Diseño Preliminar de una Honeynet para Estudiar Patrones de Ataques en las Redes de Datos de la ESPOL

Pazmiño, Mayra [1]; Avilés, Jorge[2]; Abad, Cristina Ms.Sc.[3]
[1 2 3] Grupo de Visualización Científica y Sistemas Distribuidos
[1 2 3] 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

1. Introducción

En la actualidad las redes de datos se ven frecuentemente atacadas y vulneradas. Por lo tanto, es muy importante la elaboración de una estrategia correcta que nos permita tener un grado adecuado de protección hacia las mismas. Formando parte de dicha estrategia encontramos dispositivos de detección y bloqueos de ataques.

Dentro del "arsenal de defensa" de las redes en el Campus Politécnico, podemos encontrar una gran gama de mecanismos como firewalls, sistemas de detección de intrusos (IDS), redes privadas virtuales (VPNs), listas de control de acceso, entre otras, las 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.

Un problema de los mecanismos de seguridad mencionados anteriormente, es que muchas veces no están correctamente configurados, y pueden dar una falsa sensación de seguridad. Para plantear las reglas correctas en firewalls, IDSs y ACLs, es imprescindible que el administrador de la red tenga una visión detallada y realista de los tipos de ataques a los que su red es susceptible. Con esta finalidad, los expertos en seguridades recomiendan un monitoreo constante de la red y la instalación de equipos configurados.

Según su concepto, las Honeynets son mecanismos relativamente simples, donde se crea una red muy parecida a una "pecera", en la cual podemos ver todo lo que ocurre en ella, los intrusos o hackers serán los "peces" que nadarán en el entorno virtual pero sin saber que son observados. Además igual que en una "pecera", se puede agregar diferentes cosas las cuales nos ayudarán a monitorear al intruso mientras aprendemos de sus técnicas. Esta red de datos controlada se convierte en nuestra Honeynet. Las actividades capturadas nos enseñan las herramientas, motivos y tácticas usadas por los intrusos.

Una Honeynet es un tipo concreto de Honeypot pero altamente interactivo, diseñado para la investigación y la obtención de información sobre atacantes. Una Honeynet es una arquitectura, no un producto concreto o un software determinado.

Un honeypot 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, etc. 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.

Este trabajo consiste en presentar un diseño preliminar de una Honeynet en redes de la

ESPOL, la cual nos proporcionará una visión más clara sobre los tipos de ataque que sufren nuestras redes de datos.

Con el análisis de la arquitectura en las redes de datos de la ESPOL y considerando las distintas clases de Honeynets hemos elaborado un diseño preliminar que servirá de pauta para la implantación de una Honeynet y de fuente para un futuro análisis forense de los datos obtenidos.

Algunos de nuestros objetivos para este proyecto son:

- Elaboración del diseño preliminar de una Honeynet que será implantando en las redes de la ESPOL.
- Proporcionar una herramienta de aprendizaje e investigación para cualquier curso de seguridad informática o de investigación que se esté realizando dentro de la ESPOL.
- Adquirir experiencias sobre el uso de Honeynets en una ambiente real, recolección y análisis de datos.
- Registrar y documentar las técnicas y herramientas usadas en la implantación de la honeynet así como de los datos obtenidos.

2. Materiales y Métodos

Cualquier recurso digital puede constituir un Honeypot, desde un servidor o cualquier equipo dentro de nuestra red, pero teniendo en claro que ninguno de estos recursos que sea usado debe ser un sistema de producción o formar parte de uno.

Los pasos básicos para implantar una Honeynet en una red son: (1) colocar un recurso que no contenga información de producción, así nada ni nadie en la red pueda interactuar ni saber de él, (2) registrar cualquier transacción que se realice desde o hacia el recurso, ya que significará que es un acceso no autorizado.

Una Honeynet presenta dos requerimientos básicos para ser realmente útil y que nos permita la extracción de información valiosa: (1) control de flujo de datos, y (2) captura de los datos.

El *control del flujo de datos* (data control) consiste en mantener siempre un control del flujo de datos para evitar que el atacante la utilice a la Honeynet contra terceros o contra la propia red de producción.

La *captura de los datos* (data capture) consiste en la captura sigilosa de todos los movimientos y acciones que realice el atacante en nuestra Honeynet, los cuales nos revelarán sus técnicas y motivaciones.

Para la elaboración del diseño preliminar de nuestra Honeynet presentado en este proyecto, se ha escogido a la red del Centro de Información Bibliotecario (CIB) de la ESPOL. La red ha sido analizada en su estructura y servicios. En base al análisis realizado, hemos decidido agregar nuestro Honeynet dentro del espacio de direcciones de producción debido a que contiene servicios sensibles y muy susceptibles a ataques. Entre estos servicios se encuentra un servidor Web, un servidor de base de datos y los diferentes computadores ubicados dentro del área Administrativa, que son la base de los servicios digitales prestados por la Biblioteca de la ESPOL.

Nuestro diseño preliminar, tal como lo muestra la Figura 1, estará constituido por una pasarela de capa 2, que actuará como puente. La interfaz externa de nuestra pasarela gateway (eth0) está conectada a la red de sistemas de producción. El interfaz interno de nuestro gateway (eth1) está conectado a la red de sistemas Honeynet (Honeypots) que levantarán servicios similares a los que están en producción, con el fin de ser usados como señuelos para ser detectados por intrusos. Como puente, tanto el interfaz externo como el interno están en la misma red IP. Esto nos ofrece diversas ventajas. La primera ventaja viene de el hecho de que el dispositivo sea de capa 2, lo que lo hará mucho más difícil de detectar, ya que no hay enrutamiento de tráfico ni decrementos en el tiempo de vida (TTL), además el dispositivo está

más oculto, así que los atacantes no sabrán que su tráfico está siendo analizado y controlado. La segunda ventaja es que, como pasarela, todo tráfico entrante o saliente debe pasar a través del dispositivo, de esta forma podemos capturar y controlar tanto el tráfico entrante como el saliente desde un único dispositivo.

Tanto el control del flujo de datos como la captura de datos, estarán bajo herramientas libres como sniffers, alarmas y scripts para bloqueo y control de ataques. Todo esto estará corriendo sobre una distribución Linux que soporte funciones de puente, lo cual con *ebtables* es muy sencillo y eficiente de implementar.

3. Resultados

En esta investigación e innovación de nuevas técnicas de seguridades de las redes de datos de la ESPOL, encontramos que existe un total apoyo por parte de los administradores, dando como resultado la concientización de los mismos sobre los distintos problemas a los que están expuestos las redes de la ESPOL.

Hasta el momento no se nos ha presentado ningún problema en la captura de datos para nuestro análisis, lo que nos lleva a pensar, que una vez concluido nuestro proyecto de investigación, nuestros resultados serán escuchados por los administradores encargados de las redes y sirvan para incrementar la seguridad de las redes de datos de la ESPOL.

4. Conclusión

Los resultados de nuestro análisis serán de mucha importancia para mejorar la seguridad de las redes de datos de la ESPOL. Es importante también considerar que (hasta donde hemos podido averiguar) en Ecuador no hay documentación de ningún estudio similar, por lo que la documentación de nuestros resultados podrá ser utilizado por cualquier institución ecuatoriana que desee entender mejor el tipo de ataques a los que están expuestas las redes de datos de nuestro país.

Finalmente, la implantación de un Honeynet en una institución educativa abre nuevos campos de investigación en seguridad informática forense, los cuales serán explorados en futuros proyectos del nuestro equipo de investigación.

5. Tablas y Figuras

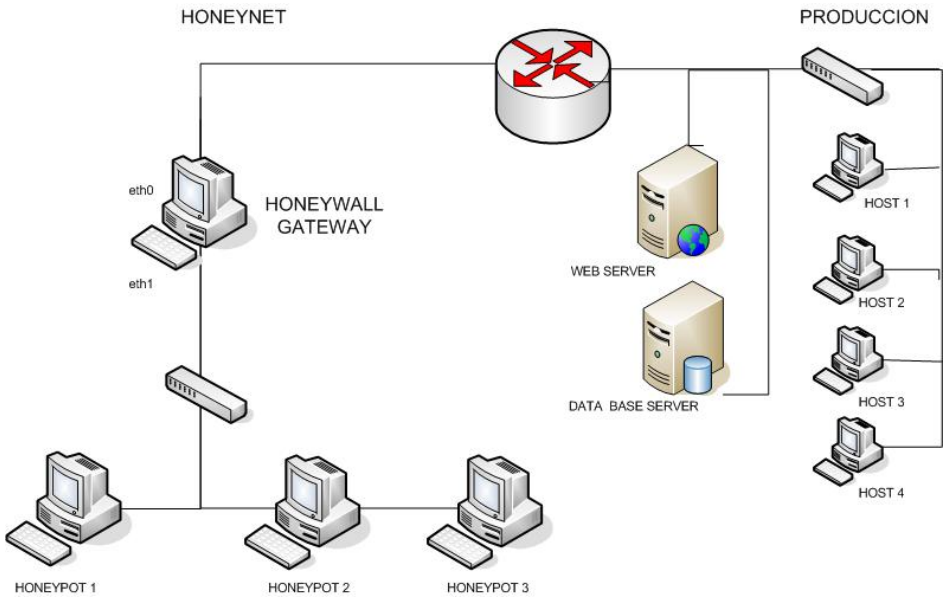

Figura 1: Arquitectura de la Honeynet y implantada en la red de producción del CENTRO DE INFORMACIÓN BIBLIOTECARIO.

Tabla 1: Tabla de las interfaces de red e IPs de los equipos en la Honeynet y la red de produción.

Equipo	eth0	eth1
Gateway	200.10.149.43	192.168.0.1
Honeypot1	192.168.0.2	
Honeypot2	192.168.0.3	
Honeypot3	192.168.0.4	
P R O D U C C I Ó N		
Equipo	**eth0**	**eth1**
Web Server	200.10.149.215	
Database Server	200.10.149.9	