataque específico estarán entre todos los registros de transacciones diarias del servidor (logging de usuarios, lecturas de cuentas de mail, archivos escritos a bases de datos, etc.), y será difícil determinar cuál es la actividad normal del día a día y que es lo que hizo el atacante.

La siguiente lista es una muestra de los ataques (o intentos de) informáticos que ha sufrido las redes de datos de la ESPOL:

- Un hacker infectó un servidor del CVR y lo estaba usando para montar ataques de negación del servicio (DoS).

- Un hacker corrompió (varias veces) el sitio Web de las Jornadas de Ingeniería de Software (2007).

- Durante el 2007, el servidor SSH del Laboratorio de Sistemas Distribuidos y Tecnologías de Internet Aplicadas recibió todos los días intentos de quebrar un usuario y contraseña, y además, barridos (escaneos) tipo toma de huellas (fingerprinting), usados por los atacantes para identificar la plataforma utilizada por el equipo a ser atacado.

- Las computadoras de los laboratorios del CIB y de los departamentos administrativos son usadas como zombies para montar ataques a otras instituciones.

- Un hacker ingreso al servidor Web del CIB para descargar las tesis que ahí están almacenadas.

Cabe recalcar que las redes de datos de instituciones de la ESPOL pueden ser atacadas con los siguientes fines:

- Falsificación de información. Por ejemplo, un estudiante puede vulnerar un sistema y lograr ingresar al académico, aumentarse un par de puntos, y conseguir aprobar una materia. O un empleado puede aumentar presupuestos asignados, etc. (sin que quede registro de quien realizó el ataque o de tal manera que parezca que el cambio fue hecho por otra persona y no por el atacante real).

- Ataques de negación del servicio (DoS).

- Para instalar una botnet (red de zombies o computadores infectados) los cuales luego son utilizados para montar ataques de negación del servicio a otras instituciones.

- Propagación de virus informáticos.

- Como punto intermedio para ataques a otros servidores (en otras instituciones o países), de tal manera que luego no se pueda rastrear el origen de los ataques.

3. Justificación

Los Honeypots y Honeynets presentan una mejor alternativa a este problema. Definiremos Honeypot como un recurso de red destinado a ser atacado o comprometido. [1] Un Honeynet es un tipo de Honeypot de alta interacción, destinado a capturar información extensa sobre ataques, con sistemas, aplicaciones y servicios reales a ser comprometidos (los cuales no se encuentran en producción). [2]

La implantación de los Honeypots y Honeynets es la solución para la detección y especialmente el análisis de patrones de ataques, debido a que no son sistemas en producción y toda actividad dirigida hacia ellos es sospechosa por naturaleza.

[2] De esta manera, las cantidades de datos que se recolectan diariamente de la actividad hacia los Honeypots y Honeynets son en comparación con otros sistemas de monitoreo, en menor cantidad.

Sin embargo esta pequeña cantidad de datos es de gran valor, debido a que toda la actividad capturada puede ser un escaneo, una prueba o un ataque, reduciendo así los tiempos de detección y de análisis de la actividad maliciosa en la red.

4. Diseño

Para realizar el análisis de patrones de ataques en las dos redes seleccionadas dentro de la ESPOL, que corresponde a la FIEC y el CIB es necesario implantar dentro de cada red de computadoras una Honeynet. Como diseño preliminar la Figura 7-1, muestra que la Honeynet estará conectada y funcionará en conjunto dentro de la misma red de producción, perteneciendo al mismo rango de IP.

Este mismo esquema servirá para ambas implementaciones (FIEC y CIB) con la variante del tipo de arquitectura de Honeynet virtual.

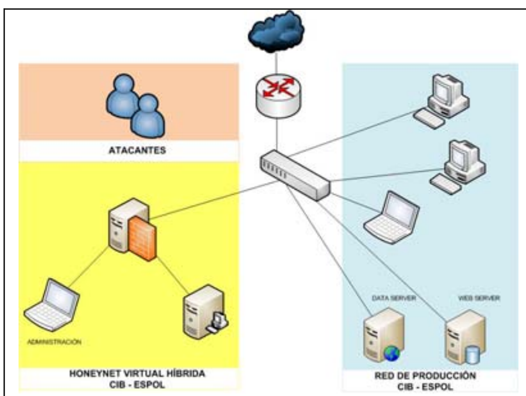

Figura 4-1 Arquitectura general del la Honeynet CIB

a. Arquitectura de la Honeynet – FIEC

Para la Honeynet implantada en la red de la FIEC se ha seleccionado la arquitectura de Honeynet Virtual que definidos como Honeynet A en el Capítulo 3, la cual corresponde a una Honeynet virtual auto-contenida, que por definición para desarrollarla solamente es necesario una máquina física que levantará como máquinas virtuales a todos los elementos que conformen la Honeynet

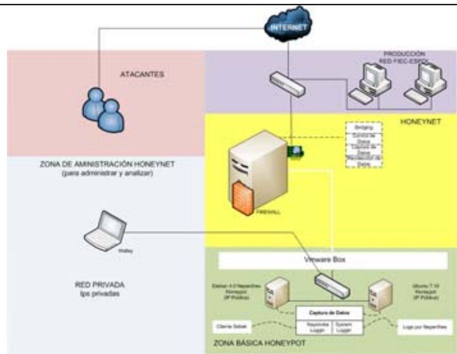

Figura 4-2 Arquitectura de la Honeynet en la FIEC

La Figura 4.1-1, muestra la máquina física que usa una aplicación de virtualización para levantar 3 máquinas virtuales, una corresponde al Honeywall, las dos siguientes son Honeypots usando Debian 4.0 y Ubuntu Server 6.10 como sistemas operativos bases.

b. Arquitectura de la Honeynet – CIB

Para la Honeynet implantada en la red de la CIB se ha seleccionado la arquitectura de Honeynet virtual que definidos como Honeynet B en el Capítulo 3, la cual corresponde a una Honeynet Virtual híbrida, como se muestra en la Figura 4.1-1. Para su desarrollo usaremos dos máquinas físicas las cuales una servirá solamente como Honeywall y la segunda mediante un software de virtualización levantará a dos máquinas virtuales que corresponden a los Honeypots, en el caso de esta red usarán los sistemas operativos: Windows XP y Debian 4.0.

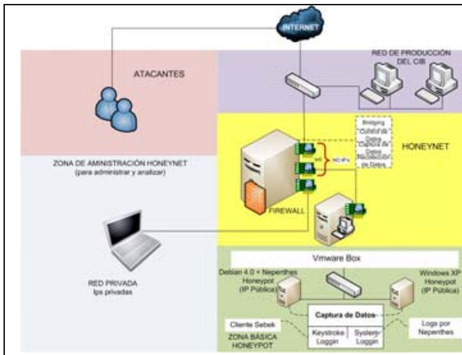

Figura 4-2 Arquitectura de la Honeynet en el CIB

5. Implementación

a. Honeynet - FIEC

i. Hardware

Para construir la Honeynet virtual auto-contenida dentro de la red de la FIEC se dispone de un computador con las siguientes características, cumpliendo así los requerimientos necesarios para levantar las tres máquinas virtuales y estos son:

- Procesador Pentium Dual Core 1.7 GHz
- Memoria RAM de 1 GB
- Disco duro de 300 GB
- Tarjeta de Red de 10/100/1000 Mbps

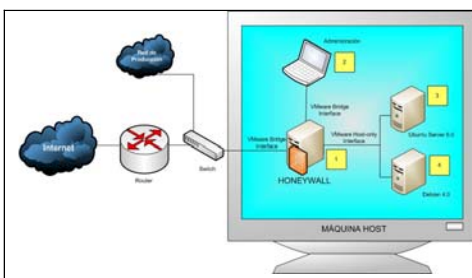

Figura 5-3 Honeynet Virtual Auto-contenida en la red FIEC

Los dispositivos virtuales que serán levantados formaran una red virtual dentro de la máquina host, tal como lo muestra la Figura 7-1 y serán configurados con los requerimientos de hardware que se detallan en la Tabla 7-1

S. O.(s)	Disco Duro (s)	Memoria
Debian 4.0	30 GB	512 MB
Ubuntu Server 7.10	30 GB	512 MB
Honeywall(Roo 1.4)	100 GB	256 MB

Tabla 7-1 Sistemas operativos

ii. Configuración de red

El diagrama de red de la Figura 7-1, muestra la Honeynet de la FIEC con sus componentes físicos y virtuales necesarios.

Una sola máquina física se encuentra conectada directamente al switch junto a la red de producción, este computador con una distribución de Linux Fedora 8 y un software virtualización VMware 6 utilizado para levantar 3 máquinas virtuales usadas dentro de esta Honeywall.

La máquina virtual Honeywall [1] utiliza tres interfaces virtuales de red: (una en modo bridge y dos en modo host-only), los Honeypots [3 y 4] utilizan cada uno una interfaz de red en modo host-only.

El modo host-only permite interconectar máquinas virtuales entre sí, así como también el sistema que las contiene, creando una red privada interna aislada del resto de la red externa.

En modo bridge se asocia una interfaz física de red del sistema host por la cual las máquinas virtuales utilizan su propia IP y les permite acceder y pertenecer al mismo segmento de red a la cual está conectada la máquina que la contiene.

b. Honeynet - CIB

i. Hardware

Para construir la Honeynet Virtual híbrida dentro de la red del CIB se dispone de dos computadoras con las siguientes características:

Computadora 1

- Procesador Pentium 4 de 1.6 GHz
- Memoria RAM 512 MB
- Disco duro de 200 GB
- 1 tarjeta de red 10/100

Computadora 2

- Procesador Pentium 4 de 1.6 GHz
- Memoria RAM 256 MB
- Disco duro de 100 GB
- 3 tarjetas de red 10/100

Por sus características la Computadora 1 será usada para levantar dos máquinas virtuales que corresponde a la red virtual de Honeypots.

La Computadora 2 será usada como Honeywall ya que no es necesario tener una máquina muy potente para esta tarea.

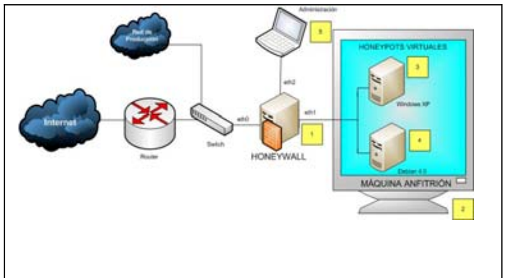

Figura 5-2 Honeynet Virtual Auto-contenida en la red FIEC

La Figura 5-2 muestra a las dos máquinas físicas Honeywall [1] y máquina anfitrión [2]. La máquina anfitrión es la encargada de levantar las dos Honeynets virtuales y serán configurados con los requerimientos de hardware que se detallan en la Tabla 5-2

S. O.(s)	Disco Duro (s)	Memoria (s)
Debian 4.0	25 GB	256 MB
Windows XP	25 GB	256 MB

Tabla 5-2 Sistemas operativos

c. Configuración de red

El diagrama de red de la Figura 7-2, muestra la Honeynet del CIB con sus componentes físicos y virtuales necesarios.

El Honeywall [1] posee tres interfaces de red: eth0, eth1 y eth2, eth0 le permite conectarse directamente con el switch, el eth2 es para uso de administración y el eth1 se conecta con la segunda máquina física de nuestra red que internamente levanta una red virtual de dos máquinas gracias a la configuración de sus tarjetas en modo host-bridge, que les proporciona la salida directa a través de la interfaz de red física de la máquina anfitrión para las Honeypots virtuales se comporten como nodos directamente conectados a la red externa.

6. Pruebas

Cada vez que una Honeynet se activaba fue imprescindible hacer que pase por una serie de pruebas, las cuales garantizaban el correcto funcionamiento de su hardware como de software, fue muy útil elaborar una lista de pasos o pruebas necesarias con las cuales podíamos determinar su una Honeynet y cada uno de sus elementos funcionaba correctamente. Con estas pruebas no solo garantizábamos la correcta recolección de datos, también garantizábamos la integridad del proyecto como tal, si dejábamos un solo indicio a los atacantes de que se trataba de un Honeypot podría introducirse ruido en las muestras recogidas, o en el peor de los casos, se intentaría usar la Honeynet como una arma contra nosotros.

Las pruebas iniciaban con un chequeo del cableado, continuando con la revisión de cada elemento de recolección en la Honeynet, finalmente se revisaba si la Honeynet no podría ser usada como una herramienta contra la red interna o alguna maquina en internet, para lograrlo se bloquearon rangos de red completos y se limitaron paquetes salientes.

7. Conclusión

Al finalizar la etapa de recolección la cantidad de paquetes recogidos subió a 4Gb, también una cantidad considerable de alertas del IDS y un registro largo de IPs alrededor del mundo que se conectaron con los Honeypots, estos eventos nos indican que ambas redes estuvieron visibles y fueron consideradas como sistemas en producción y no como un sistema de defensa.

En la Figura 7-1, tenemos como ejemplo usando los paquetes recogidos determinamos que protocolo tuvo mayor interacción con respecto a los demás, durante los cuatros meses que se implemento las Honeynets, el protocolo SSH tuvo mayor actividad en la FIEC con un 63%.

Con respecto a las arquitecturas nos sorprendió lo efectivo que fue la implementación de una Honeynet hibrida, su portabilidad y su requerimientos económicos la convierten en una herramienta que puede ser usada en un ambiente didáctico.

Figura 7-1 Paquetes FIEC

8. Agradecimientos

Este trabajo ha sido posible gracias al financiamiento del CICYT-ESPOL, el apoyo y la confianza que nos brindaron el CSI-ESPOL al permitirnos implantar nuestras Honeynets como parte de las redes de datos en la ESPOL, también queremos considerar el apoyo brindado por los administradores de red del CIB y de la FIEC, finalmente un agradecimiento especial por todo el apoyo y orientación de la Ing. Cristina Abad.

9. Referencias

[1] Lance Spitzner, “Honeypots: tracking Hackers”, Addison Wesley professional, 2002.

[2] “Honeynet Project”, Know Your Enemy: Learning about Security Threats (2nd Edition), 2004