¿Qué es Suricata?

Web https://suricata.io/download/

- **Suricata** es un **IDS/IPS (Sistema de Detección/Prevención de Intrusos)** y motor de análisis de tráfico de red.
- Fue desarrollado por **OISF (Open Information Security Foundation)**.
- Sus principales funciones:
  - Inspeccionar tráfico en tiempo real.
  - Detectar amenazas en base a **firmas (rules)**.
  - Analizar protocolos (HTTP, DNS, TLS, FTP, SSH...).
  - Generar logs detallados y estadísticas.
  - Puede actuar en modo **IDS (solo detecta)** o **IPS (detecta y bloquea)**.
- Similar a **Snort**, pero más moderno y con soporte nativo de **multihilo**, lo que lo hace más rápido en redes grandes.

🔹 ¿Qué es Suricata con Machine Learning?

- Suricata normalmente se basa en **firmas** (reglas predefinidas) → detecta ataques conocidos.
- Con **Machine Learning**:
  - Se pueden detectar **anomalías en el tráfico** sin depender de reglas exactas.
  - Se usa para identificar **ataques "zero-day"** o comportamientos sospechosos.
  - Normalmente se integra con:
    - **ELK (Elasticsearch, Logstash, Kibana)** para recolectar y visualizar datos.
    - **ML frameworks (Scikit-learn, TensorFlow, PyTorch)** para entrenar modelos sobre los logs.
  - Ejemplo: detectar patrones anormales de uso de DNS, picos de tráfico inusuales, o intentos de exfiltración de datos.

🔹 Ejercicios sencillos de Suricata en Kali Linux para alumnos

📌 Supongamos que ya tienen Kali instalado.

1 Instalar Suricata

sudo apt update

sudo apt install suricata -y

Ver versión instalada:

suricata –build-info

https://docs.suricata.io/en/latest/quickstart.html

```
/var/www/html/DVWA/config master !250 ❯ sudo apt-get install software-properties-common
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  firmware-ti-connectivity librav1e0.7 linux-image-6.12.25-amd64 python3-click-plugins
  python3-zombie-imp
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  appstream packagekit packagekit-tools python3-lazr.restfulclient python3-lazr.uri
  python3-software-properties python3-wadllib
Suggested packages:
  apt-config-icons
The following NEW packages will be installed:
  appstream packagekit packagekit-tools python3-lazr.restfulclient python3-lazr.uri
  python3-software-properties python3-wadllib software-properties-common
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,435 kB of archives.
After this operation, 8,315 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

```
/var/www/html/DVWA/config master !250 ❯ suricata –build-info
Suricata 8.0.1 ("undefined")
USAGE: suricata [OPTIONS] [BPF FILTER]


  General:
        -v                                  : be more verbose (use multiple times to increa
ty)
        -c <path>                           : path to configuration file
        -l <dir>                            : default log directory
        --include <path>                    : additional configuration file
        --set name=value                    : set a configuration value
        --pidfile <file>                    : write pid to this file
        -T                                  : test configuration file (use with -c)
        --init-errors-fatal                 : enable fatal failure on signature init error
        -D                                  : run as daemon
        --user <user>                       : run suricata as this user after init
        --group <group>                     : run suricata as this group after init
        --unix-socket[=<file>]              : use unix socket to control suricata work
        --runmode <runmode_id>              : specific runmode modification the engine shou
he argument
                                              supplied should be the id for the runmode obt
unning
```

2 Ejecutar Suricata en modo IDS con interfaz de red

sudo suricata -i eth0

👉 Sustituir eth0 por la interfaz real (pueden verlas con ip a).

```
~/Documents/box ❯ sudo suricata -i eth0
i: suricata: This is Suricata version 8.0.1 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
W: detect: 1 rule files specified, but no rules were loaded!
i: mpm-hs: Rule group caching - loaded: 0 newly cached: 0 total cacheable: 0
i: threads: Threads created → W: 4 FM: 1 FR: 1   Engine started.
```

---

3 Ver los logs de tráfico

Suricata genera logs en:

cd /var/log/suricata/

ls

```
~/Documents/box ❯ cd /var/log/suricata/

/var/log/suricata ❯ ls
eve.json  fast.log  stats.log  suricata.log
```

Archivos clave:

- fast.log → alertas rápidas.
- eve.json → logs detallados en JSON.

---

4 Probar una regla sencilla (detectar ping)

1. Editar reglas locales:

sudo nano /etc/suricata/rules/local.rules

2. Añadir:

alert icmp any any -> any any (msg:"Ping detectado"; sid:1000001; rev:1;)

```
~/Documents/box ❯ cat /etc/suricata/rules/local.rules

alert icmp any any → any any (msg:"Ping detectado"; sid:1000001; rev:1;)
```

3. Probar la regla:

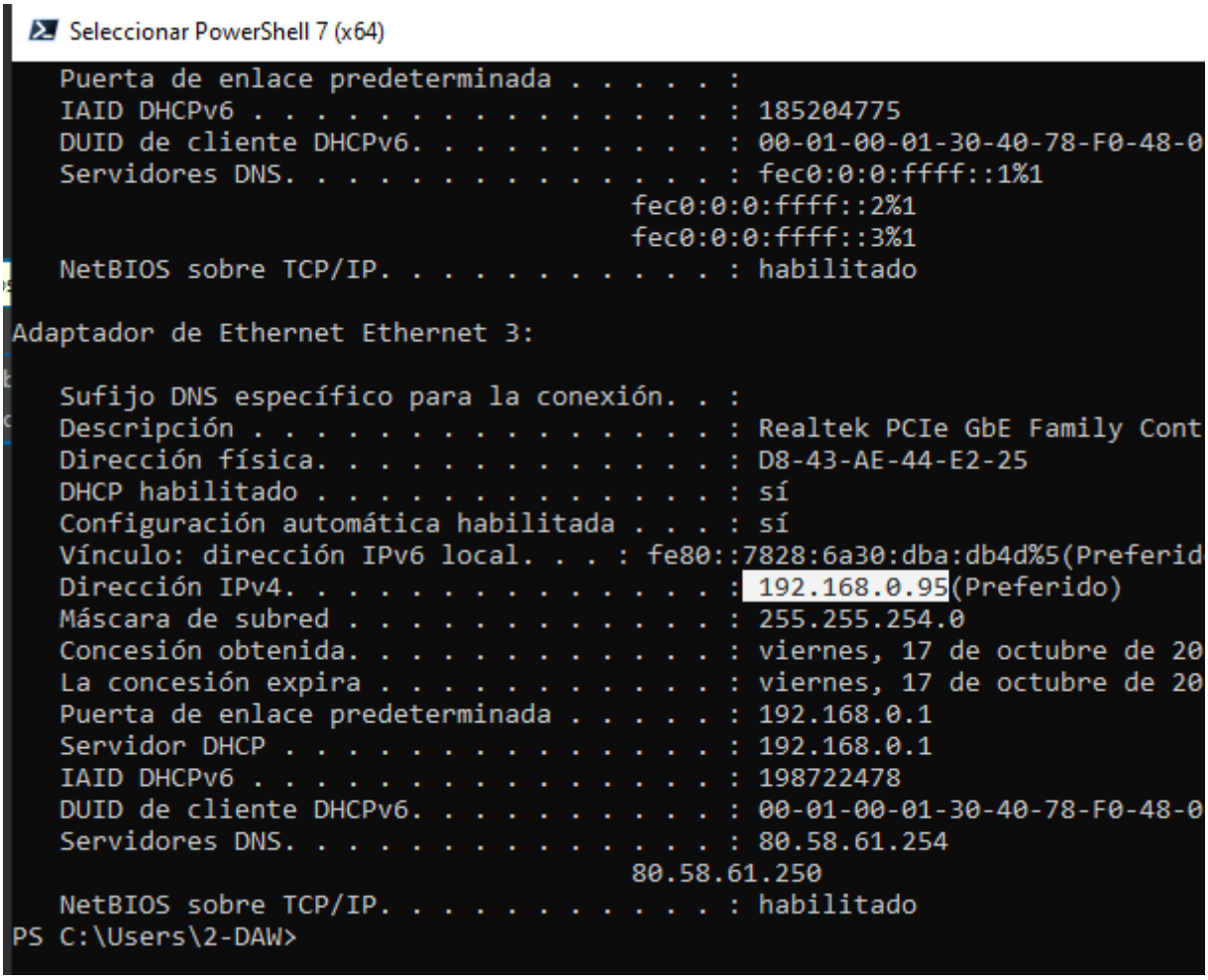
sudo suricata -i eth0 -S /etc/suricata/rules/local.rules

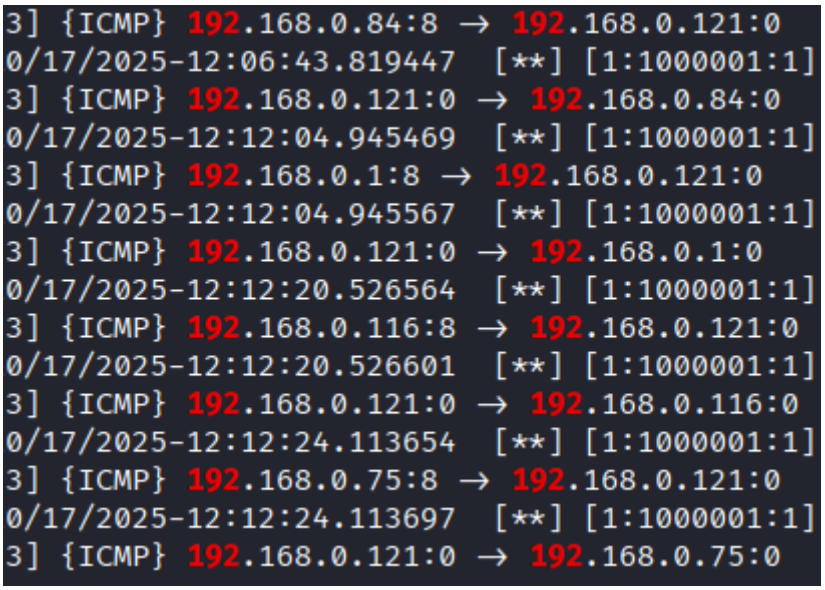
```
/var/log/suricata ❯ sudo suricata -i eth0 -S /etc/suricata/rules/local.rules
i: suricata: This is Suricata version 8.0.1 RELEASE running in SYSTEM mode
i: mpm-hs: Rule group caching - loaded: 0 newly cached: 0 total cacheable: 0
i: threads: Threads created → W: 4 FM: 1 FR: 1   Engine started.
```

4. Desde otra máquina, hacer un ping al Kali → debería registrarse en fast.log.

```
~/Documents/box ❯ cat /var/log/suricata/fast.log | head
10/17/2025-11:48:22.539235  [**] [1:1000001:1] Ping detectado [**] [Classification: (null)] [Priority:
 3] {IPv6-ICMP} fe80:0000:0000:0000:6036:0dff:fef4:4626:143 → ff02:0000:0000:0000:0000:0000:0000:0016
:0
10/17/2025-11:48:27.205193  [**] [1:1000001:1] Ping detectado [**] [Classification: (null)] [Priority:
 3] {IPv6-ICMP} fe80:0000:0000:0000:1fdc:1378:ee10:57b4:135 → ff02:0000:0000:0000:0000:0001:ffad:285e
:0
10/17/2025-11:48:37.113507  [**] [1:1000001:1] Ping detectado [**] [Classification: (null)] [Priority:
 3] {IPv6-ICMP} fe80:0000:0000:0000:0200:00ff:fe00:0000:133 → ff02:0000:0000:0000:0000:0000:0000:0002
:0
10/17/2025-11:48:46.795639  [**] [1:1000001:1] Ping detectado [**] [Classification: (null)] [Priority:
 3] {IPv6-ICMP} fe80:0000:0000:0000:3a1b:9eff:fea5:edd0:131 → ff02:0000:0000:0000:0000:0001:ffa5:edd0
:0
10/17/2025-11:48:46.860721  [**] [1:1000001:1] Ping detectado [**] [Classification: (null)] [Priority:
 3] {IPv6-ICMP} fe80:0000:0000:0000:3a1b:9eff:fea5:edd0:131 → ff02:0000:0000:0000:0000:0000:0000:00fb
:0
10/17/2025-11:48:47.309596  [**] [1:1000001:1] Ping detectado [**] [Classification: (null)] [Priority:
```

```
~/Documents/box ❯ cat /var/log/suricata/fast.log | g
10/17/2025-11:50:45.089506  [**] [1:1000001:1] Ping
 3] {ICMP} 192.168.0.95:8 → 192.168.0.121:0
10/17/2025-11:50:45.089571  [**] [1:1000001:1] Ping
 3] {ICMP} 192.168.0.121:0 → 192.168.0.95:0
10/17/2025-11:55:26.309192  [**] [1:1000001:1] Ping
 3] {IPv6-ICMP} fe80:0000:0000:0000:14b5:ab9c:d6e4:2
:0
10/17/2025-11:59:32.613496  [**] [1:1000001:1] Ping
 3] {ICMP} 192.168.0.121:8 → 192.168.0.107:0
10/17/2025-11:59:32.614258  [**] [1:1000001:1] Ping
```





5 Analizar un archivo pcap

Descargar un pcap de ejemplo:

wget https://www.malware-traffic-analysis.net/2020/08/31/2020-08-31-traffic-analysis-exercise.pcap.zip

unzip 2020-08-31-traffic-analysis-exercise.pcap.zip

Ejecutar Suricata:

sudo suricata -r 2020-08-31-traffic-analysis-exercise.pcap -l /tmp/suricata-test

Ver alertas:

cat /tmp/suricata-test/fast.log

---

6 Ejercicio final (para alumnos)

👉 **Reto en clase**:

- Crear **una regla personalizada** que detecte tráfico HTTP hacia example.com.
- Probar con:
- curl http://example.com
- Comprobar en fast.log que la alerta salta.

```
~/Downloads ❯ cat /var/log/suricata/fast.log | grep exam                    ✔ PIPE|0
10/17/2025-12:41:49.715588  [**] [1:1000002:1] SUSPICIOUS - TLS SNI example.com [**] [Classification:
Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.121:59016 → 23.192.228.80:443

~/Downloads ❯ cat /etc/suricata/rules/local.rules

alert icmp any any → any any (msg:"Ping detectado"; sid:1000001; rev:1;)

alert tls any any → any any (msg:"SUSPICIOUS - TLS SNI example.com"; \
tls.sni; content:"example.com"; nocase; \
classtype:bad-unknown; sid:1000002; rev:1;)
```

✅ Resumen para FP

- **Nivel básico**: instalación, ejecución, logs y reglas simples.
- **Nivel intermedio**: análisis de PCAPs y reglas personalizadas.
- **Nivel avanzado (explicación)**: integración con Machine Learning para detectar anomalías en tráfico.