Grupo de Seguridad Informática

Fundamentos de la Seguridad Informática

Seguridad en Redes

Mecanismos de mitigación

Sensores de seguridad

Sistemas de Detección de Intrusos IDPS

Introducción

- Muchos mecanismos intentan evitar las intrusiones
- Es imposible garantizar que se detendrán todos los ataques posibles
- Los sistemas de detección de intrusos apuntan a detectar los intentos de ataque, exitosos o nó

Necesidad

- No hay medidas de seguridad infalibles
- Puede surgir un nuevo tipo de ataque, o ataques que no hemos previsto
- Puede haber errores de configuración
- Puede haber un error o ataque interno
- Puede haber equipos que (aún) no hayan sido actualizados/parchados
- .....

¿Qué es un IDS?

- Un IDS (Intrusion Detection System) consiste en un conjunto de sensores obteniendo datos, localizados en los hosts o en la red
- Manejados desde una consola central
- Se analizan los datos, se reportan las posibles intrusiones, y posiblemente se reacciona

Comunicaciones del IDS

- Es importante que la comunicación entre la consola y los sensores esté protegida
- También es importante que haya un mecanismo seguro para obtener las actualizaciones de los patrones o “firmas” que distribuye el fabricante
  - Ha habido ataques a vulnerabilidades de los IDS
  - Las reglas de detección (patrones) se actualizan frecuentemente

Tipos de IDS

- Detección de **uso indebido**
  - Se compara la actividad con patrones de ataque, patrones de actividad que indican comportamiento sospechoso
  - Son tan buenos como la base de patrones de ataques disponibles
- Detección de **anomalías**
  - Técnicas estadísticas para detectar intrusos
  - Se establece el uso “normal”, y se detectan diferencias

IDS de red (NIDS)

- Busca patrones de ataques en el tráfico de red
- Típicamente, un adaptador de red en modo promiscuo ubicado en un sitio adecuado de la red monitorea y analiza todo el tráfico en tiempo real
- Matching de patrones, expresiones o bytecode
- Cruce de umbrales o frecuencias
- Correlación de eventos menores (aún no en productos comerciales)

IDS de Host (HIDS)

- Busca patrones de ataque en los archivos de log de los hosts
- Puede también chequear sumas de comprobación de archivos del sistema y ejecutables
- Pueden tener reglas más complejas (se ejecutó tal programa y luego se modificó tal archivo...)
- Algunos pueden generar alertas cuando ciertos puertos de red son accedidos

Falsos negativos y falsos positivos

- Un falso negativo es cuando el IDS no reporta una intrusión dada
- Un falso positivo es cuando el IDS reporta una alarma cuando no hay una intrusión
  - Son un problema grave. Se requiere una persona con conocimiento para investigar cada alarma
  - Son prácticamente inevitables
  - Recordemos la historia de Pedro y el Lobo

Falsos positivos

- Imaginemos que 1 de cada 1.000.000 sesiones es maliciosa
- Supongamos que tenemos una tasa de falsos positivos de 0.01%
- Entonces 100 sesiones serán detectadas como falsos positivos (y con suerte una correctamente)
- El problema es que típicamente las redes (en especial Internet) son muy “ruidosas”
  - Muchos paquetes con problemas, no necesariamente maliciosos

¿Acciones automáticas?

- ¿Podemos realizar alguna acción automática en base a lo detectado?
  - Si podemos garantizar baja tasa de falsos positivos
  - Si precisamos tal seguridad que la inconveniencia de actuar ante un falso positivo es aceptable
- Cuidado que puede ser utilizado para ataques de negación de servicio

¿Dónde monitorear?

- Fuera del firewall
  - Veremos todos los ataques que nuestro firewall detiene
  - ¿Vale la pena?
    - Para investigación/entrenamiento de personal sí
- Cerca de los equipos más importantes
  - Seguramente más fácil determinar qué es válido y qué no
  - Habrá menos falsos positivos, podremos habilitar reglas más “sensibles”

¿Switches?

- Problema: los switches no nos dejan ver el tráfico de otros puertos
- Puertos de monitoreo (copian el tráfico de uno o más puertos)
- Hardware especializado (Network Taps) para “interceptar” el tráfico de uno o varios segmentos

Sensores de Seguridad

Honeypots

¿Que es un Honeypot ?

Un honeypot es un **recurso** que simula ser un objetivo real, el cual se espera que sea atacado o comprometido. Los principales objetivos son el distraer a los atacantes y obtener información sobre el ataque y el atacante
[R. Baumann, C. Plattner]

Un honeypot es un **recurso de seguridad** cuyo valor se basa en ser escaneado, atacado o comprometido.
[L. Spitzner]

Idea

- La idea de un honeypot es dejar disponible un sistema, que aparentemente es fácil de atacar (carnada)
- Ese sistema (computadoras, archivos, redes) en realidad se protegen fuertemente, para evitar que quien logre comprometerlo pueda desde ahí realizar otras actividades maliciosas
- Es importante que estén bien protegidos. No queremos que ataques partan de nuestros equipos!!!

Utilidad

- Alerta temprana
  - Sobre nuevos ataques
  - Sobre ataques dirigidos específicamente a nosotros
- Alerta sobre nuevos ataques
- Distracción para los atacantes
- Examen en profundidad de los ataques

Valor del honeypot

- El equipo, o dirección IP, que se utilice para el honeypot, no debe tener (ni haber tenido en el pasado) ningún uso asociado
- De esta manera, estamos seguros que cualquier cosa que llegue a la trampa es ilegítima. ¡¡ NO HAY FALSAS ALARMAS !!
  - Spam
  - Portscans
  - Ataques

Clasificación

- Se clasifican según la interacción que se le permite al atacante
  - Baja interacción (ejemplo honeyd)
    - Solamente una fachada de los servicios
  - Interacción media (ejemplos mwcollect, nephentes, honeytrap)
    - Simulan en un entorno virtual el ambiente atacado
    - Permiten capturar ejemplos de herramientas de ataque, etc.

Clasificación (cont)

- Alta interacción (ej. Honeynet)
  - Sistemas reales, con el tráfico desde y hacia el honeypot muy monitoreados
- Spam honeypots
  - Específicamente para detectar abusos de spammers tratando de explotar open proxyes u open relays

¿En que se diferencian con los IDS?

Implementación

- Honeywall
  bridge-firewall / router-firewall
  http://www.honeynet.org/tools/cdrom/
- Herramientas de análisis y captura de datos
  http://www.honeynet.org/tools/index.html
- honeypots sobre maquinas virtuales (VMWare)
- Virtual Machine Monitors
  User-Mode Linux (UML) - Xen

Implementación

- Bajo/Medio nivel de interacción
  - Honeyd: http://www.honeyd.org
  - Argos: http://www.few.vu.nl/argos/
  - Back Officer Friendly: http://www.nfr.com/resource/backOfficer.php
  - HOACD: http://www.honeynet.org.br/tools/ Brazilian Distributed Honeypot Project
  - etc, etc, etc http://www.honeypots.net/honeypots/products

Bibliografía y referencias

- **R. Anderson**, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2001.
- **D. Gollman**, *Computer Security*, Wiley, 2006.
- **W. Stallings,** *Cryptography and Network Security. 4ta. ed.* Prentice Hall, 2005
- Documentación de SNORT IDS http://www.snort.org