**ÍNDEX**

[Introducció a IDS/IPS 1](#_Toc197724321)

[Comparació entre Sistemes IDS/IPS 1](#_Toc197724322)

[Instal·lació i Configuració Bàsica 3](#_Toc197724323)

[Definició de Polítiques de Seguretat 8](#_Toc197724324)

[Verificació de l’enviament d’alertes per correu 11](#_Toc197724325)

[SIMULACIÓ D’ATACS I RESPOSTA 12](#_Toc197724326)

[SIMULACIÓ D’AUTENTICACIÓ 13](#_Toc197724327)

[WEBGRAFIA 15](#_Toc197724328)

Introducció a IDS/IPS

Un sistema de detecció d'intrusions (IDS) és una eina de seguretat de xarxa que monitoritza el trànsit i els dispositius de la xarxa per cercar activitats malicioses conegudes, activitats sospitoses o infraccions de les polítiques de seguretat.

Un sistema de prevenció d'intrusions (IPS), és una tecnologia que vigila una xarxa per detectar qualsevol activitat maliciosa que intenti aprofitar la vulnerabilitat coneguda.

Aquests sistemes són essencials per la seguretat en xarxa perquè permet detectar i prevenir diferents amenaces proporcionant una capa addicional de protecció de la infraestructura de TI.

**Amenaces comunes:**

* Atacs de denegació de servei **(DoS/DDoS)**
* Injeccions SQL
* Escaneigs de ports i reconeixement de xarxa
* Atacs de codi maliciós i exploits coneguts

Comparació entre Sistemes IDS/IPS

|  |  |  |  |
| --- | --- | --- | --- |
| **Característica** | **Snort** | **Suricata** | **Zeek** |
| **Enfocament de detecció** | Basat en signatures | Signatura + basat en anomalies | Anàlisi del trànsit de xarxa |
| **Arquitectura de processament** | Monofil | Multiprocés | Multiprocés |
| **Cas d'ús** | IDS/IPS en temps real | IDS/IPS + NSM en temps real | Investigació forense, cerca d'amenaces |
| **Inspecció profunda de paquets** | Limitada | DPI avançat | Registra metadades, no càrregues útils de paquets |
| **Anàlisi de protocol** | Bàsic | Avançat (HTTP, TLS, DNS, etc.) | Amplia recopilació de metadades |
| **Bloqueig d'amenaces en temps real** | Sí | Sí | No (monitorització passiva) |
| **Rendiment** | Més lent i amb alt ús de CPU | Alt rendiment | Alt requeriment d'emmagatzematge |
| **Personalització** | Basat en regles | Detecció basada en regles + protocol | Basat en scripts |
| **Corba d'aprenentatge** | Apte per a principiants | Moderat | Pronunciada (requereix scripting) |
| **Integració** | pfSense, SIEM | SIEM, pila ELK | SIEM, ELK Stack, plataformes de cerca d'amenaces |

Nosaltres hem elegit utilitzar l’Snort perquè és un sistema àmpliament utilitzat per IDS/IPS. Es pot utilitzar en equips amb recursos moderats sense necessitat de comprometre el rendiment, compta amb un extensa base de dades de signatures que permet detectar ràpidament amenaces conegudes on facilita una protecció efectiva de la xarxa. A part d’això també té una facilitat per configurar-lo i es pot integrar amb eines com pfSense, SIEM i sistemes de monitorització.

Instal·lació i Configuració Bàsica

Primer hem preparat el nostre entorn de Linux per fer ús del Snort, hem instal·lat totes les **dependències necessàries per poder compilar i instal·lar Snort.**

**Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.**

Després hem descarregat l’ultima versió del Snort des de la web oficial i la descomprimim en el mateix directori.

**Texto

El contenido generado por IA puede ser incorrecto.**

**Texto

El contenido generado por IA puede ser incorrecto.**

Un cop hem descarregat el Snort hem executat la comanda make install per començar la instal·lacció.

**Texto

El contenido generado por IA puede ser incorrecto.**

Per poder compilar Snort amb suport per scripts Lua, vam haver d’instal·lar les biblioteques LuaJIT, que permeten afegir funcionalitats avançades a través de scripts.

**Texto

El contenido generado por IA puede ser incorrecto.**

Després d’instal·lar les dependències, vam accedir a la carpeta de Snort descomprimit i vam executar el script de configuració.

**Texto

El contenido generado por IA puede ser incorrecto.**

Un cop configurat correctament Snort, vam procedir a compilar-lo i instal·lar-lo al sistema.

**Texto

El contenido generado por IA puede ser incorrecto.**

**Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.**

Abans de poder executar Snort amb la nostra pròpia configuració i regles, vam haver de crear manualment els directoris i fitxers que aquest necessita per funcionar correctament.

**Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.**

Hem definit les variables de xarxa per indicar quina subxarxa 10.0.2.X vol protegir dins de snort.conf.

**Texto

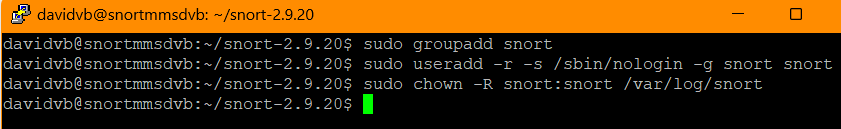
El contenido generado por IA puede ser incorrecto.**

Després hem configurat el directori on esguardaran els logs de Snort.

**Texto

El contenido generado por IA puede ser incorrecto.**

Per millorar la seguretat del sistema vam decidir executar Snort amb un usuari específic i limitat.

****

Definició de Polítiques de Seguretat

En el nostre Snort hem creat les següents regles:

**Ping ICMP:** Detecta qualsevol petició ICMP de tipus ping.

**Connexió SSH específica:** Detecta intents de connexió al port 22 d'una màquina concreta.

**Escaneig de ports amb Nmap:** Aquesta regla identifica patrons de tràfic amb molts paquets SYN en pocs segons.

**Peticions HTTP GET:** Detecta peticions HTTP GET cap a un servidor web.

**Força bruta a SSH:** Detecta quan una mateixa IP fa més de 5 intents de connexió per SSH en 10 segons.

Texto

El contenido generado por IA puede ser incorrecto.

Vam instal·lar **Postfix** i **mailutils**, eines bàsiques per enviar correus des del sistema.

Texto

El contenido generado por IA puede ser incorrecto.

Durant la instal·lació, vam escollir l’opció Internet Site i vam definir el nom del sistema com a ubuntumin.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Després vam configurar l’enviament mitjançant **Gmail com a servidor SMTP** editant /etc/postfix/main.cf.

Texto

El contenido generado por IA puede ser incorrecto.

Vam crear el fitxer /etc/postfix/sasl\_passwd amb el següent contingut.

Texto

El contenido generado por IA puede ser incorrecto.

Vam crear un script snort\_alert\_mailer.sh on **comprova si hi ha alertes noves**, les envia per correu i esborra el fitxer per començar net.

Texto

El contenido generado por IA puede ser incorrecto.

Finalment, vam afegir el script al crontab de root perquè s’executés automàticament cada 5 minuts.

Texto

El contenido generado por IA puede ser incorrecto.

Verificació de l’enviament d’alertes per correu

Un cop vam configurar el sistema de notificació per correu mitjançant Postfix i vam programar l’execució periòdica de l’script snort\_alert\_mailer.sh.

Texto

El contenido generado por IA puede ser incorrecto.

Després vam revisar els logs on apareixen les diferents alertes de ping.

Imagen de la pantalla de un computador

El contenido generado por IA puede ser incorrecto.

Després d’uns segons, vam accedir al correu de destí i vam comprovar que havíem rebut un email amb l’assumpte **ALERTA SNORT**, enviat des de la pròpia màquina amb el contingut exacte del fitxer alerts.log.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

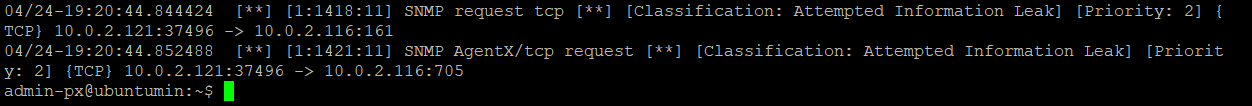
SIMULACIÓ D’ATACS I RESPOSTA

Un cop vam tenir Snort completament operatiu, vam realitzar una sèrie de proves i simulacions d’atacs reals per validar el bon funcionament del sistema i comprovar fins a quin punt era capaç de detectar accions sospitoses.

Aquest escaneig ràpid de ports va ser detectat per Snort com a Nmap Port Scan, tal com indicava l’alerta amb el sid:1000002 al fitxer de logs.

**Texto

El contenido generado por IA puede ser incorrecto.**



Vam haver de descomprimir la famosa llista de contrasenyes rockyou.txt.

**Texto

El contenido generado por IA puede ser incorrecto.**

SIMULACIÓ D’AUTENTICACIÓ

Amb tot preparat, vam executar la següent comanda per simular un atac d’autenticació contra el servei SSH de la màquina monitoritzada.

**Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.**

Mentre es produïa l’atac, vam obrir una consola a la màquina amb Snort per monitoritzar en directe el fitxer de registres.

**Pantalla de computadora con letras

El contenido generado por IA puede ser incorrecto.**

Amb això, vam deixar Snort monitoritzant tot el tràfic de la nostra xarxa interna, preparat per registrar qualsevol comportament sospitós.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Per automatitzar respostes, vam crear un script anomenat snort-blocker.sh, que analitza el fitxer de logs i bloqueja IPs sospitoses utilitzant iptables.

Texto

El contenido generado por IA puede ser incorrecto.

Snort va detectar l’atac i va escriure l’alerta corresponent. L’script snort-blocker.sh va llegir el log i, de forma automàtica, va bloquejar la IP atacant mitjançant una regla de iptables.

Texto

El contenido generado por IA puede ser incorrecto.

WEBGRAFIA

<https://unamiradaentrebytes.wordpress.com/2024/06/07/como-implementar-un-ids-en-linux-con-snort/>

<https://tolumichael.com/snort-vs-suricata-vs-zeek/>