Primeros pasos en el mundo de los IDS/IPS

ALVEIRO MEJÍA LARA
INGENIERO DE SISTEMAS
EST. ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MAYO 2017

¿Por qué esta charla?
¿Qué es un IDS?
¿En qué se diferencia de un IPS?
¿Cómo funcionan estos programas?
¿Cómo se clasifican?
¿Cuáles son los más populares?
¿Por qué instalar SmoothSec?
¿Cómo funciona Snorby?
¿Cómo entender una regla?
Otras inquietudes…

¿Por qué esta charla?

*-Era uno de los temas para mi Proyecto de grado de la especialización.
*-Aprendo más cuando intento compartir lo aprendido.
*-Tener la oportunidad de conversar sobre el tema y aprender de ustedes.

¿Qué es un IDS?

Intrusion Detection System

Es una herramienta de seguridad, implementada como hardware o software, que se encarga de monitorear los eventos que ocurren en un sistema informático tratando de detectar intentos de intrusión por terceros no autorizados.

¿Qué es un IDS?

El concepto de Sistemas de Detección de Intrusos fue introducido en el año 1980 por Anderson en su reporte computer security threat monitoring and surveillance cuyo objetivo era mejorar la capacidad de auditoría y vigilancia de la seguridad informática de los sistemas de los clientes.

¿En qué se diferencia de un IPS?

Intrusion Prevention System

IDS Informa, IPS toma acciones para frenar el posible ataque.

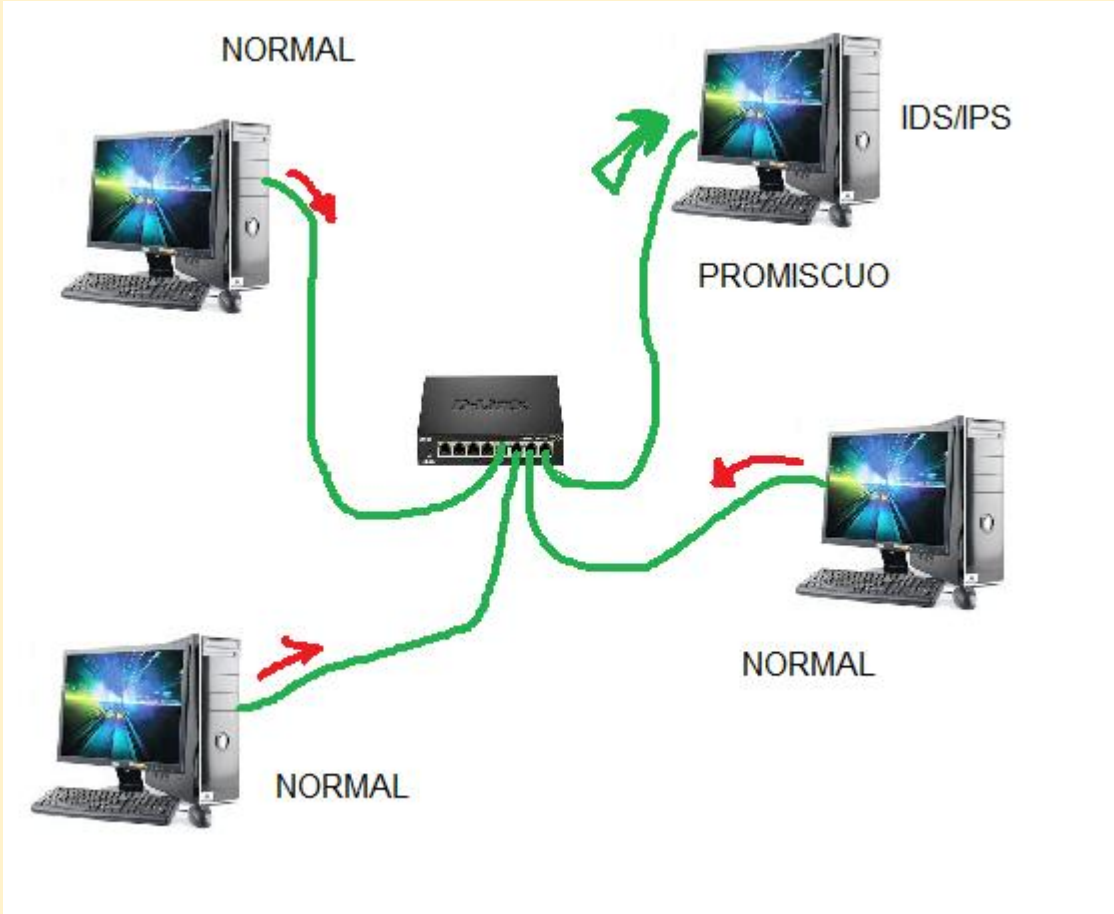
¿Cómo funcionan estos programas?

*- Cambia el modo de funcionamiento de la NIC a promiscuo, para escuchar todo el tráfico de la red.

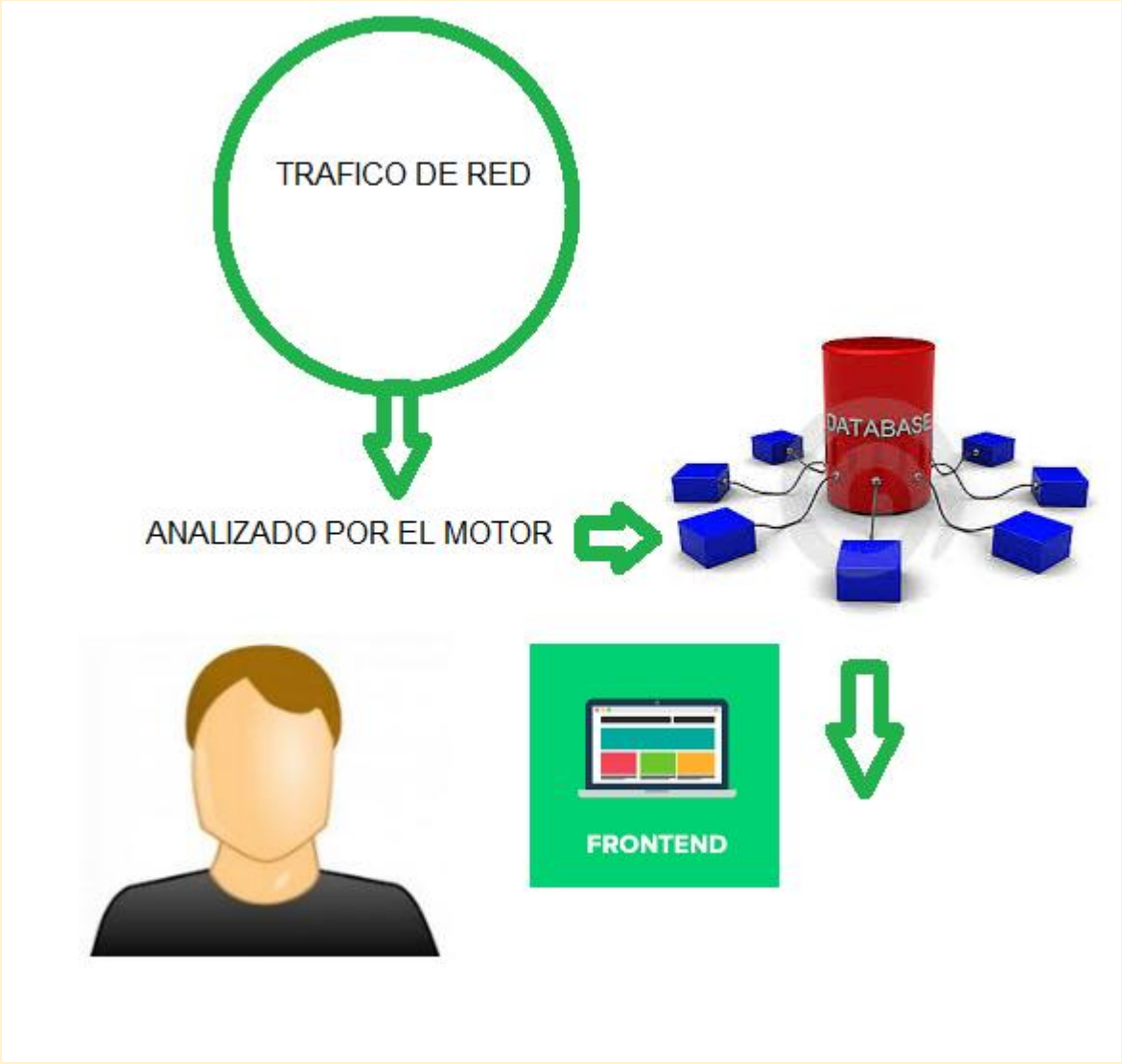
*- Revisa ese tráfico en busca de patrones de bits ya conocidos como sospechosos.

*- Genera un alerta indicando toda la información relacionada con la detección.

¿Cómo funcionan estos programas?



¿Cómo funcionan estos programas?



¿Cómo se clasifican?

Criterio de clasificación	Tipos
Fuentes de información	IDS basados en red (NIDS)
	IDS basados en host (HIDS)
Tipo de análisis	Detección de abusos o firmas
	Detección de anomalías
Respuesta	Respuestas pasivas
	Respuestas activas

Fuente: http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

¿Cuáles son los más populares? Comerciales. Networtworld*

1- Secure IDS de Cisco. Los Mejores de los Cinco.
2- RealSecure de ISS. Los Mejores de los Cinco.
3- IDS Dragon de Enterasys (Rendimiento: OK. Complicada instalación, configuración y gestión: Baja)
4- eTrust de CA (poderosa gestión, estupenda funcionalidad, Gestión lógica e intuitiva: OK. Demasiadas aplicaciones separadas: Baja)
5- SecureNet Pro de Intrusion.com, (Sencillo de instalar: OK. Problemas de rendimiento: baja).

¿Cuáles son los más populares? Gratuitos:

SNORT: Por Sourcefire. Mayor aplicación mundial. Usa BASE (Basic Analysis and Security Engine). BASE es desarrollado por Secure Ideas.

OSSEC (Open Source SECurity): Análisis de registro, valida la comprobación de la integridad, hace seguimiento de políticas, realiza detección de rootkits.

SURICATA : Gran rendimiento, monitoreo basado en red. Propiedad de la Fundación Seguridad de la Información abierta (OISF).

SAMHAIN : Comprobación de integridad de registros, descubrimiento de rootkits, supervisión de puertos y procesos que están ocultos.

EASYIDS : Fácil de instalar. Seguridad de red. Incluye CentOS, Barnyard2, Snort, MYSQL, NTOP, BASE, Arpwatch entre otras aplicaciones.

SMOOTH-SEC : Distribución Linux basada en Debian que contiene un IDS/IPS totalmente listo y muy liviano. Contiene Snorby, Suricata, Snort y Pulledpork. (Phillip Baley)

PATRIOT NG : Monitorea sistemas Windows. Avisa cambios en el ordenador, dando la posibilidad de permitirlos o rechazarlos.

TRIPWIRE : es el IDS basado en host más aclamado para Linux. Asegura controles fundamentales para protegerse contra ataques cibernéticos.

SWATCH : Notifica a los administradores de las incoherencias en el registro del equipo.

LIDS : (Linux Intrusion Detection System) es un parche del kernel, instrumento de administración, vigila la modificación de ficheros y preserva procesos y archivos, incluso del propio superusuario.

¿Cuáles son los más populares?

SURICATA

Multi-Threaded Processing. Varios procesos / subprocesos de forma simultánea, procesa gran cantidad de paquetes de forma simultánea.

Automatic Protocol Detection. A parte de los protocolos IP, TCP, UDP e ICMP, tiene palabras claves para otros protocolos como FTP, HTTP, TLS, SMB. De esa forma escribir reglas independientemente del puerto que un protocolo use, ya sea por defecto o no ya que éste es automáticamente detectado.

Performance Statistics. Las estádísticas se vuelcan el en archivo /var/log/suricata/stat.log.

HTTP Log Module. Vuelca todas las peticiones HTTP (tanto desde HOME_NET > EXTERNAl_NET como en el sentido contrario) en un archivo /var/log/http.log.

Descompresión Gzip por parte del analizador HTTP.

Soporta, al igual que Snort, Unified2 Output.

Soporta IPv6.

¿Cuáles son los más populares?

Configuración de Suricata.
etc/suricata/surucata.yaml
max-pending-packets: 50 (5000-2000)
action-order (– pass – drop –reject – alert)
outputs (/var/log/ids_1/)
Stats
	enabled: yes
	filename: estadisticas.log
	interval: 5
	append: yes/no
address-groups:
	HOME_NET: “[192.168.1.0/24,172.16.1.0/24]”
	EXTERNAL_NET: any
	HTTP_SERVERS: “$HOME_NET”
	SMTP_SERVERS: “$HOME_NET”
	SQL_SERVERS: “$HOME_NET”
	DNS_SERVERS: “$HOME_NET”

¿Cuáles son los más populares?

Configuración de Suricata.

port-groups:

HTTP_PORTS: “80”
SHELLCODE_PORTS: “!80”
ORACLE_PORTS: 1521
SSH_PORTS: 22

default-rule-path /etc/suricata/rules
rule-files:

- local.rules
- backdoor.rules
- bad-traffic.rules
- chat.rules
- ddos.rules
- nmap.rules

¿Por qué instalar SmoothSec?

Snort

- Problemas con las versiones de Linux y los comandos
- Cómo ver las alertas

EasyIDS

- Dos NIC
- No detectó Ataques

Me Funcionó

SmoothSec
Intrusion Detection Made Simple

¿Cómo funciona Snorby?

Vídeo

¿Cómo entender una regla?

#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "BLEEDING-EDGE VIRUS Agobot/Phatbot Infection Successful"; flow: established; dsize: 40; content:"221 Goodbye, have a good infection |3a 29 2e 0d 0a|"; reference:url,www.lurhq.com/phatbot.html; classtype: trojan-activity; sid: 2000014; rev:3;)

¿Cómo entender una regla?

Emerging Threats (ET)
Emerging Threats Pro
VRT
Snort

¿Cómo entender una regla?

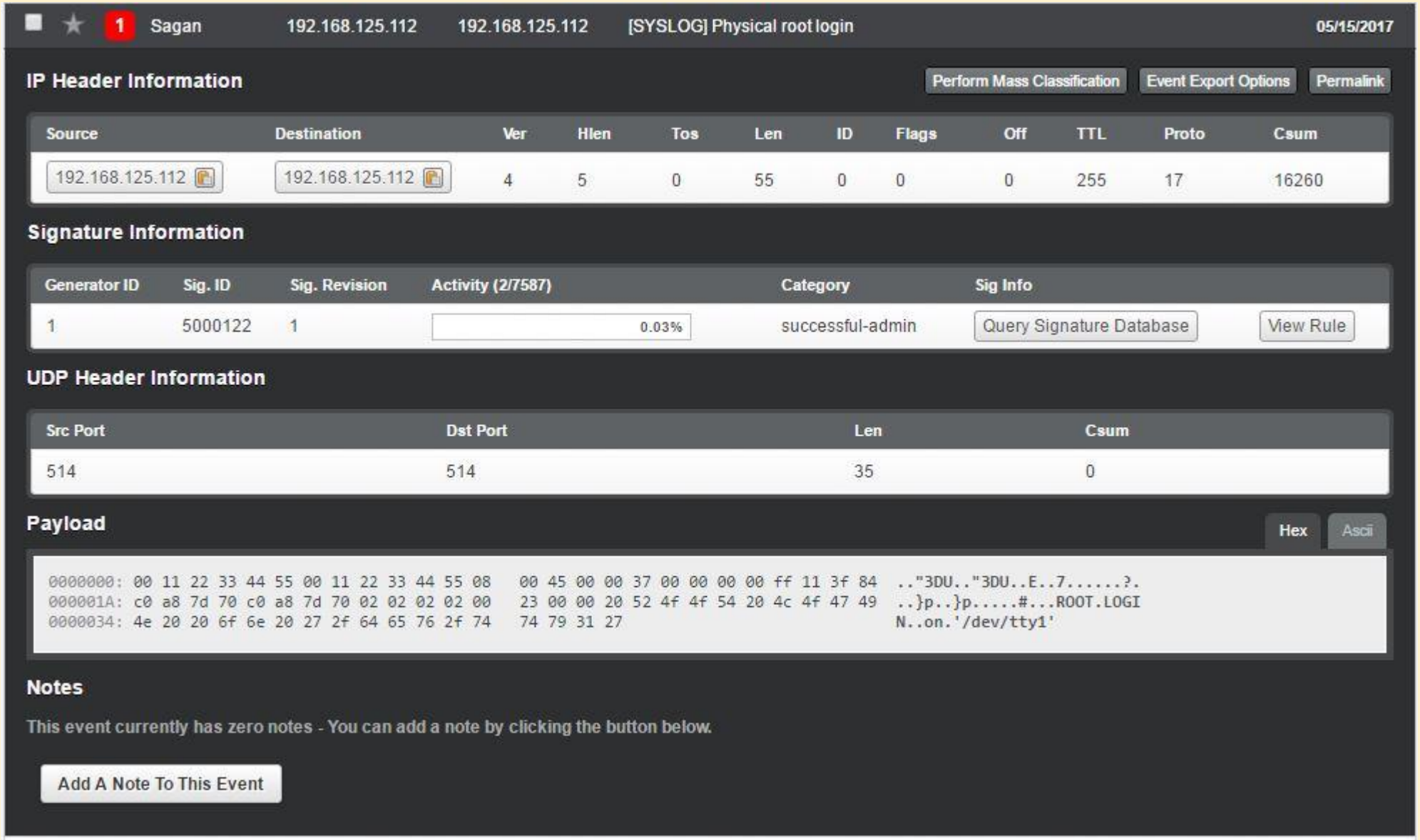
[103.236.201.110,103.250.73.6,103.27.124.82,103.29.70.23,103.3.61.114,103.56.207.84,104.167.116.234,104.200.20.46,104.200.24.17,104.206.237.21] any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node Traffic group 1";
reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold: type limit, track by_src, seconds 60, count 1; classtype:misc-attack;
flowbits:set,ET.TorIP; sid:2520000; rev:2965;)
alert ip
[104.208.158.116,104.233.105.123,104.236.128.108,104.236.141.156,106.187.37.101,107.181.174.84,107.191.56.192,108.175.11.230,108.85.99.10,109.108.3.87] any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node Traffic group 2";
reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold: type limit, track by_src, seconds 60, count 1; classtype:misc-attack;
flowbits:set,ET.TorIP; sid:2520002; rev:2965;)
alert ip
[109.126.9.228,109.163.234.2,109.163.234.4,109.163.234.5,109.163.234.7,109.163.234.8,109.163.234.9,109.169.33.163,109.190.182.44,109.201.133.100] any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node Traffic group 3";
reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold: type limit, track by_src, seconds 60, count 1; classtype:misc-attack;
flowbits:set,ET.TorIP; sid:2520004; rev:2965;)
alert ip
[109.63.235.182,110.174.43.136,111.90.145.133,117.201.240.2,118.163.74.160,120.29.217.46,124.109.1.207,125.212.241.182,128.127.105.159,128.153.146.125] any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node Traffic group 4";
reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold: type limit, track by_src, seconds 60, count 1; classtype:misc-attack;
flowbits:set,ET.TorIP; sid:2520006; rev:2965;)
alert ip
[128.199.47.160,130.204.161.3,130.226.169.137,130.25.55.39,136.243.249.6,137.74.167.224,137.74.167.96,137.74.169.241,137.74.224.142,138.197.207.243] any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node Traffic group 5";
reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold: type limit, track by_src, seconds 60, count 1; classtype:misc-attack;
flowbits:set,ET.TorIP; sid:2520008; rev:2965;)

Otras inquietudes…

MUCHAS GRACIAS…

Imágenes de Apoyo

Imágenes de Apoyo



Imágenes de Apoyo