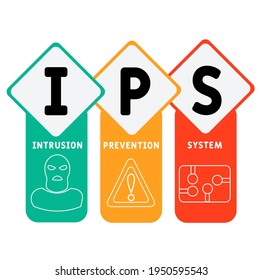
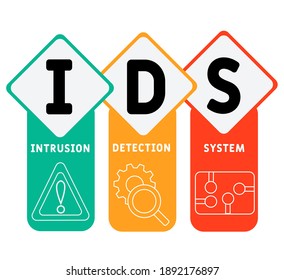
**ANEX 4**



**IMPLEMENTACIÓ D'UN SISTEMA DE DETECCIÓ I/O PREVENCIÓ D'INTRUSIONS**

Daniel Santiago Tabares Romero

JOAN POU



Contingut

[Introducció 2](#_Toc197615311)

[Teoria 2](#_Toc197615312)

[Definicion i funcions dels sistemes IDS/IPS 2](#_Toc197615313)

[Tipologies d'IDS/IPS 2](#_Toc197615314)

[Amenaces i vectors d' atac comuns 3](#_Toc197615315)

[Selecció de Tecnologia 3](#_Toc197615316)

[Comparació de solucions disponibles 3](#_Toc197615317)

[Anàlisi de requisits 4](#_Toc197615318)

[Justificació de la tecnologia escollida 4](#_Toc197615319)

[Instal·lació i Configuració Inicial 5](#_Toc197615320)

[Instal·lació de Snort 5](#_Toc197615321)

[Configuració de Snort 6](#_Toc197615322)

[Simulació d'Atacs des de Kali Linux 10](#_Toc197615323)

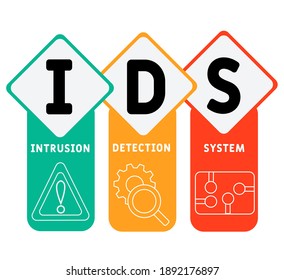
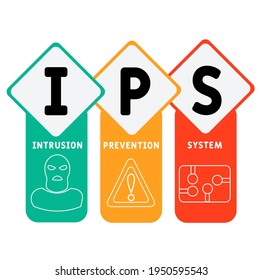
[Millores a fer 15](#_Toc197615324)

[Anàlisi de Logs i Avaluació dels Resultats 16](#_Toc197615325)

[Conclusions i Valoració 17](#_Toc197615326)

# Introducció

En aquest projecte, m'he proposat analitzar, seleccionar i implementar un sistema de detecció i prevenció d'intrusions (IDS/IPS) amb l'objectiu de millorar la seguretat de la xarxa. La importància d' aquests sistemes rau en la seva capacitat per identificar i mitigar amenaces en temps real, protegint els sistemes contra atacs malintencionats. Al llarg del desenvolupament d' aquest treball, s' abordaran conceptes teòrics, anàlisi de tecnologies disponibles i una implementació pràctica.



# Teoria

## Definicion i funcions dels sistemes IDS/IPS

Els(IDS/IPS) són eines en la ciberseguretat, dissenyades per monitorar el trànsit de xarxa a la recerca d'activitats sospitoses. Un IDS identifica possibles amenaces i genera alertes, mentre que un IPS, bloqueja activament les amenaces detectades. Aquests sistemes funcionen mitjançant l' analisi de patrons de trànsit, firmes d' atacs coneguts i anomalies a la xarxa, contribuint a la protecció contra accessos no autoritzats i atacs informatics.

## Tipologies d'IDS/IPS

Existeixen diversos IDS/IPS en funció del seu mètode de detecció i la seva ubicació a la xarxa:

* **Basats en firma**: Detecten amenaces comparant el trànsit amb una base de dades de patrons coneguts d'atacs.
* **Basats en anomalies**: Utilitzen models de comportament normal per identificar desviacions sospitoses.
* **IDS/IPS de xarxa (NIDS/NIPS)**: Supervisen i protegeixen segments de xarxa complets.
* **IDS/IPS basats en host (HIDS/HIPS)**: Monitoren l'activitat de sistemes individuals per detectar comportaments anòmals.

Cadascuna d' aquestes té aplicacions específiques segons l' entorn i les necessitats de seguretat.

## Amenaces i vectors d' atac comuns

Durant la implementació d'un IDS/IPS, he tingut en compte les amenaces més freqüents en entorns de xarxa, com ara:

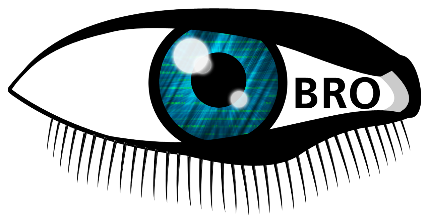
* **Escanejos de ports**: Eines com Nmap permeten als atacants identificar serveis vulnerables en una xarxa.
* **Atacs de denegació de servei (DoS/DDoS)**: Sobrecarreguen servidors amb trànsit maliciós per interrompre el seu funcionament.
* **Injecció de codi (SQL Injection, XSS)**: Exploten vulnerabilitats en aplicacions web per obtenir accés no autoritzat a dades.
* **Atacs de força bruta**: Intents repetitius d' accés a comptes mitjançant combinacions de contrasenyes.

Aquests atacs representen un risc significatiu per a la seguretat dels sistemes, per la qual cosa la implementació d'un IDS/IPS és fonamental per a la seva detecció i mitigació.

# Selecció de Tecnologia

## Comparació de solucions disponibles

Abans de seleccionar una tecnologia específica per a la implementació de l'IDS/IPS, he dut a terme una anàlisi comparativa entre les solucions més populars:



|  |  |  |  |
| --- | --- | --- | --- |
| Tecnologia | Tipus | Avantatges | Desavantatges |
| Snort | IDS/IPS basat en signatura i anomalies | Codi obert, altament configurable, gran comunitat de suport | Requereix configuració avançada |
| Suricata | IDS/IPS basat en signatura i flux de xarxa | Alt rendiment, suport multifil, anàlisi en profunditat | Major consum de recursos |
| Zeek (Bro) | IDS basat en comportament i anàlisi de trànsit | Anàlisi detallada, potent per a forense de xarxa | Menor capacitat de resposta activa |
| Wazuh | HIDS amb funcions de monitoratge | Integració amb SIEM, detecció en host | Dependència de configuració centralitzada |

Després d'analitzar aquestes solucions, he decidit optar per **Snort**, a causa de la seva flexibilitat, la seva capacitat de detecció en temps real i la possibilitat d'integrar-lo amb eines d'anàlisi de logs.

## Anàlisi de requisits

Per a la implementació de Snort, he definit els requisits següents:

* **Maquinari i programari:** Un servidor amb Ubuntu Server amb almenys 4 GB de RAM i 2 CPU
* **Xarxa:** Connexió a una xarxa simulada on es generaran atacs i trànsit
* **Compatibilitat:** Integració amb eines com Kibana i Logstash per a visualització de logs
* **Facilitat de configuració:** Ús de regles personalitzades per a detecció i resposta

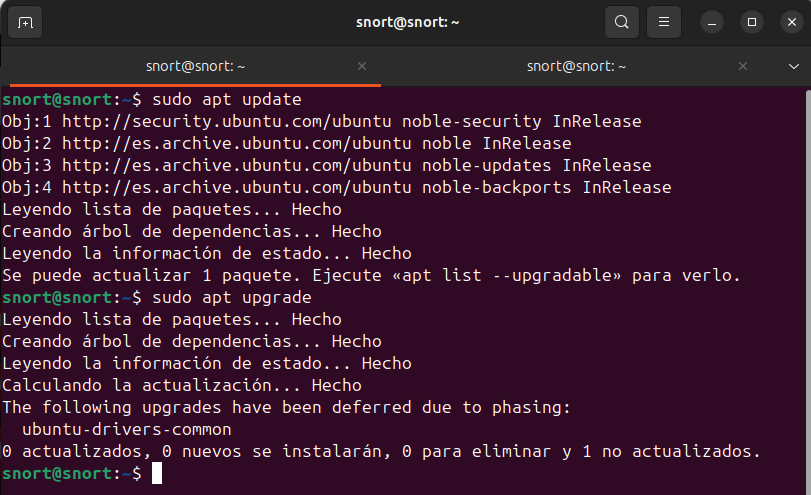
## Justificació de la tecnologia escollida

He triat **Snort** perquè compleix amb els requisits definits, ofereix una detecció eficaç d'amenaces i permet una configuració adaptada a diferents escenaris de seguretat i la seva integració amb eines de monitoratge facilita l'anàlisi d'esdeveniments i resposta davant incidents. Aquesta decisió em permetrà demostrar a la pràctica la detecció i mitigació d'amenaces en una xarxa simulada.

# Instal·lació i Configuració Inicial

## Instal·lació de Snort

Per començar amb la implementació de l'IDS, actualitzo el sistema operatiu i poso un entorn grafic al meu servidor de linux per fer més amigable la instal·lació de snort i quan hàgim de fer-lo servir.



Després, instal·la les dependències necessàries per a la compilació de Snort

sudo apt install -y build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev

Descarregueu l'última versió de Snort des del seu lloc web oficial i procediu a descomprimir-la:

wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz

tar -xvzf snort-2.9.20.tar.gz

cd snort-2.9.20

Compilé e instalé Snort executando:

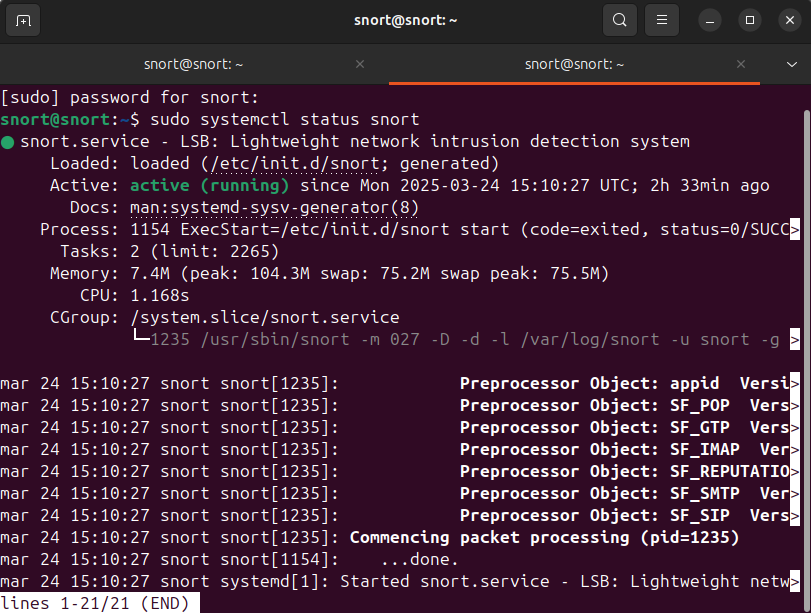
./configure --enable-sourcefire

make

sudo make install

Per verificar que la instal·lació va ser exitosa, comprovo la versió instal·lada:

snort -V



## Configuració de Snort

Després de la instal·lació, creieu els directoris necessaris per a la configuració i emmagatzematge de registres:

sudo mkdir -p /etc/snort/rules

sudo mkdir -p /var/log/snort

sudo touch /etc/snort/rules/local.rules

sudo touch /etc/snort/snort.conf

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat amb IA no sigui correcte.

Asseguré els permisos adequats per a l' usuari de Snort:

sudo groupadd snort

sudo useradd -r -s /sbin/nologin -g snort snort

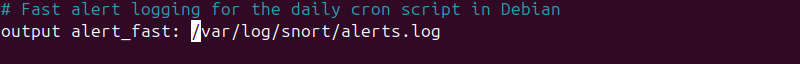
sudo chown -R snort:snort /var/log/snort

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat amb IA no sigui correcte.

Modifiqués l'arxiu de configuració /etc/snort/snort.conf per definir la ruta de les regles i els registres d'alertes:

output alert\_fast: /var/log/snort/alerts.log



Agregueu una regla bàsica en /etc/snort/rules/local.rules per detectar pings ICMP:

Imatge que conté text, captura de pantalla, programari, Font

Pot ser que el contingut generat amb IA no sigui correcte.

sudo snort -T -c /etc/snort/snort.conf

Imatge que conté text, captura de pantalla, Font

Pot ser que el contingut generat amb IA no sigui correcte.

Finalment, prova Snort en mode detecció:

sudo snort -c /etc/snort/snort.conf -A console

Imatge que conté text, captura de pantalla

Pot ser que el contingut generat amb IA no sigui correcte.

A baix i utilitzat més paràmetres per veure en temps real totes les alertes

## Simulació d'Atacs des de Kali Linux

**Per comprovar el correcte funcionament de les regles creades a Snort, vaig utilitzar una màquina Kali Linux connectada a la mateixa xarxa que l'IDS. Des de Kali, vaig generar diferents tipus de tràfic per activar les regles configurades al fitxer local.rules.**

**-Ping (ICMP) – Regla 1**

**Vaig executar un ping simple des de Kali al servidor amb Snort per activar la regla de detecció de paquets ICMP:**

**ping -c 3 192.168.1.100**

**Imatge que conté text, programari, Software de multimèdia, Programari de gràfics

Pot ser que el contingut generat amb IA no sigui correcte.**

**-Escaneig SYN amb Nmap – Regla 2**

**Vaig simular un escaneig de ports utilitzant Nmap amb l'objectiu de generar una alerta per escaneig SYN:**

**sudo nmap -sS 192.168.1.100**

**Imatge que conté captura de pantalla, text, Software de multimèdia, electrònica

Pot ser que el contingut generat amb IA no sigui correcte.**

**-Sol·licitud HTTP – Regla 3**

**Per a aquesta prova, primer vaig iniciar un servidor HTTP simple a la màquina amb Snort per obrir el port 80:**

**sudo python3 -m http.server 80**

**Després, des de Kali, vaig fer una sol·licitud HTTP amb curl:**

**curl http://192.168.1.100**

**Imatge que conté text, captura de pantalla, programari, Software de multimèdia

Pot ser que el contingut generat amb IA no sigui correcte.**

**-Connexió SSH – Regla 4**

**Per activar aquesta regla, simplement vaig intentar connectar-me via SSH al servidor amb Snort:**

**ssh 192.168.1.100**

**Imatge que conté text, captura de pantalla, programari, Software de multimèdia

Pot ser que el contingut generat amb IA no sigui correcte.**

**-Petició DNS a TikTok – Regla 0**

**Finalment, vaig provar la detecció d'una consulta DNS específica a tiktok.com com a exemple de tràfic potencialment restringit:**

**dig tiktok.com**

**Imatge que conté text, captura de pantalla, Software de multimèdia, programari

Pot ser que el contingut generat amb IA no sigui correcte.**

# Millores a fer

**Per qüestions de temps i abast de l'entorn, no vaig poder realitzar algunes simulacions addicionals que tenia planejades. Tanmateix, considero que usar aquestes proves permetria ampliar l'anàlisi del sistema IDS:**

**- Atac de força bruta amb Hydra sobre SSH**

**- Atac d'injecció SQL amb SQLmap en una aplicació web vulnerable**

**- Simulació d'atac DDoS amb hping3**

**- Integració amb eines de resposta automatitzada com Fail2Ban**

**A més aquest projecte el faré servir com a base per a una part complementària de cpd on l'utilitzaré perquè el cpd tingui més seguretat davant de diferents atacs com ddos entre d'altres i així fer el meu suposat cpd més segur**

# Anàlisi de Logs i Avaluació dels Resultats

**Després de realitzar cada atac, vaig revisar el fitxer de registres de Snort ubicat a /var/log/snort/alert analice los logs generats i vaig ajustar les regles si era necessari per evitar falsos positius i que la majoria funcions perque tenia diversos errors.**

# Conclusions i Valoració

**Aquest projecte m'ha permès reforçar els coneixements sobre la detecció d'intrusions. Tot i no haver provat tots els vectors, les regles implementades van detectar correctament els atacs realitzats des de Kali.**