Seguridad y Privacidad en Redes

IDS

Honeypots

Temario

- IDS
- Tipos de IDS
- Herramientas
- Ejemplos
- Monitoreo de Logs
- Honeypots

IDS

Definición: La detección de intrusiones es el arte de detectar actividad sospechosa, incorrecta o inapropiada.

...pero si ya tenemos un firewall instalado ¿porque necesitamos un IDS?

IDS

En la seguridad física de una organización, **un firewall** es el equivalente a instalar una cerca alrededor de la propiedad con un custodio en la puerta de acceso.

Por otro lado, **un IDS** es el equivalente a las cámaras, sensores y alarmas internas que existen dentro de la propiedad. Estos guardan y analizan la información que reciben para detectar patrones de comportamiento sospechoso.

IDS - Tipos

TIPOS DE IDS

- Basados en Red
- Basados en HOST
- Basados en filesystem

IDS – TIPOS

IDS basados en Red:

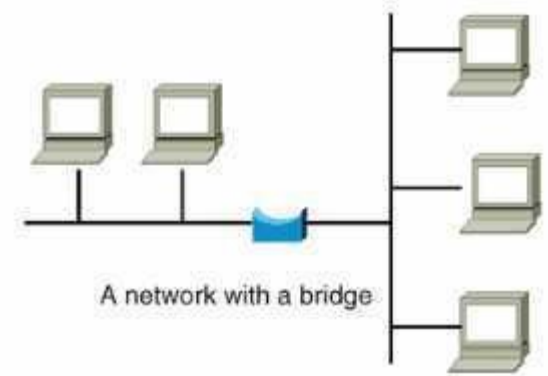
Monitorea todo el tráfico que pasa por el segmento en el que éste se encuentra, reaccionando ante cualquier anomalía o signo de actividad sospechosa. Básicamente es un sniffer que busca patrones de ataques en los paquetes observados.

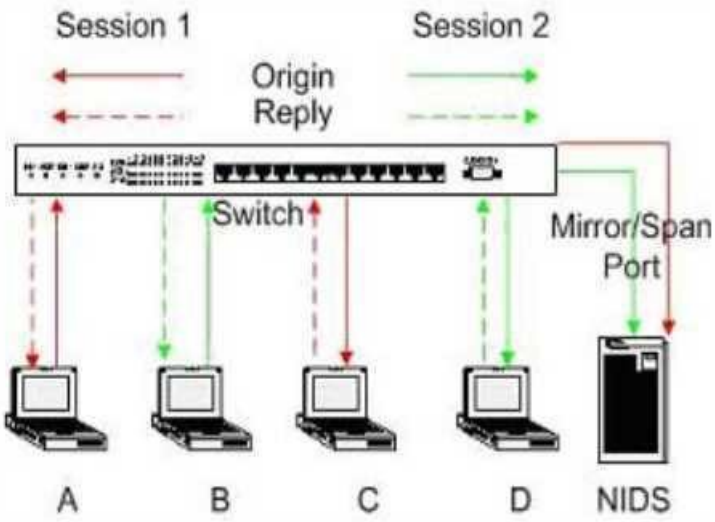
Ejemplo: Snort, BRO-IDS.

IDS – TIPOS

¿Cómo obtener el tráfico para monitorear?

- HUB
- Puerto de SPAN (Security Port Analizer) en Switch
- Modo Inline





Productos

NIDS: SNORT

Snort es un NIDS Open Source, capaz de realizar análisis y bloqueo de tráfico en tiempo real.

Puede realizar análisis de protocolos y filtros por contenido, los cuales son usados para detectar una gran variedad de ataques, como ser: escaneos, OS fingerprint, ejecución de exploits conocidos, tráfico no deseado, DoS, intentos de penetración de otros tipos (virus, backdoors).

IDS – TIPOS

IDS basados en host:

Un IDS basado en host monitorea los logs del mismo con el fin de detectar actividad sospechosa. Entre sus ventajas podemos mencionar la detección de patrones de ataques en tiempo real, pudiendo evitarlos y reportarlos.

Ejemplos: OSSEC, Fail2ban, Personals firewalls, etc.

Productos

HIDS: OSSEC

OSSEC es un Open Source Host-based Intrusion Detection System. Hace análisis de log, chequeos de integridad, monitoreo de la registry en entornos Windows, detección de rootkits, alertas en tiempo real y respuesta activa.

Corre en: Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows.

Productos

HIDS: FAIL2BAN

Banea IPs que causan múltiples errores de autenticación.

Funciona monitoreando archivos de log (ej /var/log/auth.log, /var/log/apache/access.log) y temporalmente o permanentemente filtra las ips con muchos fallos actualizando las reglas del firewall.

Desde la versión 0.7 soporta otras acciones, ej enviar un mail de notificación

IDS – TIPOS

IDS basados en FileSystem :

Cuando la seguridad de un sistema es comprometida, el atacante generalmente altera ciertos archivos claves para asegurarse nuevamente el acceso y para prevenir que lo detecten. Un IDS basado en filesystem realiza una función de hash sobre los archivos que luego chequea periódicamente para determinar si algo fue cambiado.

Ejemplo: Tripwire, Saint

Productos

Fileserver IDS TRIPWIRE:

```
===============================================================================
Report Summary:
===============================================================================

Host name:                    lihuen
Host IP address:              127.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/lihuen.twd
Command line used:            tripwire --check /etc /etc/hosts

===============================================================================
Rule Summary:
===============================================================================


-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                     Severity Level    Added    Removed  Modified
  ---------                     --------------    -----    -------  --------
* Other configuration files     66                0        0        2
  (/etc)
```

Productos

Filesystem IDS TRIPWIRE:

```
================================================================================
Object Detail:
================================================================================

--------------------------------------------------------------------------------
  Section: Unix File System
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Rule Name: Other configuration files (/etc)
Severity Level: 66
--------------------------------------------------------------------------------
  ----------------------------------------
  Modified Objects: 2
  ----------------------------------------

Modified object name:  /etc

  Property:             Expected                  Observed
  -------------         -----------               -----------
* Size                  260                       280
* Modify Time           Tue Oct 25 22:12:57 2011  Wed Oct 26 02:58:29 2011


Modified object name:  /etc/hosts

  Property:             Expected                  Observed
  -------------         -----------               -----------
* Inode Number          456619                    463650
* Size                  37                        65
* Modify Time           Tue Aug 30 15:04:46 2011  Wed Oct 26 02:58:29 2011
* Blocks                1                         8
* CRC32                 Aog4p9                    DJdJLq
* MD5                   AbxXiW5ksFCiO0MbXnJFES    C98p4cm7U89FflCL3MQW7d
```

IPS

Los sistemas de prevención de intrusiones son mecanismos de defensa proactivos diseñados para detectar actividad maliciosa y detener intrusiones, bloqueando dicha actividad “ofensiva” automáticamente antes de que ésta realice algún daño.

Tipos de IPS:

- Basado en Host: es aquél en el cual la aplicación de prevención de intrusiones reside en un host específico y previene intrusiones únicamente en el mismo.
- Basado en red: Es aquél que reside en un host de la red y toma acciones para prevenir intrusiones en dicha red.

Productos

SNORT – Respuesta activa

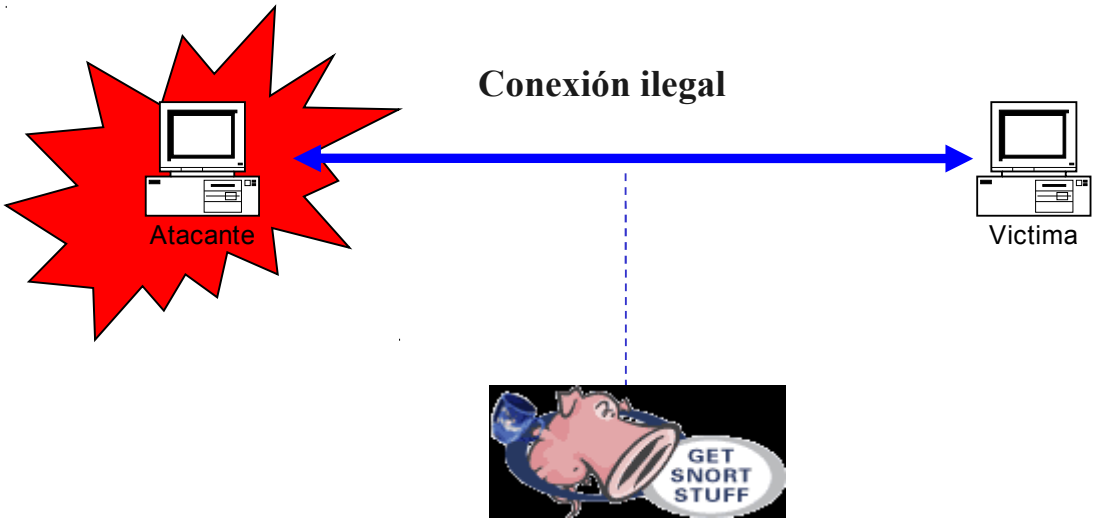
La respuesta activa permite que las sesiones sean derribadas de forma automática basándose en las reglas de Snort. Para ello existen dos métodos:

- TCP: crea paquetes RST para cada uno de los extremos de la conexión.
- UDP: Crea una variedad de respuestas de ICMP a uno o ambos extremos de la conexión.

Productos

SNORT – Respuesta activa

DETECCIÓN

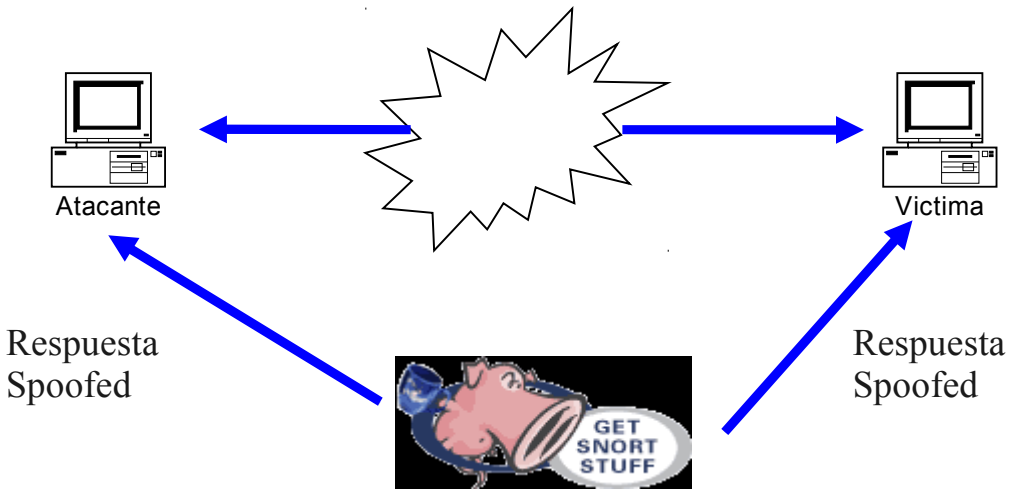


SNORT

Productos

SNORT – Respuesta activa

ACCIÓN



Productos

IPS Snort-inline

Es básicamente una versión modificada de Snort. Usa nuevos tipos de directivas para el encabezado (drop, sdrop, reject) para indicar a Iptables qué debe hacer con el paquete (descartarlo y loguear, descarta e interrumpe la conexión, simplemente descarta).

Es un IPS que usa firmas existentes del IDS para tomar decisiones.

Análisis de logs de la red

Algunos problemas:

Muchas veces los administradores ignoran los archivos de logs debido a:

- Falta de tiempo para revisar los mismos.
- Falta de conocimiento respecto al formato de los logs
- Falta de conocimiento respecto a los procedimientos que deben seguirse para hacer un buen análisis de los archivos de log.

Existen muchos tipos diferentes de archivos de logs ya que los mismos provienen de distintas fuentes como ser firewalls, routers, IDSs.

Análisis de logs de la red

Importancia de los archivos de logs:

Como el propósito principal de los archivos de log es registrar eventos significativos o interesantes, se pueden usar para:

- Manejo de incidentes
- Detección de intrusiones
- Correlación de eventos
- Troubleshooting en general

Permiten detectar escaneos, intentos de intrusión, equipamiento mal configurado, etc.

Análisis de logs de la red

Algunos tips:

- Establecer una frecuencia razonable para analizar los logs.
- Establecer la cantidad de tiempo que se invertirá en cada análisis de logs.
- Establecer el nivel de detalle que se usará para analizar los logs.

Es importante también:

- Automatizar el análisis de logs
- Identificar los datos importantes de los archivos de logs.

Por ello es de gran utilidad contar con herramientas que faciliten esta tarea.

Análisis de logs de la red

Un ejemplo: Logwatch:

Logwatch es un analizador de logs customizable que se ejecuta durante un un período de tiempo dado y crea un reporte en base a los logs de los servicios que el usuario ha especificado.

El nivel de detalle de la información que muestra también puede ser especificado por el usuario.

Tiene como fin brindar la información más relevante de los archivos de logs, a partir de la cual el administrador, si así lo desea, puede recurrir al correspondiente archivo de log para obtener información más detallada.

Honeypots

HoneyPots :

Es una herramienta que puede simular uno o más host vulnerables, siendo un blanco fácil de atacar.

Dado que éstos no son reales, cualquier intento de conexión es sospechoso:

- Ataque
- Prueba
- Escaneo

Honeypots

HoneyPots :

"Todo arte de la guerra se basa en el engaño"

Permiten ganar tiempo, ya que los intentos de intrusión se concentran en el HoneyPot, permitiendo solucionar posibles problemas reales.

Su propósito es ser comprometido por un usuario malicioso para aprender de las herramientas, tácticas y motivos que alientan a los intrusos.

Honeypots

HoneyPots :

Son un recurso de seguridad proactivos.

Se pueden agrupar dentro de dos categorías o tipos:

- Producción (directamente ayudan a proteger una organización)
- Investigación (predicción, reunir datos)

Honeypots

HoneyPots :

Pueden ser usados para:

- Prevención (Para ataques automatizados y para desmoralizar a los atacantes)
- Detección de actividad no autorizada
- Responder ataques

Honeypots

HoneyPots :

Ventajas:

- Gran valor de los datos de actividad recolectados.
- Uso de los recursos: no requieren tecnología de punta.
- Simplicidad

Desventajas

- Fingerprinting: Hay patrones y características que delatan su propósito.
- Riesgo: agregan un riesgo adicional ya que si son comprometidos pueden ser usados para atacar.

Honeypots

HoneyPots :

De acuerdo al nivel de interacción que tendrá el atacante con el honeypot, los mismos pueden clasificarse como :

- Honeypots de baja interacción
- Honepots de alta interacción

Honeypots

HoneyPots de baja interacción:

Características

- Emulación de servicios
- Fáciles de implantar, configurar, mantener y monitorear.
- Funcionalidad reducida
- Su principal propósito es detectar escaneos e intentos de sesión no autorizados.
- Bajo riesgo.
- Reunión de poca información.

Honeypots

HoneyPots de alta interacción:

Características

- Equipo real con servicios reales
- Alto riesgo
- Se reúne bastante información sobre la actividad del intruso.
- Difíciles de implantar, configurar, mantener y monitorear.
- Para mitigar riesgos se colocan dentro de un ambiente controlado, por ejemplo detrás de un firewall.
- Control de tráfico de salida

Honeypots

Nepenthes

Honeypot de baja interacción.

Permite detectar estaciones infectadas en la red.

Permite recolectar malware, el cual si se quiere puede ser analizado.

Simula diversos servicios vulnerables a través de los cuales el malware se suele propagar.

Honeypots

Honey Google

Es un honeypot indexado en google

http://gray-world.net/etc/passwd/#wtf

Se encuentra realizando la siguiente búsqueda en GOOGLE:

Name Size index "/etc/passwd" admin Apache "Last Modified"

Honeypots

Honeynets:

- Es una red real de varios sistemas y aplicaciones. Pueden utilizar varios sistemas operativos con diferentes servicios al mismo tiempo creando un entorno que refleja una red productiva.

Es usada por el Honeynet Project a fin de aprender herramientas, tácticas y motivos de la comunidad blackhat y compartir lo aprendido.

http://www.honeynet.org/

Referencias

- http://www.snort.org
- http://acidlab.sourceforge.net/
- http://www.ossec.net/
- http://sourceforge.net/projects/tripwire/
- http://www.alienvault.com/community.php?section=Home