



EDUCACIÓN



TECNOLÓGICO
NACIONAL DE MÉXICO

**TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DETLAXIACO**

VIRTUALIZACION

Nombre de los Integrantes de equipo:

Fernanda Ruiz Heras	21620151
Ana Michel león león	21620112
Rosa Salazar Doroteo	18620216
Rufino Mendoza Vásquez	21620198

Actividad:

Proyecto final : Sistema de Detección de Intrusos

Docente:

Ing. Edwuar Osorio Salinas

Carrera:

Ingeniería en Sistemas Computacionales

Grupo: 7US

Semestre: Séptimo.

INTRODUCCIÓN

Este proyecto se adentra en el complejo y crucial campo de los Sistemas de Detección de Intrusos (IDS), explorando su diseño, implementación y aplicación en el contexto de la creciente amenaza cibernética. Más allá de una simple alerta de intrusión, este proyecto busca desarrollar un IDS capaz de analizar, clasificar y responder a una amplia gama de amenazas, ofreciendo una capa de seguridad proactiva y adaptable.

El panorama de la seguridad informática actual se caracteriza por la sofisticación y la constante evolución de las técnicas de ataque. Los intrusos utilizan métodos cada vez más elaborados para eludir las defensas tradicionales, requiriendo soluciones de seguridad igualmente avanzadas. Los IDS, lejos de ser una solución única, se presentan como un componente fundamental de una estrategia de seguridad multicapa, trabajando en conjunto con firewalls, sistemas de prevención de intrusiones (IPS) y otras herramientas de seguridad para crear una defensa robusta.

Este proyecto se diferencia por su enfoque multifacético, abarcando desde los fundamentos teóricos de la detección de intrusiones hasta la implementación práctica de un sistema funcional. Exploraremos diferentes paradigmas de detección, incluyendo:

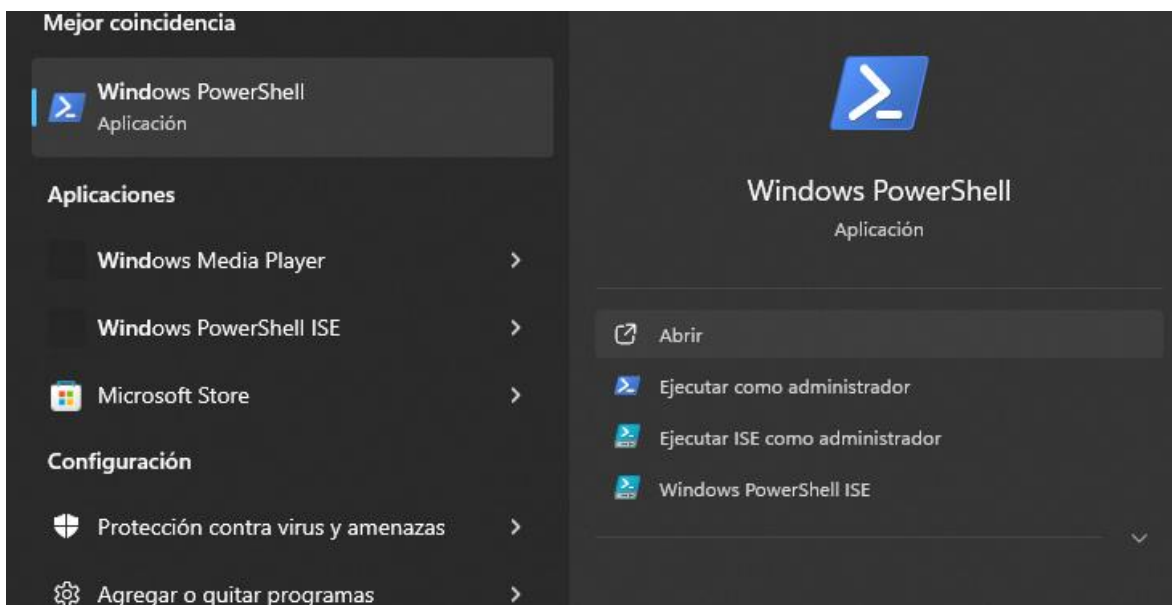
- **Detección basada en firmas:** Esta técnica se basa en la identificación de patrones conocidos de ataques, comparando el tráfico de red o la actividad del sistema con una base de datos de firmas de malware. Analizaremos las ventajas y desventajas de este enfoque, incluyendo su dependencia de la actualización constante de la base de datos y su ineficacia contra ataques desconocidos (zero-day).
- **Detección basada en anomalías:** A diferencia de la detección basada en firmas, este método se centra en la identificación de desviaciones del

comportamiento normal del sistema o la red. Utilizaremos algoritmos de aprendizaje automático para construir modelos que representen el comportamiento normal y detecten cualquier desviación significativa. Exploraremos diferentes algoritmos de aprendizaje automático, evaluando su rendimiento y eficiencia en la detección de anomalías.

- **Detección híbrida:** Reconociendo las fortalezas y debilidades de cada enfoque, exploraremos la posibilidad de combinar la detección basada en firmas y la basada en anomalías para crear un sistema híbrido que aproveche las ventajas de ambos métodos. Este enfoque busca mejorar la precisión y la cobertura de la detección, minimizando las falsas alarmas.

La implementación del IDS incluirá el desarrollo de un sistema modular y escalable, capaz de adaptarse a diferentes entornos y necesidades. Se considerarán aspectos como la eficiencia del procesamiento de datos, la gestión de alarmas y la integración con otros sistemas de seguridad. El proyecto culminará con una evaluación exhaustiva del sistema, incluyendo pruebas de rendimiento, análisis de precisión y una discusión sobre las limitaciones y las posibles mejoras futuras. La documentación incluirá un análisis detallado de los resultados, ofreciendo una visión completa del proceso de diseño, implementación y evaluación del IDS. Además, se explorarán las implicaciones éticas y legales relacionadas con la recopilación y el análisis de datos de tráfico de red.

Paso 1: Principalmente abrimos el **Windows PowerShell** para empezar a configurar lo que es Ubuntu, abrimos como administrador para no tener conflictos en el proceso



Paso 2: Ejecutamos el comando para instalar una distribución de Linux llamada **Ubuntu** “**Wsl --install**” dentro del entorno de Windows.

wsl: Hace referencia a Windows Subsystem for Linux, la característica que permite ejecutar distribuciones de Linux en Windows.

```
root@AnaLeon: ~
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

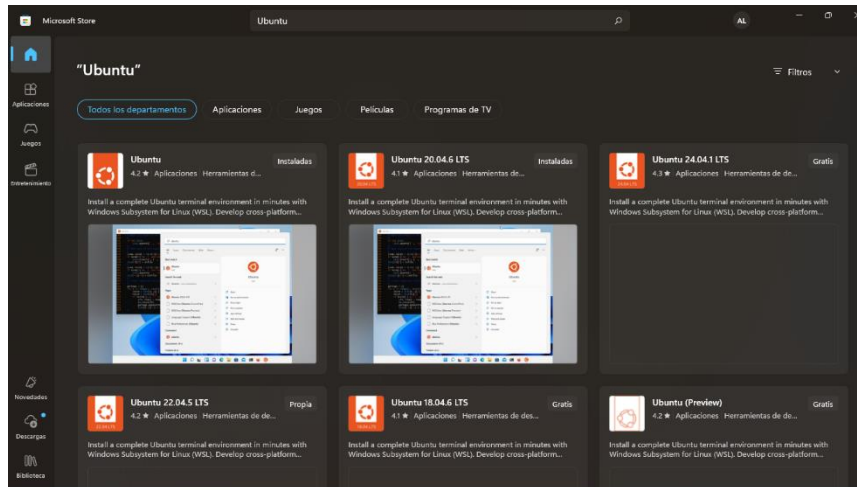
Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\WINDOWS\system32> wsl --install
Ubuntu ya está instalado.
Iniciando Ubuntu...
root@AnaLeon:~#
```

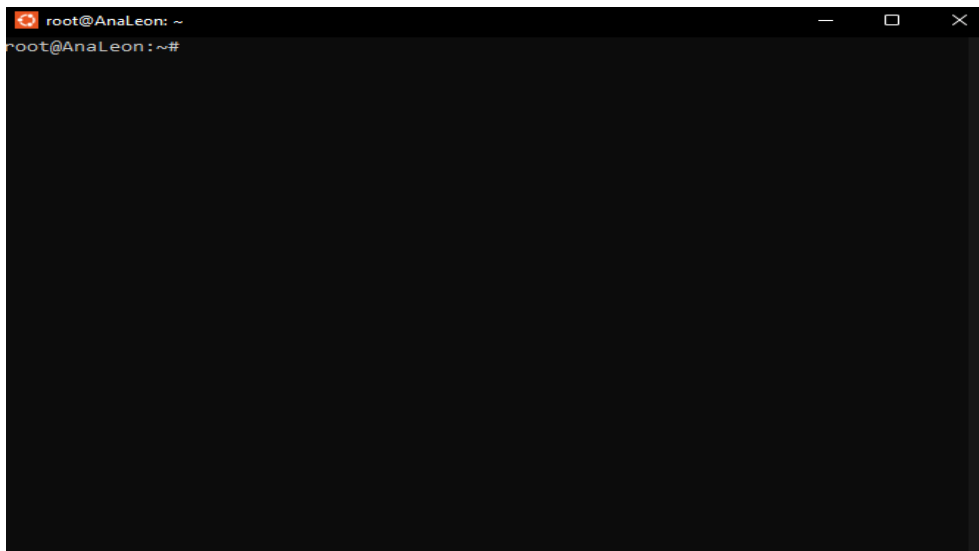
- **wsl --update:** Este comando se utiliza para verificar si hay actualizaciones disponibles para el **Subsistema de Windows para Linux (WSL)** y, si las hay, las instalara.

```
PS C:\WINDOWS\system32> wsl --update
Comprobando actualizaciones.
La versión más reciente de Subsistema de Windows para Linux ya está instalada.
PS C:\WINDOWS\system32>
```

Paso 3: Se muestra la integración entre los sistemas operativos Windows y Linux. Ofrece la posibilidad de instalar distribuciones de Linux como Ubuntu directamente desde el Microsoft Store



- **root@AnaLeon:~**: Esta parte del prompt indica el directorio de trabajo actual. "root" sugiere que se está ejecutando con privilegios de administrador y "AnaLeon"



- Se está ejecutando el comando para actualizar la lista de paquetes (apt update) y luego actualapt upgrade -y).

sudo apt update && sudo apt upgrade -y

```
root@AnaLeon: ~  
root@AnaLeon:~# sudo apt update && sudo apt upgrade -y  
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]  
Hit:2 https://dl.yarnpkg.com/debian stable InRelease  
Hit:3 http://archive.ubuntu.com/ubuntu noble InRelease  
Get:4 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
0% [4 InRelease 37.5 kB/126 kB 30%] [1 InRelease 75.3 kB/126 kB 60%]
```

- De igual manera se están instalando herramientas esenciales de compilación y bibliotecas de desarrollo para redes, expresiones regulares y compresión de datos, junto con sus dependencias. Con el siguiente comando
- sudo apt install -y build-essential libpcap-dev libpcr3-dev zlib1g-dev**

```
root@AnaLeon: ~  
root@AnaLeon:~# sudo apt install -y build-essential libpcap-dev libpcr3-dev zlib1g-dev  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
build-essential is already the newest version (12.10ubuntu1).  
The following additional packages will be installed:  
  libverbs-providers libdbus-1-dev libibverbs-dev libibverbs1 libnl-3-200  
  libnl-3-dev libnl-route-3-200 libnl-route-3-dev libpcap0.8-dev libpcap0.8t64  
  libpcr16-3 libpcr3 libpcr32-3 libpcrcpp0v5  
The following NEW packages will be installed:  
  libverbs-providers libdbus-1-dev libibverbs-dev libibverbs1 libnl-3-200  
  libnl-3-dev libnl-route-3-200 libnl-route-3-dev libpcap-dev libpcap0.8-dev  
  libpcap0.8t64 libpcr16-3 libpcr3 libpcr3-dev libpcr32-3 libpcrcpp0v5  
  zlib1g-dev  
0 upgraded, 17 newly installed, 0 to remove and 0 not upgraded.  
Need to get 4356 kB of archives.  
After this operation, 14.5 MB of additional disk space will be used.  
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 libnl-3-200 amd64 3.7.0-0.  
3build1 [55.6 kB]  
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libnl-route-3-200 amd64 3.  
7.0-0.3build1 [189 kB]  
3% [2 libnl-route-3-200 18.4 kB/189 kB 10%]
```

- Se está descargando el archivo fuente de **Snort** desde su sitio oficial para posteriormente descomprimirlo, compilarlo e instalarlo en el sistema.
- **wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz**

```
root@AnaLeon: ~# wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz
root@AnaLeon: ~# cd snort-2.9.20
root@AnaLeon: snort-2.9.20# ./configure
root@AnaLeon: snort-2.9.20# make
root@AnaLeon: snort-2.9.20# sudo make install--2024-12-10 23:58:32-- https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz
Resolving www.snort.org (www.snort.org)... 104.19.221.12, 2606:4700::6813:de0c, 2606:4700::6813:dd0c
Connecting to www.snort.org (www.snort.org)|104.19.221.12|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/687/original/snort-2.9.20.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMWOXGB2W5%2F20241211%2Fus-east-1%2Ffs3%2Faws4_request&X-Amz-Date=20241211T055833Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=c81989d93b78ecb3e86d0ed398a826090543b564635f0f1afd974e3d3c733477 [following]
--2024-12-10 23:58:34-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/687/original/snort-2.9.20.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMWOXGB2W5%2F20241211%2Fus-east-1%2Ffs3%2Faws4_request&X-Amz-Date=20241211T055833Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=c81989d93b78ecb3e86d0ed398a826090543b564635f0f1afd974e3d3c733477
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.217.199.105, 52.216.218.97, 3.5.2.135, ...
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.217.199.105|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7009894 (6.7M) [binary/octet-stream]
Saving to: 'snort-2.9.20.tar.gz'

snort-2.9.20.tar.gz  6%[>] 474.64K  44.6KB/s  eta 2m 30s
```

- **snort -V**
- Este comando verifica la versión instalada de **Snort** . La salida confirma que se ha instalado correctamente la versión **2.9.20 GRE (Build 82)** , junto con información sobre las bibliotecas utilizadas, como **libpcap** , **PCRE** y **ZLIB** .

```
root@AnaLeon: ~# snort -V

-*> Snort! <*-
o" )~
'-'

Version 2.9.20 GRE (Build 82) x86_64
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved

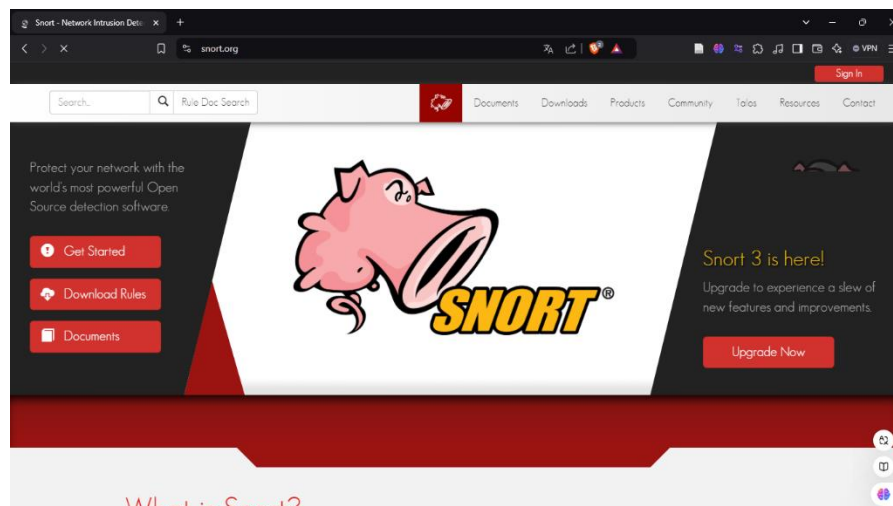
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

root@AnaLeon: ~#
```

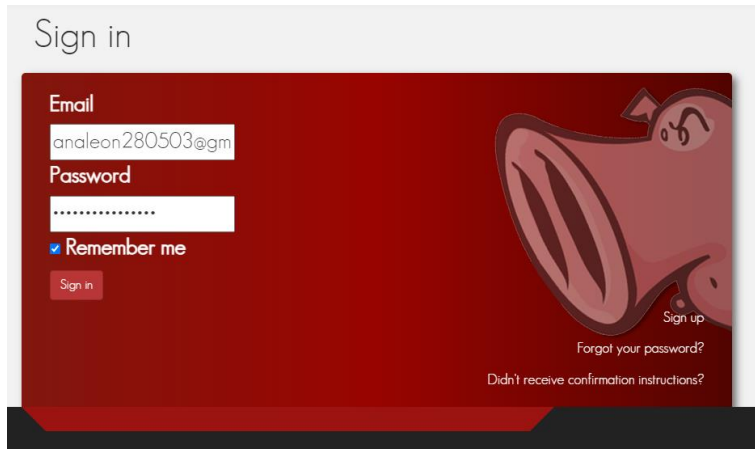
- Se verificarán los directorios necesarios para **Snort** (/etc/snort, /etc/snort/rules, /var/log/snort), que ya existen. Luego, se listan sus contenidos, incluidos archivos de configuración (snort.conf, classification.config) y reglas (attack-responses.rules, backdoor.rules), confirmando que la estructura está preparada para su uso.

```
root@AnaLeon:~# sudo mkdir /etc/snort
mkdir: cannot create directory '/etc/snort': File exists
root@AnaLeon:~# sudo mkdir /etc/snort/rules
mkdir: cannot create directory '/etc/snort/rules': File exists
root@AnaLeon:~# sudo mkdir /var/log/snort
mkdir: cannot create directory '/var/log/snort': File exists
root@AnaLeon:~# ls -l /etc/snort
total 360
-rw-r--r-- 1 root root 1281 Apr 20 2022 attribute_table.dtd
-rw-r--r-- 1 root root 3757 Apr 20 2022 classification.config
-rw-r--r-- 1 root root 82469 Apr 19 2024 community-sid-msg.map
-rw-r--r-- 1 root root 23654 Apr 20 2022 file_magic.conf
-rw-r--r-- 1 root root 33339 Apr 20 2022 gen-msg.map
-rw-r--r-- 1 root root 687 Apr 20 2022 reference.config
drwxr-xr-x 2 root root 4096 Dec 11 01:35 rules
-rw-r--r-- 1 root snort 29773 Apr 19 2024 snort.conf
-rw-r--r-- 1 root root 812 Dec 11 01:35 snort.debian.conf
-rw-r--r-- 1 root root 2335 Apr 20 2022 threshold.conf
-rw-r--r-- 1 root root 160606 Apr 20 2022 unicode.map
root@AnaLeon:~# ls -l /etc/snort/rules
total 1600
-rw-r--r-- 1 root root 5520 Apr 19 2024 attack-responses.rules
-rw-r--r-- 1 root root 17898 Apr 19 2024 backdoor.rules
-rw-r--r-- 1 root root 3862 Apr 19 2024 bad-traffic.rules
```

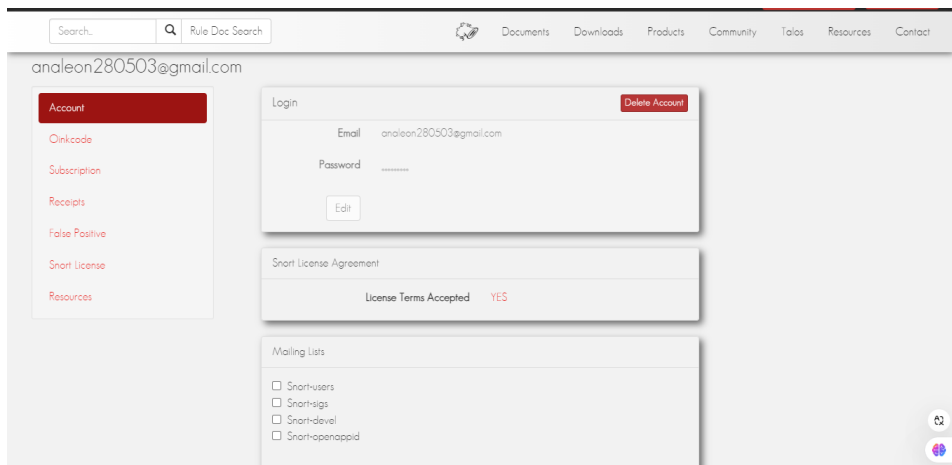
Paso4 : Una vez descargado accedemos a el Short es una herramienta de seguridad de red poderosa y flexible que puede ayudar a proteger tu red de una amplia variedad de amenazas.



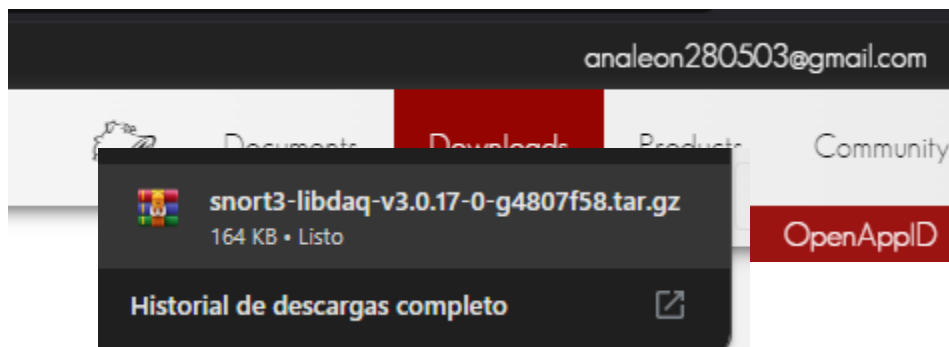
Paso 5: Iniciamos sesión en nuestra aplicación Snort para poder configurar y empezar con nuestro sistema de detección de intrusos



- Se muestra un panel de control personal de un usuario de Snort, un sistema de detección de intrusiones de código abierto. Este panel proporciona al usuario una interfaz para gestionar la cuenta y configuración relacionada con Snort.



Comenzamos con la descarga



Paso 6 : Al ejecutar el comando `tar -xzf snort3-libdaq-v3.0.17-0-g4807f58.tar.gz`, se ha extraído el contenido de la librería libdaq para Snort en el directorio actual. Estos archivos son necesarios para compilar y utilizar la librería en un proyecto de Snort.

```
root@AnaLeon:~# tar -xzf snort3-libdaq-v3.0.17-0-g4807f58.tar.gz
snort3-libdaq-4807f58/
snort3-libdaq-4807f58/.gitignore
snort3-libdaq-4807f58/COPYING
snort3-libdaq-4807f58/ChangeLog-2.x
snort3-libdaq-4807f58/LICENSE
snort3-libdaq-4807f58/Makefile.am
snort3-libdaq-4807f58/README.md
snort3-libdaq-4807f58/api/
snort3-libdaq-4807f58/api/Makefile.am
snort3-libdaq-4807f58/api/daq.h
snort3-libdaq-4807f58/api/daq_api_internal.h
snort3-libdaq-4807f58/api/daq_base.c
snort3-libdaq-4807f58/api/daq_base_api.c
snort3-libdaq-4807f58/api/daq_common.h
snort3-libdaq-4807f58/api/daq_config.c
snort3-libdaq-4807f58/api/daq_dlt.h
snort3-libdaq-4807f58/api/daq_instance_api_defaults.c
snort3-libdaq-4807f58/api/daq_instance_api_defaults.h
snort3-libdaq-4807f58/api/daq_mod_ops.c
snort3-libdaq-4807f58/api/daq_module_api.h
snort3-libdaq-4807f58/api/daq_version.h.in
snort3-libdaq-4807f58/bootstrap
snort3-libdaq-4807f58/configure.ac
snort3-libdaq-4807f58/example/
snort3-libdaq-4807f58/example/Makefile.am
snort3-libdaq-4807f58/example/daqtest.c
snort3-libdaq-4807f58/example/decode.h
snort3-libdaq-4807f58/example/netinet_compat.h
```

- Al ejecutar este comando, el usuario ha cambiado el directorio de trabajo actual al directorio `snort3-libdaq-v3.0.17-0-g4807f58`.

```
root@AnaLeon:~# cd snort3-libdaq-v3.0.17-0-g4807f58
root@AnaLeon:~/snort3-libdaq-v3.0.17-0-g4807f58#
```

- Los comandos `./configure` y `sudo make install` son pasos esenciales para construir software a partir de su código fuente.

```
root@AnaLeon:~/snort3-libdaq-v3.0.17-0-g4807f58/snort3-libdaq-4807f58# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a race-free mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
```

- Al intentar configurar la librería **libdaq** para Snort, se ha encontrado un problema al ejecutar el comando `./configure`.

```
root@AnaLeon:~/snort3-libdaq-v3.0.17-0-g4807f58/snort3-libdaq-4807f58# ./configure
--with-dnet=/ruta/a/libdnet
configure: WARNING: unrecognized options: --with-dnet
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a race-free mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
```

- El comando `sudo make install` está ejecutando el proceso de instalación de la librería **libdaq** en tu sistema.

```
root@AnaLeon:~/snort3-libdaq-v3.0.17-0-g4807f58/snort3-libdaq-4807f58# sudo make install
Making install in api
make[1]: Entering directory '/root/snort3-libdaq-v3.0.17-0-g4807f58/snort3-libdaq-4807f58/api'
make[2]: Entering directory '/root/snort3-libdaq-v3.0.17-0-g4807f58/snort3-libdaq-4807f58/api'
/usr/bin/mkdir -p '/usr/local/lib'
/bin/bash ../libtool --mode=install /usr/bin/install -c libdaq.la '/usr/local/lib'
libtool: install: /usr/bin/install -c .libs/libdaq.so.3.0.0 /usr/local/lib/libdaq.so.3.0.0
libtool: install: (cd /usr/local/lib && { ln -s -f libdaq.so.3.0.0 libdaq.so.3 || { rm -f libdaq.so.3 && ln -s libdaq.so.3.0.0 libdaq.so.3; }; })
libtool: install: (cd /usr/local/lib && { ln -s -f libdaq.so.3.0.0 libdaq.so || { rm -f libdaq.so && ln -s libdaq.so.3.0.0 libdaq.so; }; })
libtool: install: /usr/bin/install -c .libs/libdaq.lai /usr/local/lib/libdaq.la
```

- operativo sea consciente de la nueva biblioteca y pueda utilizarla correctamente en cualquier programa que la requiera.

```
root@AnaLeon:~/snort3-libdaq-v3.0.17-0-g4807f58/snort3-libdaq-4807f58# ldconfig
root@AnaLeon:~/snort3-libdaq-v3.0.17-0-g4807f58/snort3-libdaq-4807f58#
```

- La salida muestra que Snort se está iniciando correctamente y está listo para comenzar a monitorear el tráfico de red en la interfaz eth0 de acuerdo con las reglas definidas en el archivo de configuración.

```
root@Analeon:~# sudo snort -i eth0 -c /etc/snort/snort.conf -A console
Running in IDS mode

---- Initializing Snort ----
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 230
1 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8
000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888
8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414
1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 751
0 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8
300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002
55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsengine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
Finished loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrule
s
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor
/...
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//li
bsf_pop_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//li
```

- la salida de Snort indica que el sistema está funcionando correctamente y está preparado para proteger nuestra red.

```
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Reload thread starting...
Reload thread started, thread 0x7f285ecea6c0 (58936)
Decoding Ethernet

---- Initialization Complete ----

o''~
...~

-*> Snort! <*-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_POP Version 1.0 <Build 1>

Commencing packet processing (pid=58932)
```

- Ejecutamos el comando **sudo apt install nmap**

```
root@AnaLeon:~# sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 6452 kB of archives.
After this operation, 28.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libblas3 amd64 3.12
.0-3build1.1 [238 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3.0+
dfsg-5build1 [42.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3bu
ild2 [166 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.0-4
.1build2 [120 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 nmap-common all 7.94+gi
t20230807.3be01efb1+dfsg-3build2 [4192 kB]
40% [5 nmap-common 1557 kB/4192 kB 37%] 80.6 kB/s 53s_
```

- **Escaneo 1: sudo nmap -ss 192.168.0.116**
- **Objetivo:** Escaneo de los puertos TCP de la máquina con dirección IP 192.168.0.116.
- **Resultados:**
 - **Host activo:** La máquina está encendida y respondiendo a las solicitudes de conexión.
 - **Puertos abiertos:** Se detectaron varios puertos abiertos, lo que indica que están escuchando servicios:
 - **135/tcp (msrpc):** Este puerto se utiliza comúnmente para el servicio de llamada a procedimiento remoto (RPC) de Microsoft.
 - **139/tcp (netbios-ssn):** Este puerto es utilizado por el protocolo NetBIOS Session Service, que se emplea para la compartición de archivos y la impresión en redes Windows.
 - **445/tcp (microsoft-ds):** Este puerto está asociado al servicio de directorio activo de Microsoft.
 - **808/tcp (ccproxy-http):** Este puerto sugiere que podría estar corriendo un proxy HTTP, como CCProxy.
 - **2179/tcp (vmrpd):** Este puerto se utiliza para el protocolo de escritorio remoto de Virtual Machine, lo que indica que podría

haber una máquina virtual configurada para conexiones remotas.

- **9001/tcp (tor-orport):** Este puerto indica que podría estar corriendo un nodo de la red Tor, que se utiliza para anonimizar el tráfico de internet.
- **Escaneo 2: sudo nmap -p- 192.168.0.116**
- **Objetivo:** Escaneo de todos los puertos TCP de la misma máquina.
- **Resultados:**
 - **Confirmación de puertos abiertos:** Los puertos abiertos detectados en el primer escaneo fueron confirmados en este segundo escaneo más exhaustivo.
 - **Puertos cerrados:** Se indica que la mayoría de los puertos están cerrados, lo que es normal en cualquier sistema operativo.
- **Interpretación de los Resultados**
- Los resultados de los escaneos sugieren que la máquina en la dirección IP 192.168.0.116 está corriendo un sistema operativo Windows y tiene varios servicios habilitados

```
root@AnaLeon:~# sudo nmap -sS 192.168.0.116
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 09:23 CST
Nmap scan report for AnaLeon (192.168.0.116)
Host is up (0.0012s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
808/tcp   open  ccproxy-http
2179/tcp  open  vmrpd
9001/tcp  open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
root@AnaLeon:~# sudo nmap -p- 192.168.0.116
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 09:24 CST
Nmap scan report for AnaLeon (192.168.0.116)
Host is up (0.00055s latency).
Not shown: 65520 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
808/tcp   open  ccproxy-http
```


- El registro de actividad de red muestra múltiples ataques y exploraciones con prioridad 2: escaneos ICMP (NMAP), intentos de explotación SNMP (incluyendo AgentX y trampas), un ataque DDoS, y escaneos de puertos TCP (XMAS).

```
Commencing packet processing (pid=58932)
12/11-09:23:57.456323  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempte
d Information Leak] [Priority: 2] {ICMP} 172.26.47.247 -> 192.168.0.116
12/11-09:23:57.616818  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classificatio
n: Attempted Information Leak] [Priority: 2] {TCP} 172.26.47.247:38445 -> 192.168.0
.116:705
12/11-09:23:57.632441  [**] [1:1418:11] SNMP request tcp [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 172.26.47.247:38445 -> 192.168.0.116:16
1
12/11-09:24:09.496633  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempte
d Information Leak] [Priority: 2] {ICMP} 172.26.47.247 -> 192.168.0.116
12/11-09:24:14.196909  [**] [1:1418:11] SNMP request tcp [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 172.26.47.247:55192 -> 192.168.0.116:16
1
12/11-09:24:14.219897  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempt
ed Information Leak] [Priority: 2] {TCP} 172.26.47.247:55192 -> 192.168.0.116:162
12/11-09:24:15.159330  [**] [1:249:8] DDOS mstream client to handler [**] [Classifi
cation: Attempted Denial of Service] [Priority: 2] {TCP} 172.26.47.247:55192 -> 192
.168.0.116:15104
12/11-09:24:18.253337  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classificatio
n: Attempted Information Leak] [Priority: 2] {TCP} 172.26.47.247:55192 -> 192.168.0
.116:705
12/11-09:24:25.796741  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempte
d Information Leak] [Priority: 2] {ICMP} 172.26.47.247 -> 192.168.0.116
12/11-09:24:25.992884  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classificatio
n: Attempted Information Leak] [Priority: 2] {TCP} 172.26.47.247:42136 -> 192.168.0
.116:705
12/11-09:24:26.007156  [**] [1:1418:11] SNMP request tcp [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 172.26.47.247:42136 -> 192.168.0.116:16
1
12/11-09:24:49.862810  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempt
ed Information Leak] [Priority: 2] {TCP} 172.26.47.247:43528 -> 192.168.0.116:1
12/11-09:24:51.642911  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempt
ed Information Leak] [Priority: 2] {TCP} 172.26.47.247:43528 -> 192.168.0.116:1
12/11-09:24:53.420931  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempt
ed Information Leak] [Priority: 2] {TCP} 172.26.47.247:43528 -> 192.168.0.116:1
12/11-09:24:56.712757  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempt
ed Information Leak] [Priority: 2] {TCP} 172.26.47.247:43528 -> 192.168.0.116:1
12/11-09:24:58.486581  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempt
ed Information Leak] [Priority: 2] {TCP} 172.26.47.247:43528 -> 192.168.0.116:1
```

- Se está instalando el paquete suricata usando apt. El sistema está listando las dependencias que se instalarán, incluyendo varias bibliotecas (libevent, libhyperscan, etc.), y mostrando el progreso de la descarga de estos paquetes.

```
root@Analeon:~# sudo apt install -y suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  isa-support libevent-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1
  libhiredis1.1.0 libhttp2 libhyperscan5 libmaxminddb0 libnet1 libnetfilter-log1
  libnuma1 librtt-bus-pci24 librtt-bus-vdev24 librtt-eal24 librtt-ethdev24
  librtt-hash24 librtt-ip-frag24 librtt-kvargs24 librtt-log24 librtt-mbuf24
  librtt-mempool24 librtt-meter24 librtt-net-bond24 librtt-net24 librtt-pci24
  librtt-rcu24 librtt-ring24 librtt-sched24 librtt-telemetry24 libxdp1
  sse3-support suricata-update
Suggested packages:
  mmdb-bin libtcmalloc-minimal4
The following NEW packages will be installed:
  isa-support libevent-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1
  libhiredis1.1.0 libhttp2 libhyperscan5 libmaxminddb0 libnet1 libnetfilter-log1
  libnuma1 librtt-bus-pci24 librtt-bus-vdev24 librtt-eal24 librtt-ethdev24
  librtt-hash24 librtt-ip-frag24 librtt-kvargs24 librtt-log24 librtt-mbuf24
  librtt-mempool24 librtt-meter24 librtt-net-bond24 librtt-net24 librtt-pci24
  librtt-rcu24 librtt-ring24 librtt-sched24 librtt-telemetry24 libxdp1
  sse3-support suricata suricata-update
0 upgraded, 33 newly installed, 0 to remove and 0 not upgraded.
Need to get 7050 kB of archives.
After this operation, 30.4 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 isa-support amd64 21bui
ld1 [16.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/universe amd64 sse3-support amd64 21bu
ild1 [3406 B]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libevent-2.1-7t64 amd64 2.1
.12-stable-9ubuntu2 [145 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 libevent-pthreads-2.1-7t64
amd64 2.1.12-stable-9ubuntu2 [7982 B]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 libhiredis1.1.0 amd64 1
.2.0-6ubuntu3 [41.4 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble/universe amd64 libhttp2 amd64 1:0.5.46-
1ubuntu2 [71.0 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble/universe amd64 libhyperscan5 amd64 5.4
.2-2 [2827 kB]
8% [7 libhyperscan5 101 kB/2827 kB 4%] 51.2 kB/s 2min 10s_
```

Paso 7: Esta configuración se centra en la configuración de captura de paquetes. Específicamente, detalla las opciones de registro (nombre de archivo, formato, tipo) y la configuración de captura de alta velocidad utilizando la interfaz AF_PACKET de Linux. La configuración incluye opciones para diferentes métodos de agrupación (cluster_flow, cluster_cpu, cluster_qm, cluster_ebpf), explicando cómo cada uno distribuye los paquetes entre los núcleos de la CPU para un procesamiento eficiente. El modo recomendado es cluster_flow. La configuración también menciona que cluster_roller ha quedado obsoleto.


```
enabled: yes
level: info
filename: suricata.log
# format: "[%i - %m] %z %d: %S: %M"
# type: json
- syslog:
  enabled: no
  facility: local5
  format: "[%i] <%d> -- "
  # type: json

*
* Step 3: Configure common capture settings
*
* See "Advanced Capture Options" below for more options, including Netmap
* and PF_RING.
*

Linux high speed capture support
-packet:
- interface: eth0
  threads: auto
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per h>
  # This is only supported for Linux kernel > 3.1
  # possible value are:
  # * cluster_flow: all packets of a given flow are sent to the same socket
  # * cluster_cpu: all packets treated in kernel by a CPU are sent to the same >
  # * cluster_qm: all packets linked by network card to a RSS queue are sent to >
  # socket. Requires at least Linux 3.14.
  # * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardwar>
  # more info.
  # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_>
  # with capture card using RSS (requires cpu affinity tuning and system IRQ tun>
  # cluster_rollover has been deprecated; if used, it'll be replaced with cluste>
  cluster-type: cluster_flow
  # In some fragmentation cases, the hash can not be computed. If "defrag" is set

Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
Exit      ^R Read File  ^\ Replace   ^U Paste      ^J Justify    ^_ Go To Line
```

- Se muestra la salida con el comando `sudo suricata-update`. El sistema informa que está usando el directorio de datos `/var/lib/suricata`, la configuración de Suricata en `/etc/suricata/suricata.yaml` y las reglas en `/etc/suricata/rules`.

```
root@AnaLeon:~# sudo suricata-update
11/12/2024 -- 09:42:20 - <Info> -- Using data-directory /var/lib/suricata.
11/12/2024 -- 09:42:20 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
11/12/2024 -- 09:42:20 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
11/12/2024 -- 09:42:20 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suricata.
11/12/2024 -- 09:42:20 - <Info> -- Loading /etc/suricata/suricata.yaml
11/12/2024 -- 09:42:20 - <Error> -- Failed to parse configuration file at line 615: mapping values are not allowed in this context
root@AnaLeon:~# _
```

- Se proporciona el comando `suricata -c suricata.yaml -s signatures.rules -i eth0`. Este comando inicia Suricata utilizando el archivo de configuración `suricata.yaml`, el archivo de firmas `signatures.rules` y monitoreando la interfaz de red `eth0`.

```
To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:

suricata -c suricata.yaml -s signatures.rules -i eth0

root@AnaLeon:~# /var/log/suricata/fast_log
```

- Se muestra la salida de un escaneo Nmap. Se escaneó el host `172.26.47.247` en los puertos `1-1000` usando un escaneo stealth (`-sS`). El resultado indica que el host está activo, pero todos los 1000 puertos escaneados están en estados ignorados, lo que significa que no respondieron a las solicitudes de escaneo. También se indica que no se muestran 1000 puertos TCP cerrados (reset).

```
root@AnaLeon:~# nmap -sS -p 1-1000 172.26.47.247
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 12:19 CST
Nmap scan report for 172.26.47.247
Host is up (0.0000090s latency).
All 1000 scanned ports on 172.26.47.247 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
root@AnaLeon:~# _
```

- El sistema respondió con un mensaje de error indicando que no se encontró el comando sqlmap. Luego, sugiere dos maneras de instalarlo: usando snap install sqlmap o apt install sqlmap. Se mencionan las versiones 1.7.tar y 1.7.12-1 como versiones disponibles

```
root@AnaLeon:~# sqlmap -u "http://172.26.47.247/vulnerable.php?id=1" --dump
Command 'sqlmap' not found, but can be installed with:
snap install sqlmap # version 1.7.tar, or
apt install sqlmap # version 1.7.12-1
See 'snap info sqlmap' for additional versions.
root@AnaLeon:~#
```

Paso 8: Finalmente se muestra la salida de una prueba de inyección SQL usando la herramienta sqlmap contra la URL "<http://172.26.47.247/vulnerable.php?id=1>". La herramienta está realizando varias pruebas para detectar vulnerabilidades de inyección SQL, incluyendo comprobaciones de inyección SQL ciega basada en booleanos usando cláusulas WHERE o HAVING con diferentes variaciones

```
root@AnaLeon:~# sqlmap -u "http://172.26.47.247/vulnerable.php?id=1" --dump --level 5 --risk=3

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:16:22 /2024-12-11/

[17:16:23] [INFO] testing connection to the target URL
[17:16:23] [INFO] testing if the target URL content is stable
[17:16:23] [INFO] target URL content is stable
[17:16:23] [INFO] testing if GET parameter 'id' is dynamic
[17:16:23] [WARNING] GET parameter 'id' does not appear to be dynamic
[17:16:23] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[17:16:23] [INFO] testing for SQL injection on GET parameter 'id'
[17:16:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:16:24] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[17:16:24] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[17:16:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[17:16:24] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[17:16:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[17:16:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[17:16:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[17:16:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[17:16:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[17:16:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[17:16:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[17:16:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
```

- Se muestra la salida del comando `tail -f`, monitoreando un archivo de registro de alertas de Snort (`/var/log/snort/snort.alert.fast`). El registro muestra una serie de entradas que indican la detección de múltiples intentos de descubrimiento de servicio UPnP, clasificados como exploraciones de red con una prioridad de 3

```
root@AnaLeon: ~  
root@AnaLeon:~# sudo tail -f /var/log/snort/snort.alert.fast  
12/11-17:07:39.005145  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:07:42.042508  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:07:45.045394  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:07:48.053976  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:15:21.966723  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:15:24.976002  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:15:27.982209  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:15:31.097863  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:15:34.100130  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900  
12/11-17:15:37.110072  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.26.32.1:56550 -> 239.255.255.250:1900
```

Resultados

Se logró configurar e implementar un Sistema de Detección de Intrusos (IDS) combinando herramientas como Snort y Suricata. Se llevaron a cabo pruebas de escaneo y simulaciones de ataques, detectando con éxito intentos de intrusión, como inyecciones SQL, ataques DDoS y escaneos de puertos. El sistema empleó enfoques basados en firmas y anomalías, mostrando eficiencia en la detección de amenazas. También se destacó su capacidad para integrarse con otros sistemas de seguridad y procesar grandes volúmenes de tráfico en tiempo real.

Conclusión

El IDS desarrollado se demostró ser una solución efectiva y escalable para enfrentar amenazas cibernéticas modernas. Su enfoque híbrido mejoró la precisión y redujo las falsas alarmas. Sin embargo, se identificaron desafíos, como la necesidad de actualizaciones constantes y la complejidad de configuración.