Unidad VI

DETECCIÓN Y PREVENCIÓN DE INTRUSOS

Características de los IDS e IPS

- Los sistemas de detección de intrusiones IDS (intrusion Detection Systems) fueron implementados para monitorizar de manera pasiva el tráfico de la red.
- Un IDS copia el tráfico de red y lo analiza en lugar de reenviar los paquetes reales
- Compara el tráfico capturado con firmas maliciosas conocidas de manera offline del mismo modo que el software busca virus.
- Esta implementación de IDS se conoce como "modo promiscuo"
- Al operar con una copia del tráfico, el IDS no tiene efectos negativos sobre el flujo real de paquetes del tráfico reenviado; sin embargo, no puede evitar que el tráfico malicioso de ataque alcance al sistema objetivo.

Modo promiscuo

- Las características del IDS en modo promiscuo son las siguientes:
  - No tiene impacto sobre la red, no crea latencia ni genera jitter.
  - La acción de respuestas no puede detectar los paquetes disparados.
  - No tiene impacto sobre la red si el sensor falla o se sobrecarga
  - Se requieren ajustes correctos para las acciones de respuesta
  - Se necesita de una política de seguridad bien definida
  - Son más vulnerables a técnicas de evasión.

IPS (Intrusion Prevention System)

- Se implementa en modo en línea
- No permite el paso de tráfico malicioso respondiendo inmediatamente. Esto significa que todo el tráfico de entrada y de salida debe fluir a través de él para ser procesado.

Modo en línea

- Las características del IPS en modo en línea son las siguientes:
  - Detiene los paquetes disparadores
  - Puede tener algún impacto sobre la red, al crear latencia y jitter.
  - Los posibles problemas de los sensores afectan el tráfico de red
  - Puede obtener técnicas de normalización de flujo
  - Se necesita una política de seguridad bien definida

Sensores

Las tecnologías IDS e IPS se despliegan como sensores, que pueden ser cualquiera de los siguientes dispositivos:

- Un router configurado con software IPS
- Un dispositivo diseñado específicamente para proporcionar servicios IDS o IPS dedicados
- Un módulo de red instalado en un dispositivo de seguridad adaptable
- Un servidor

Plataforma de sensores

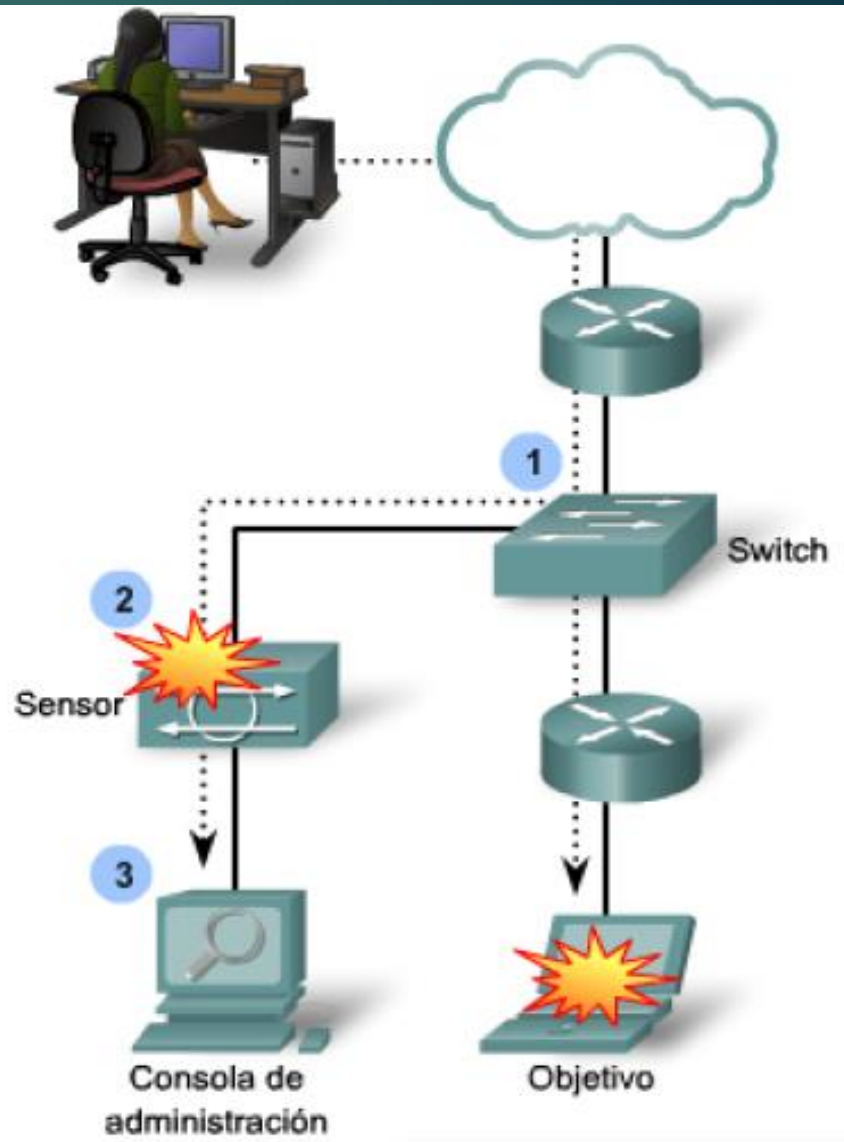
- Appliance dedicado, serie 4200
- Software en Cisco IOS (advance security)
- Software Open Source
- Módulo router AIM-IPS NME-IPS
- ASA firewall
- Multilayer Switch 6500

Sistema de detección de intrusos

1. Se lanza un ataque en una red que tiene un sensor en modo IDS promiscuo; por lo tanto, se envían copias de todos los paquetes al sensor IDS para análisis. Sin embargo, la máquina a la que el ataque está dirigido experimentará el ataque malicioso.

2. El sensor IDS busca coincidencias entre el tráfico malicioso y las firmas y envía al switch un comando para denegarle el acceso.

3. El IDS envía una alarma a una consola de administración con el propósito de registrar el incidente y otros.



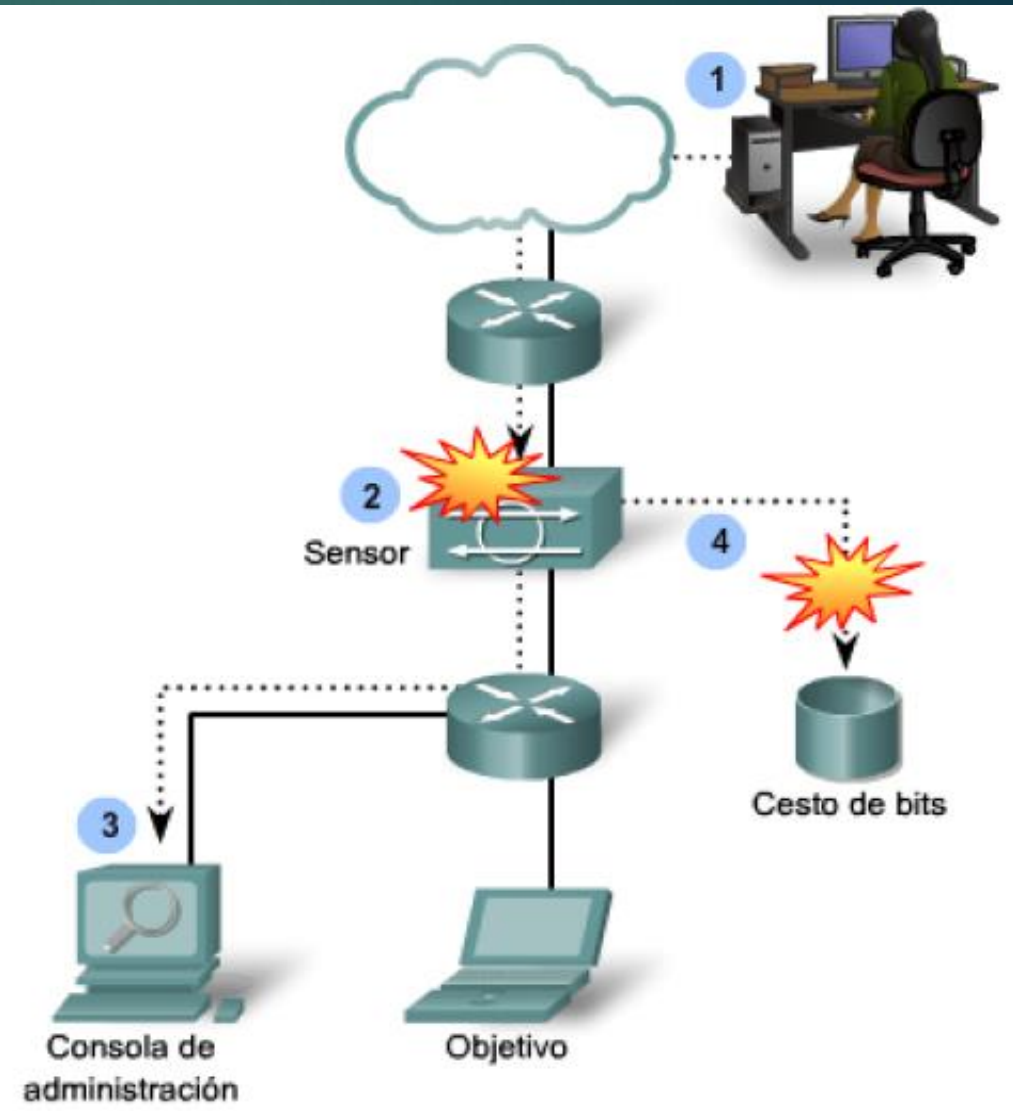
Sistemas de prevención de intrusos

1. Se lanza un ataque en una red que tiene un sensor en modo IPS (modo en línea).

2. El sensor IPS analiza los paquetes a mendida que entran a la interfaz del sensor IPS. El sensor IPS busca coincidencias entre el tráfico malicioso y las firmas y el ataque se detiene inmediatamente.

3. El sensor IPS puede enviar una alarma a la consola de administración con el propósito de registrar el incidente u otros.

4. El tráfico que viola una política puede ser descartado por el sensor IPS.



Características de IDS/IPS

- Ambas tecnologías se despliegan como sensores
- Ambas tecnologías usan reglas para detectar patrones de mal uso en el tráfico de la red
- Ambas pueden detectar patrones atómicos (un solo paquete) o patrones compuestos (multipaquetes).

Comparaciones de IDS/IPS

	Ventajas	Desventajas
IDS (Modo promiscuo)	• No tiene impacto sobre la red (latencia, jitter) • No tiene impacto sobre la red si el sensor falla • No tiene impacto sobre la red si el sensor se sobrecarga	• La acción de respuestas no puede detener los paquetes disparadores • Se requieren ajustes correctos para las acciones de respuesta • Se debe tener una política de seguridad bien definida • Más vulnerable a técnicas de evasión
IPS (Modo en línea)	• Detiene paquetes disparadores • Puede usar técnicas de normalización de flujo	• Los problemas de los sensores pueden afectar el tráfico de la red • La sobrecarga del sensor tiene impacto sobre la red • Se debe tener una política de seguridad bien definida • Algún impacto en la red (latencia, jitter)

IPS basados en red

Las implementaciones IPS basadas en red analizan la actividad de toda la red en búsqueda de actividad maliciosa. Los dispositivos de red, como los routers ISR, los dispositivos firewall ASA, los módulos de red Catalyst 6500 o los dispositivos IPS dedicados son configurados para monitorear firmas conocidas. También pueden detectar patrones de tráfico anormal.

IPS basados en hosts (HIPS)

Las implementaciones basadas en hosts son instaladas en computadoras individuales usando software de sistemas de prevención de intrusiones de host (host intrusion prevention system - HIPS)

Ventajas y desventajas de los HIPS

Ventajas	Desventajas
• Puede determinarse fácilmente el éxito o fracaso de un ataque. • Los HIPS no tienen que preocuparse por ataques de fragmentación o Time to Live (TTL) variable. • Los HIPS tienen acceso al tráfico de forma no cifrada.	• Los HIPS no proporcionan una visualización completa de la red. • Los HIPS deben ser soportados en múltiples sistemas operativos.

Comparación HIPS vs IPS

	Ventajas	Desventajas
HIPS	• Específico de cada host • Protege a los hosts luego del descifrado • Proporciona protección de cifrado de nivel de aplicación	• Depende del sistema operativo • No son vistos eventos de red de nivel menor • El host es visible para los atacantes
IPS de red	• Eficiente en el costo • No es visible en la red • Independiente del sistema operativo • Son vistos eventos de red de menor nivel	• No puede examinar tráfico cifrado • No sabe si un ataque fue exitoso

Firmas

- Cuando los sensores escanean los paquetes de red, utilizan las firmas para detectar algún tipo de actividad intrusiva, como ataques de DoS.
- Estas firmas identifican puntualmente gusanos, virus, anomalías en los protocolos o tráfico malicioso específico.
- Las firmas de dividen en tres partes bien definidas:
  - Tipo
  - Alarma
  - Acción

Niveles de severidad

Basándose en la severidad de la firma puede ajustarse a uno de estos cuatro niveles de severidad:

- **Alto:** se detectan los tipos de la ataques usados para ganar acceso o causar un ataque DoS y es extremadamente probable una amenaza inmediata
- **Medio:** se detecta la actividad de la red anormal que puede ser considerada maliciosa y es probable una amenaza inmediata
- **Bajo:** la actividad de la red anormal que puede ser considerada maliciosa es detectada, pero es poco probable una amenaza inmediata
- **Informativo:** la actividad que dispara la firma no es considerada una amenaza inmediata, pero muestra información útil

Tipos de firma

- Atómicos: es la forma más simple. Consiste en un solo paquete, actividad o evento examinado para determinar si coincide con una forma configurada.

- Compuestos: También se conoce como firmas stateful (con estados). Este tipo de firma identifica una secuencia de operaciones distribuidas en múltiples hosts durante un periodo de tiempo arbitrario.

Firmas

- Para detener el tráfico malicioso, la red debe ser capaz de identificarlo primero.
- Afortunadamente, el tráfico malicioso tiene características, o "firmas", distintivas.
- Una firma es un grupo de reglas que los IDS e IPS usan para detectar actividad intrusiva típica, como ataques de DoS. Estas firmas identifican puntualmente gusanos, virus, anomalías en los protocolos o tráfico malicioso específico.
- Las firmas IPS son conceptualmente similares al archivo virus.dat usado por escáner de virus.

	Ventajas	Desventajas
Detección basada en patrones	• Configuración fácil • Menos falsos positivos • Buen diseño de firma	• No hay detección de firmas desconocidas • Inicialmente devuelve muchos falsos positivos • Deben crearse, actualizarse y ajustarse las firmas
Detección basada en anomalías	• Simple y confiable • Políticas personalizadas • Puede detectar ataques desconocidos	• Salida genérica • Debe crearse la política
Detección basada en políticas	• Configuración fácil • Puede detectar ataques desconocidos	• Dificultad para perfilar la actividad típica en grandes redes • El perfil del tráfico debe ser constante
Detección basada en honeypots	• Ventana para ver los ataques • Distrae y confunde a los atacantes • Disminuye la velocidad y evita los ataques • Recolecta información sobre el ataque	• Servidor honeypot dedicado • El servidor honeypot no puede ser confiable

Terminología Positivo/Negativo

- **Falso Positivo**
  - Es el tráfico que existe en la red que NO es malicioso, pero que generó una alarma.
- **Falso negativo**
  - Es el tráfico malicioso que existe en una red, pero ni el IDS/IPS generan una alarma.
- **Positivo verdadero**
  - Es el tráfico malicioso que el IDS/IPS generó alarma
- **Positivo negativo**
  - Es el tráfico NO malicioso y el IDS/IPS no genera alarma

Acciones de las firmas

1. Generar una alerta
2. Ingresar a la actividad en el registro
3. Descartar o detener la actividad
4. Reiniciar una conexión TCP
5. Bloquear actividad futura
6. Permitir la actividad

Mejores prácticas

- Implementar IPS para analizar el tráfico que va hacia los servidores críticos
- Tratar de instalar Appliance
- Automatizar la actualización de firmas
- Hacer un “tunning” de la infraestructura de IDS/IPS

Administración y monitorización IDS/IPS

- **Administración:** Pueden ser administrados individualmente o centralmente de acuerdo del tamaño de la red

- **Correlación de eventos:** Es el proceso por el cual se correlacionan ataques y otros eventos que toman lugar simultáneamente en diferentes puntos de una red

- **Personal de seguridad:** Se necesita personal apropiado para analizar esta actividad y determinar como el IDS/IPS está protegiendo la red.

- **Plan de respuesta de incidentes:** Cuando un sistema de red se halla comprometido, debe de implementarse un plan de respuesta para que el sistema comprometido vuelta a su estado normal y determinar las consecuencias de lo acontecido.

PRÁCTICA

- Instalación de HIPS
  - Endpoint ESET

https://www.youtube.com/watch?v=p4-SIPH83L8