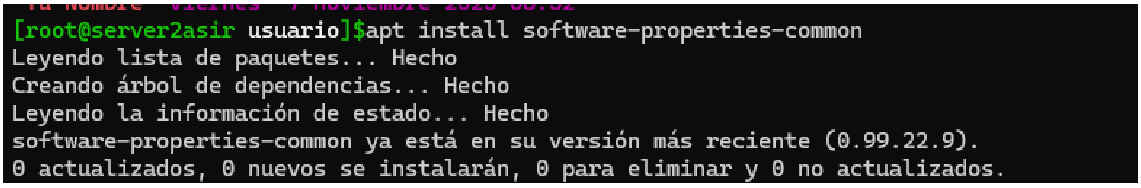
Suricata

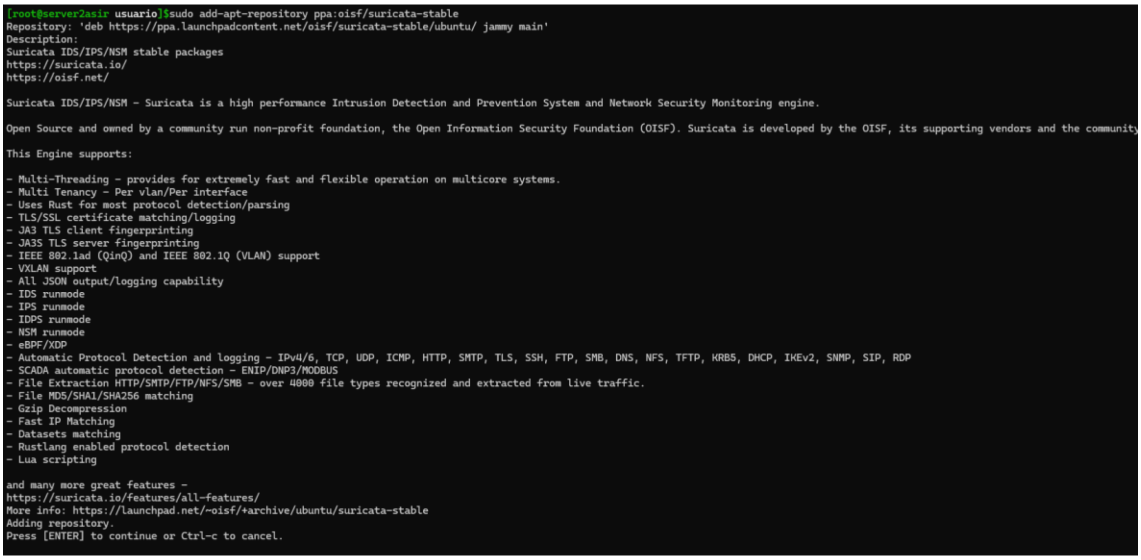
Instala Suricata

sudo apt install software-properties-common



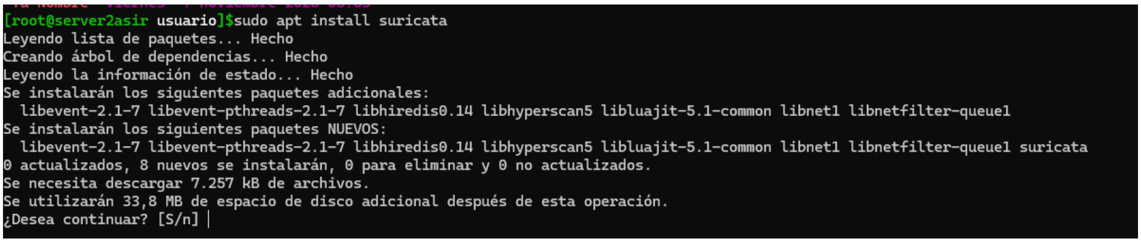
```
[root@server2asir usuario]$apt install software-properties-common
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
software-properties-common ya está en su versión más reciente (0.99.22.9).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

sudo add-apt-repository ppa:oisf/suricata-stable



```
[root@server2asir usuario]$sudo add-apt-repository ppa:oisf/suricata-stable
Repository: 'deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy main'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.

Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the community

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
- IDS runmode
- IPS runmode
- IDPS runmode
- NSM runmode
- eBPF/XDP
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRB5, DHCP, IKEv2, SNMP, SIP, RDP
- SCADA automatic protocol detection - ENIP/DNP3/MODBUS
- File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted from live traffic.
- File MD5/SHA1/SHA256 matching
- Gzip Decompression
- Fast IP Matching
- Datasets matching
- Rustlang enabled protocol detection
- Lua scripting

and many more great features -
https://suricata.io/features/all-features/
More info: https://launchpad.net/~oisf/+archive/ubuntu/suricata-stable
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
```

sudo apt install suricata

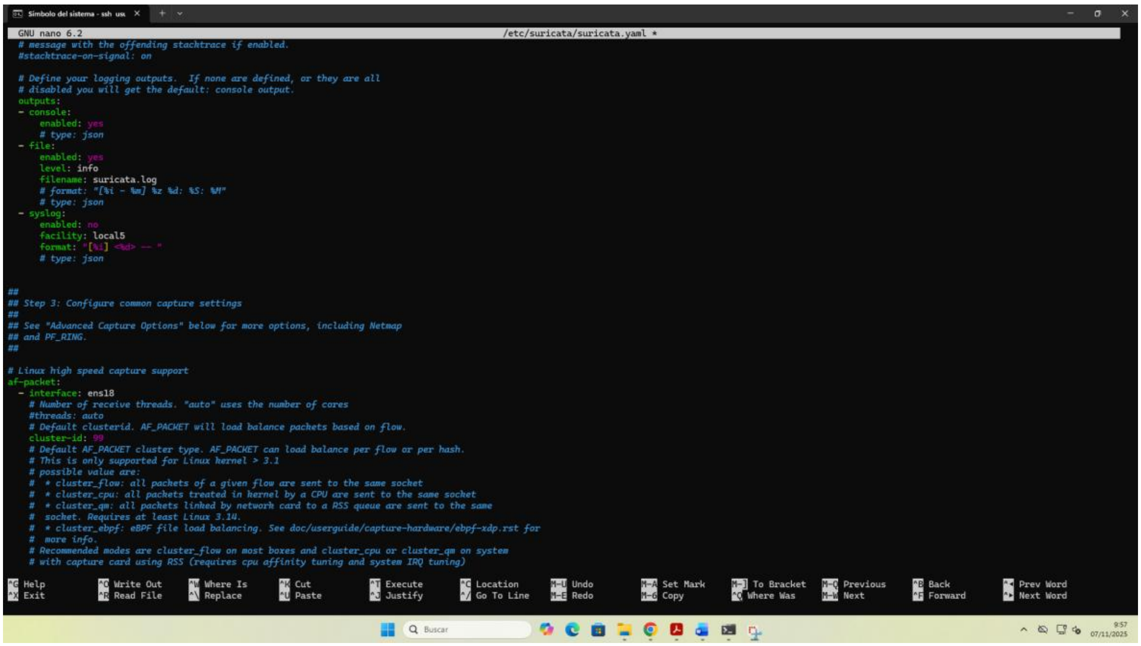


```
[root@server2asir usuario]$sudo apt install suricata
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libevent-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhyperscan5 libluajit-5.1-common libnet1 libnetfilter-queue1
Se instalarán los siguientes paquetes NUEVOS:
  libevent-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhyperscan5 libluajit-5.1-common libnet1 libnetfilter-queue1 suricata
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 7.257 kB de archivos.
Se utilizarán 33,8 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] |
```

Configurarlo

sudo nano /etc/suricata/suricata.yaml

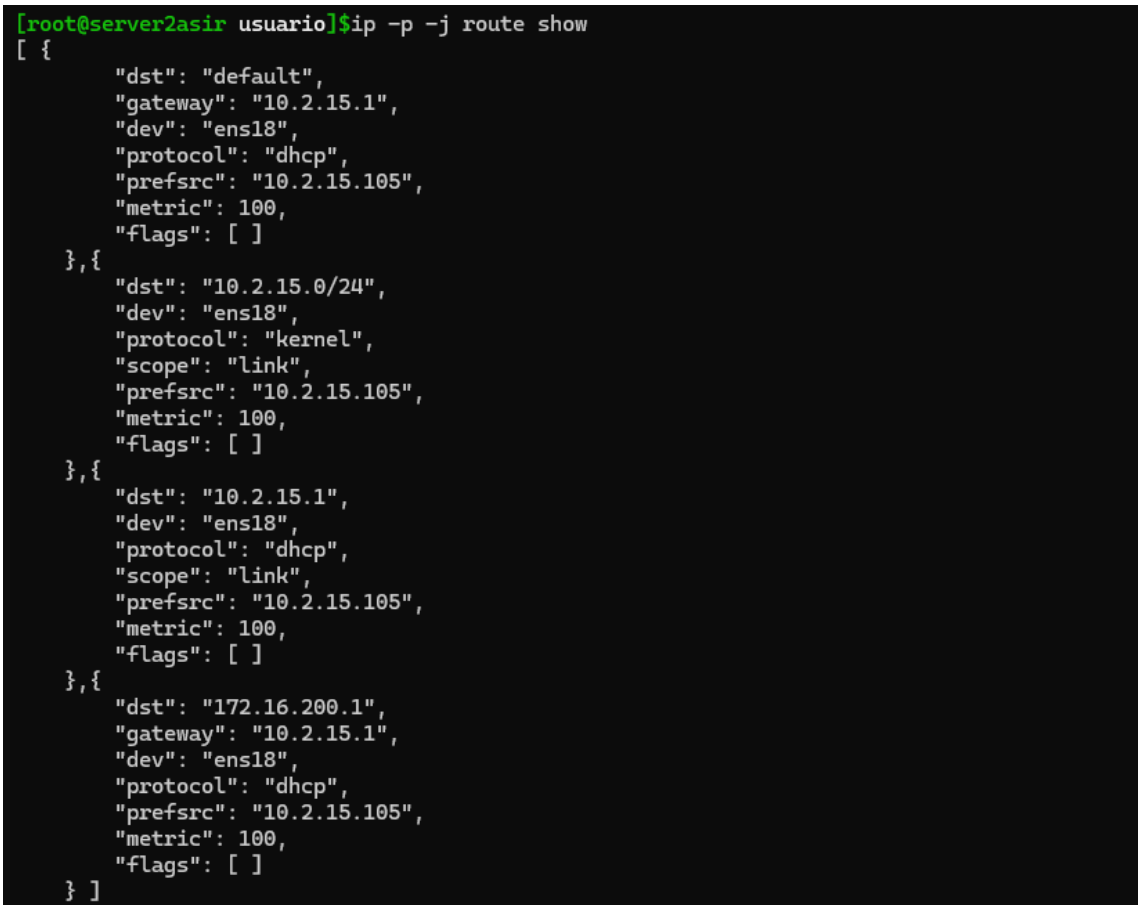
Habilita interfaces de red



```
  GNU nano 6.2                                   /etc/suricata/suricata.yaml *
  # message with the offending stacktrace if enabled.
  #stacktrace-on-signal: on

  # Define your logging outputs.  If none are defined, or they are all
  # disabled you will get the default: console output.
  outputs:
  - console:
      enabled: yes
      # type: json
  - file:
      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
af-packet:
  - interface: ens18
    # 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 hash.
    # 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 socket
    #  * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
    #  socket. Requires at least Linux 3.14.
    #  * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.rst for
    #  more info.
    # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
    # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)
```

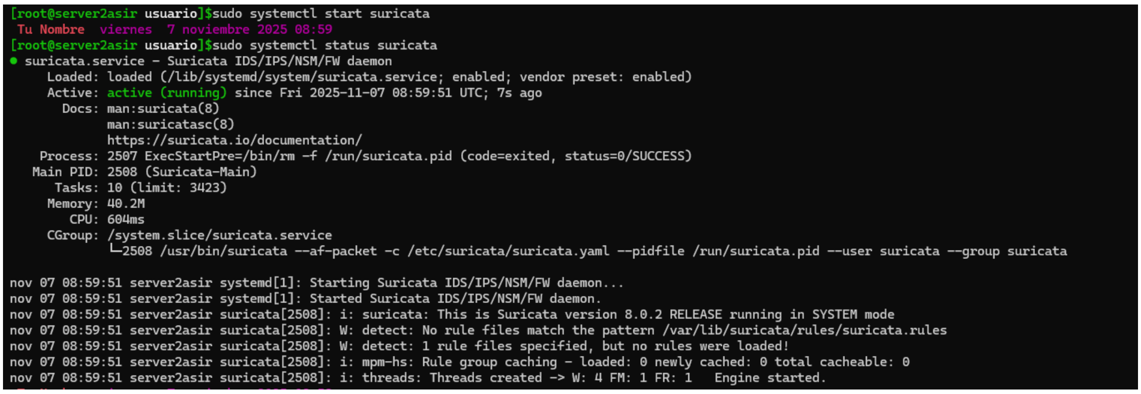
Se habilita nuestro interfaz para que supervise ese

este comando es para mostrar la interfaz por defecto y otra información de enrutamiento



```
[root@server2asir usuario]$ip -p -j route show
[ {
        "dst": "default",
        "gateway": "10.2.15.1",
        "dev": "ens18",
        "protocol": "dhcp",
        "prefsrc": "10.2.15.105",
        "metric": 100,
        "flags": [ ]
    },{
        "dst": "10.2.15.0/24",
        "dev": "ens18",
        "protocol": "kernel",
        "scope": "link",
        "prefsrc": "10.2.15.105",
        "metric": 100,
        "flags": [ ]
    },{
        "dst": "10.2.15.1",
        "dev": "ens18",
        "protocol": "dhcp",
        "scope": "link",
        "prefsrc": "10.2.15.105",
        "metric": 100,
        "flags": [ ]
    },{
        "dst": "172.16.200.1",
        "gateway": "10.2.15.1",
        "dev": "ens18",
        "protocol": "dhcp",
        "prefsrc": "10.2.15.105",
        "metric": 100,
        "flags": [ ]
    } ]
```

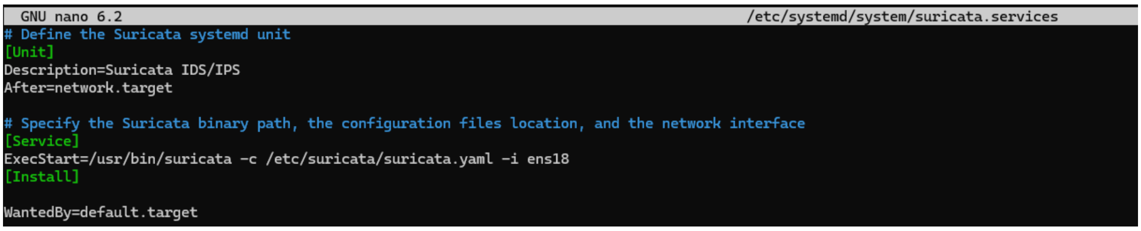
Inicia Suricata



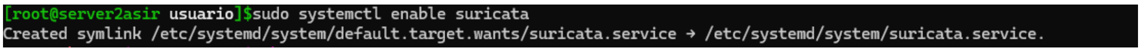
```
[root@server2asir usuario]$sudo systemctl start suricata
 Tu Nombre  viernes  7 noviembre 2025 08:59
[root@server2asir usuario]$sudo systemctl status suricata
● suricata.service - Suricata IDS/IPS/NSM/FW daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-11-07 08:59:51 UTC; 7s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 2507 ExecStartPre=/bin/rm -f /run/suricata.pid (code=exited, status=0/SUCCESS)
   Main PID: 2508 (Suricata-Main)
      Tasks: 10 (limit: 3423)
     Memory: 40.2M
        CPU: 604ms
     CGroup: /system.slice/suricata.service
             └─2508 /usr/bin/suricata --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid --user suricata --group suricata

nov 07 08:59:51 server2asir systemd[1]: Starting Suricata IDS/IPS/NSM/FW daemon...
nov 07 08:59:51 server2asir systemd[1]: Started Suricata IDS/IPS/NSM/FW daemon.
nov 07 08:59:51 server2asir suricata[2508]: i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
nov 07 08:59:51 server2asir suricata[2508]: W: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
nov 07 08:59:51 server2asir suricata[2508]: W: detect: 1 rule files specified, but no rules were loaded!
nov 07 08:59:51 server2asir suricata[2508]: i: mpm-hs: Rule group caching - loaded: 0 newly cached: 0 total cacheable: 0
nov 07 08:59:51 server2asir suricata[2508]: i: threads: Threads created -> W: 4 FM: 1 FR: 1   Engine started.
```

Luego le haremos un stop para automatizar el inicio de Suricata

sudo nano /etc/systemd/system/suricata.service

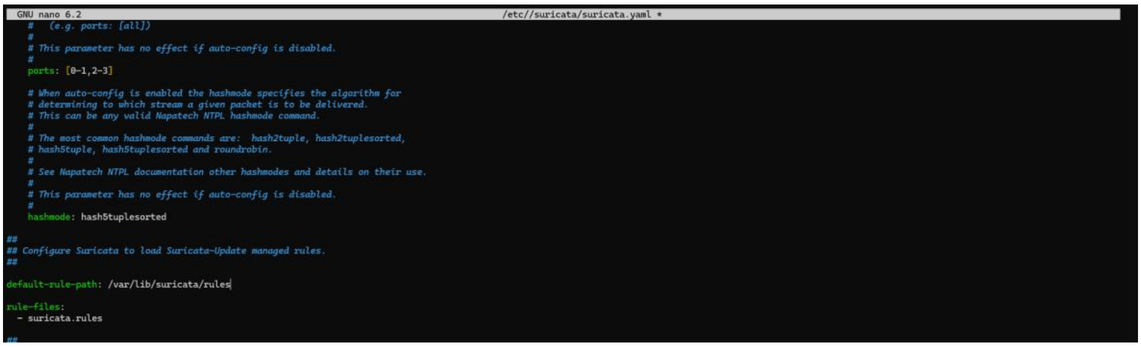


```
  GNU nano 6.2                                                        /etc/systemd/system/suricata.services
# Define the Suricata systemd unit
[Unit]
Description=Suricata IDS/IPS
After=network.target

# Specify the Suricata binary path, the configuration files location, and the network interface
[Service]
ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens18
[Install]

WantedBy=default.target
```



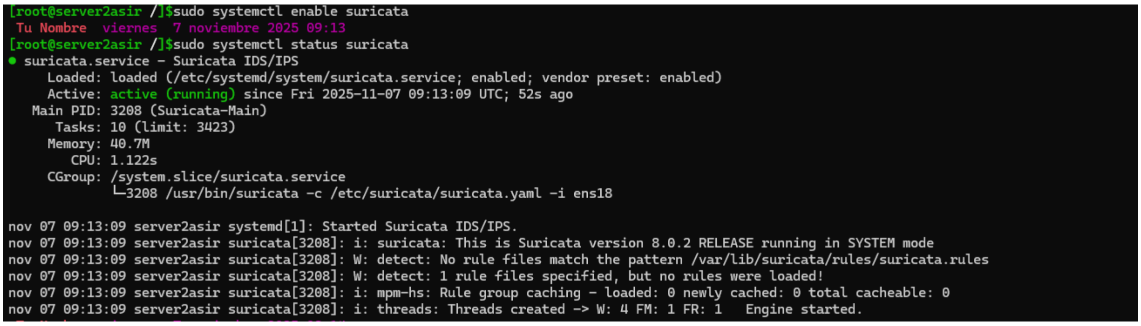
```
[root@server2asir usuario]$sudo systemctl enable suricata
Created symlink /etc/systemd/system/default.target.wants/suricata.service → /etc/systemd/system/suricata.service.
```

Debemos modificar lo de abajo



```
  GNU nano 6.2                                       /etc//suricata/suricata.yaml *
    #   (e.g. ports: [all])
    #
    # This parameter has no effect if auto-config is disabled.
    #
    ports: [0-1,2-3]

    # When auto-config is enabled the hashmode specifies the algorithm for
    # determining to which stream a given packet is to be delivered.
    # This can be any valid Napatech NTPL hashmode command.
    #
    # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
    # hash5tuple, hash5tuplesorted and roundrobin.
    #
    # See Napatech NTPL documentation other hashmodes and details on their use.
    #
    # This parameter has no effect if auto-config is disabled.
    #
    hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules

##
```

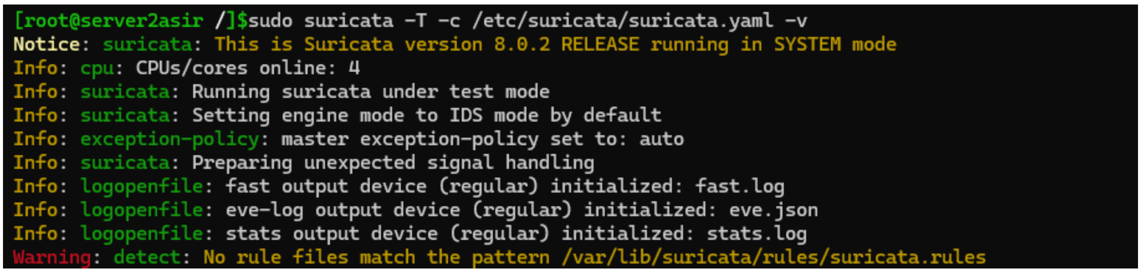
Luego volvemos a propar esto



```
[root@server2asir /]$sudo systemctl enable suricata
 Tu Nombre  viernes  7 noviembre 2025 09:13
[root@server2asir /]$sudo systemctl status suricata
● suricata.service - Suricata IDS/IPS
     Loaded: loaded (/etc/systemd/system/suricata.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-11-07 09:13:09 UTC; 52s ago
   Main PID: 3208 (Suricata-Main)
      Tasks: 10 (limit: 3423)
     Memory: 40.7M
        CPU: 1.122s
     CGroup: /system.slice/suricata.service
             └─3208 /usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens18

nov 07 09:13:09 server2asir systemd[1]: Started Suricata IDS/IPS.
nov 07 09:13:09 server2asir suricata[3208]: i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
nov 07 09:13:09 server2asir suricata[3208]: W: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
nov 07 09:13:09 server2asir suricata[3208]: W: detect: 1 rule files specified, but no rules were loaded!
nov 07 09:13:09 server2asir suricata[3208]: i: mpm-hs: Rule group caching - loaded: 0 newly cached: 0 total cacheable: 0
nov 07 09:13:09 server2asir suricata[3208]: i: threads: Threads created -> W: 4 FM: 1 FR: 1   Engine started.
```

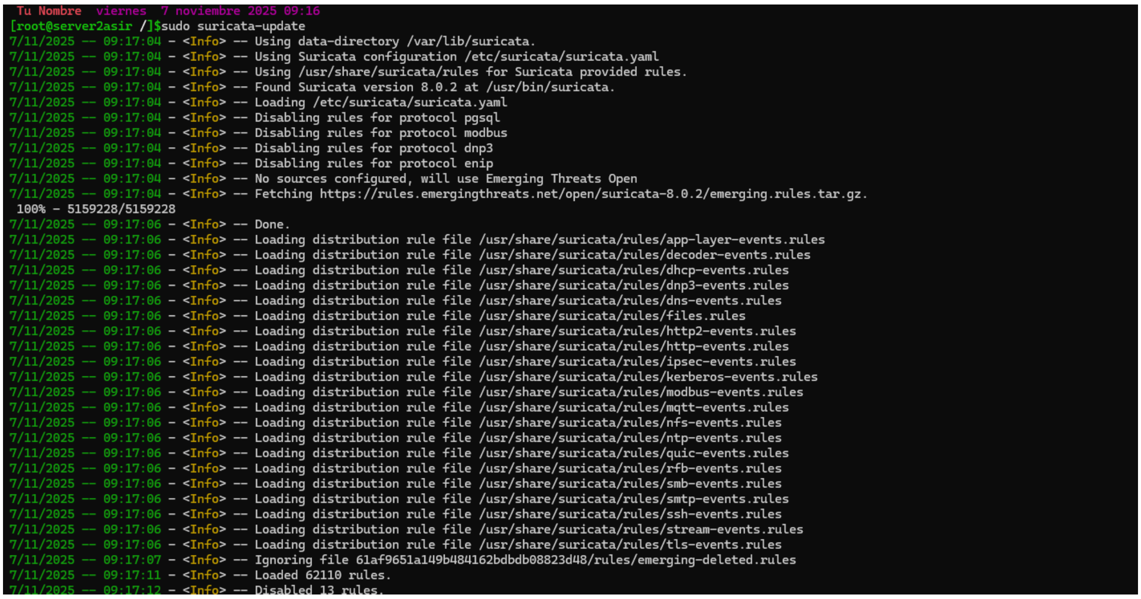
Prueba la funcionalidad de Suricata

sudo suricata -T -c /etc/suricata/suricata.yaml -v



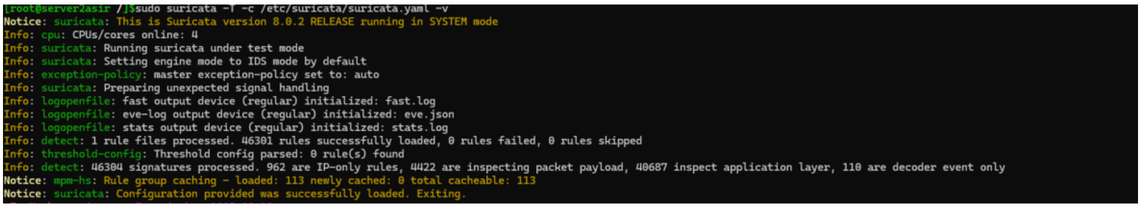
```
[root@server2asir /]$sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: suricata: Preparing unexpected signal handling
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Warning: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
```

Actualizamos que no machea



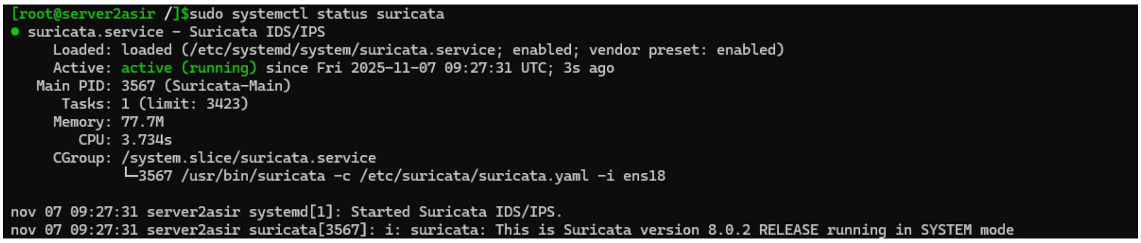
```
 Tu Nombre  viernes  7 noviembre 2025 09:16
[root@server2asir /]$sudo suricata-update
7/11/2025 -- 09:17:04 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2025 -- 09:17:04 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
7/11/2025 -- 09:17:04 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
7/11/2025 -- 09:17:04 - <Info> -- Found Suricata version 8.0.2 at /usr/bin/suricata.
7/11/2025 -- 09:17:04 - <Info> -- Loading /etc/suricata/suricata.yaml
7/11/2025 -- 09:17:04 - <Info> -- Disabling rules for protocol pgsql
7/11/2025 -- 09:17:04 - <Info> -- Disabling rules for protocol modbus
7/11/2025 -- 09:17:04 - <Info> -- Disabling rules for protocol dnp3
7/11/2025 -- 09:17:04 - <Info> -- Disabling rules for protocol enip
7/11/2025 -- 09:17:04 - <Info> -- No sources configured, will use Emerging Threats Open
7/11/2025 -- 09:17:04 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-8.0.2/emerging.rules.tar.gz.
 100% - 5159228/5159228
7/11/2025 -- 09:17:06 - <Info> -- Done.
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/app-layer-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dhcp-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dnp3-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dns-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/files.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http2-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ipsec-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/kerberos-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/modbus-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/mqtt-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/nfs-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ntp-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/quic-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/rfb-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/smb-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/smtp-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ssh-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/stream-events.rules
7/11/2025 -- 09:17:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/tls-events.rules
7/11/2025 -- 09:17:07 - <Info> -- Ignoring file 61af9651a149b484162bdbdb08823d48/rules/emerging-deleted.rules
7/11/2025 -- 09:17:11 - <Info> -- Loaded 62110 rules.
7/11/2025 -- 09:17:12 - <Info> -- Disabled 13 rules.
```

Despues si hacemos lo mismo hemos solucionado el warning



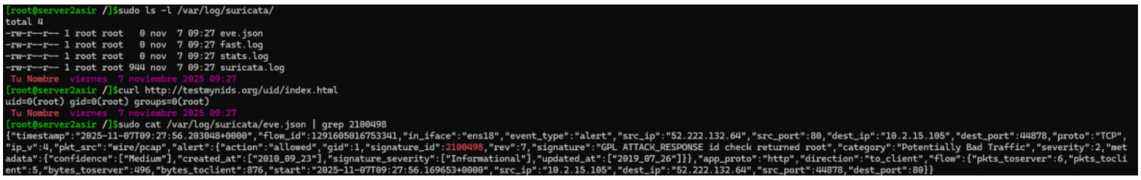
```
[root@server2asir /]$sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: suricata: Preparing unexpected signal handling
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 46301 rules successfully loaded, 0 rules failed, 0 rules skipped
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 46304 signatures processed. 962 are IP-only rules, 4422 are inspecting packet payload, 40687 inspect application layer, 110 are decoder event only
Notice: mpm-hs: Rule group caching - loaded: 113 newly cached: 0 total cacheable: 113
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

D

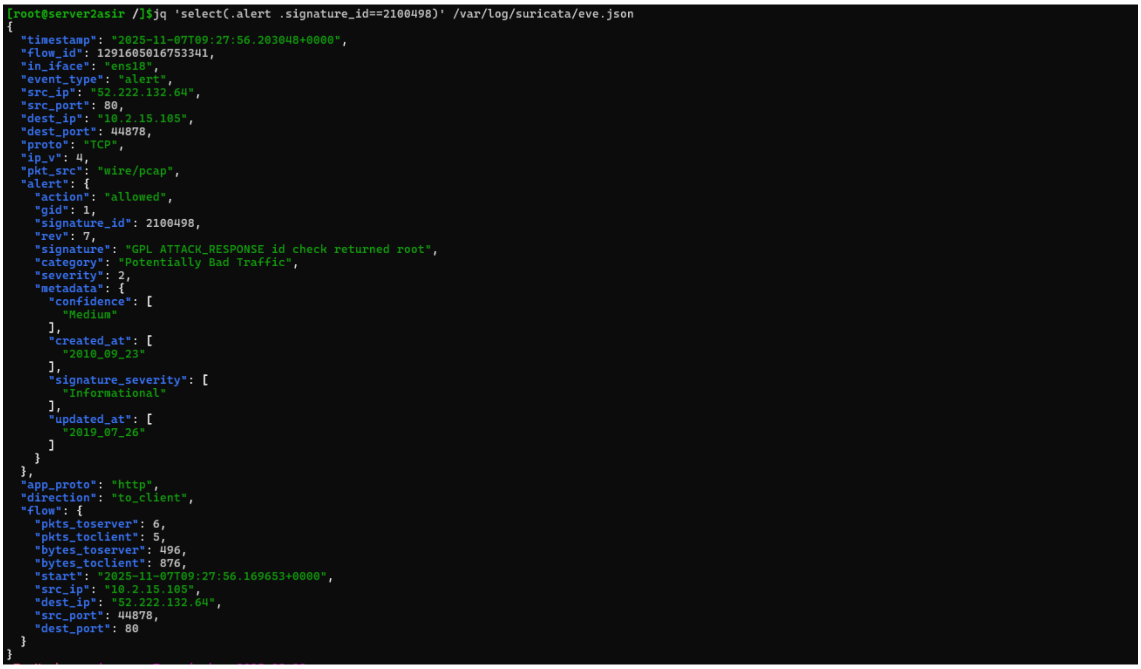


```
[root@server2asir /]$sudo systemctl status suricata
● suricata.service - Suricata IDS/IPS
     Loaded: loaded (/etc/systemd/system/suricata.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-11-07 09:27:31 UTC; 3s ago
   Main PID: 3567 (Suricata-Main)
      Tasks: 1 (limit: 3423)
     Memory: 77.7M
        CPU: 3.734s
     CGroup: /system.slice/suricata.service
             └─3567 /usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens18

nov 07 09:27:31 server2asir systemd[1]: Started Suricata IDS/IPS.
nov 07 09:27:31 server2asir suricata[3567]: i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
```

Vemos la hota de creación porque es importante saber que cuando se reinicia se ha creado



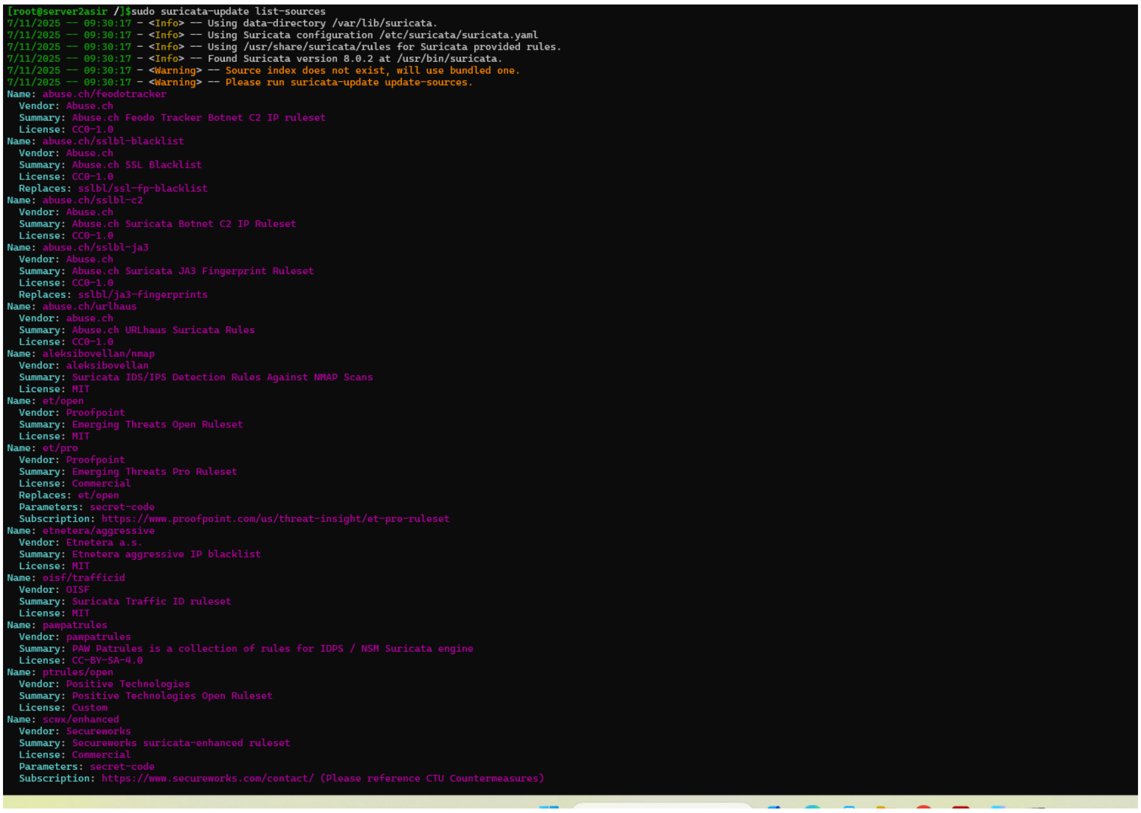
```
[root@server2asir /]$sudo ls -l /var/log/suricata/
total 4
-rw-r--r-- 1 root root   0 nov  7 09:27 eve.json
-rw-r--r-- 1 root root   0 nov  7 09:27 fast.log
-rw-r--r-- 1 root root   0 nov  7 09:27 stats.log
-rw-r--r-- 1 root root 944 nov  7 09:27 suricata.log
 Tu Nombre  viernes  7 noviembre 2025 09:27
[root@server2asir /]$curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
 Tu Nombre  viernes  7 noviembre 2025 09:27
[root@server2asir /]$sudo cat /var/log/suricata/eve.json | grep 2100498
{"timestamp":"2025-11-07T09:27:56.203048+0000","flow_id":1291605016753341,"in_iface":"ens18","event_type":"alert","src_ip":"52.222.132.64","src_port":80,"dest_ip":"10.2.15.105","dest_port":44878,"proto":"TCP",
"ip_v":4,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":2100498,"rev":7,"signature":"GPL ATTACK_RESPONSE id check returned root","category":"Potentially Bad Traffic","severity":2,"met
adata":{"confidence":["Medium"],"created_at":["2010_09_23"],"signature_severity":["Informational"],"updated_at":["2019_07_26"]}},"app_proto":"http","direction":"to_client","flow":{"pkts_toserver":6,"pkts_tocli
ent":5,"bytes_toserver":496,"bytes_toclient":876,"start":"2025-11-07T09:27:56.169653+0000","src_ip":"10.2.15.105","dest_ip":"52.222.132.64","src_port":44878,"dest_port":80}}
```



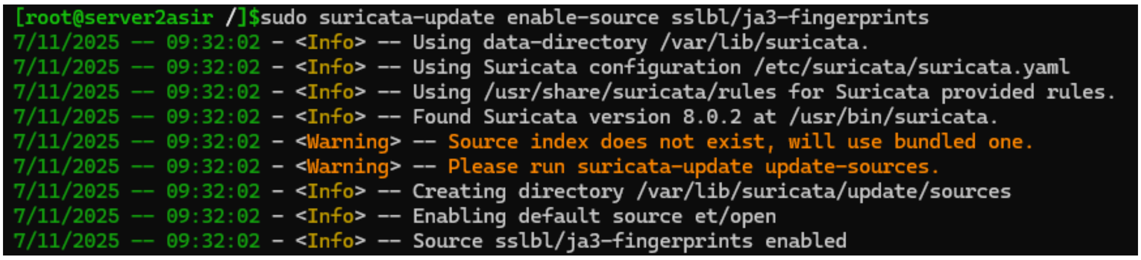
```
[root@server2asir /]$jq 'select(.alert .signature_id==2100498)' /var/log/suricata/eve.json
{
  "timestamp": "2025-11-07T09:27:56.203048+0000",
  "flow_id": 1291605016753341,
  "in_iface": "ens18",
  "event_type": "alert",
  "src_ip": "52.222.132.64",
  "src_port": 80,
  "dest_ip": "10.2.15.105",
  "dest_port": 44878,
  "proto": "TCP",
  "ip_v": 4,
  "pkt_src": "wire/pcap",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2100498,
    "rev": 7,
    "signature": "GPL ATTACK_RESPONSE id check returned root",
    "category": "Potentially Bad Traffic",
    "severity": 2,
    "metadata": {
      "confidence": [
        "Medium"
      ],
      "created_at": [
        "2010_09_23"
      ],
      "signature_severity": [
        "Informational"
      ],
      "updated_at": [
        "2019_07_26"
      ]
    }
  },
  "app_proto": "http",
  "direction": "to_client",
  "flow": {
    "pkts_toserver": 6,
    "pkts_toclient": 5,
    "bytes_toserver": 496,
    "bytes_toclient": 876,
    "start": "2025-11-07T09:27:56.169653+0000",
    "src_ip": "10.2.15.105",
    "dest_ip": "52.222.132.64",
    "src_port": 44878,
    "dest_port": 80
  }
}
```

Actualiza las normas de Suricata

sudo suricata-update list-sources

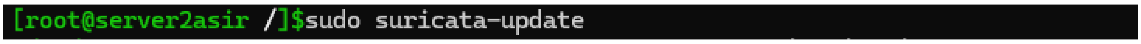


```
[root@server2asir /]$sudo suricata-update list-sources
7/11/2025 -- 09:30:17 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2025 -- 09:30:17 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
7/11/2025 -- 09:30:17 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
7/11/2025 -- 09:30:17 - <Info> -- Found Suricata version 8.0.2 at /usr/bin/suricata.
7/11/2025 -- 09:30:17 - <Warning> -- Source index does not exist, will use bundled one.
7/11/2025 -- 09:30:17 - <Warning> -- Please run suricata-update update-sources.
Name: abuse.ch/feodotracker
  Vendor: Abuse.ch
  Summary: Abuse.ch Feodo Tracker Botnet C2 IP ruleset
  License: CC0-1.0
Name: abuse.ch/sslbl-blacklist
  Vendor: Abuse.ch
  Summary: Abuse.ch SSL Blacklist
  License: CC0-1.0
  Replaces: sslbl/ssl-fp-blacklist
Name: abuse.ch/sslbl-c2
  Vendor: Abuse.ch
  Summary: Abuse.ch Suricata Botnet C2 IP Ruleset
  License: CC0-1.0
Name: abuse.ch/sslbl-ja3
  Vendor: Abuse.ch
  Summary: Abuse.ch Suricata JA3 Fingerprint Ruleset
  License: CC0-1.0
  Replaces: sslbl/ja3-fingerprints
Name: abuse.ch/urlhaus
  Vendor: abuse.ch
  Summary: Abuse.ch URLhaus Suricata Rules
  License: CC0-1.0
Name: aleksibovellan/nmap
  Vendor: aleksibovellan
  Summary: Suricata IDS/IPS Detection Rules Against NMAP Scans
  License: MIT
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: etnetera/aggressive
  Vendor: Etnetera a.s.
  Summary: Etnetera aggressive IP blacklist
  License: MIT
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: pawpatrules
  Vendor: pawpatrules
  Summary: PAW Patrules is a collection of rules for IDPS / NSM Suricata engine
  License: CC-BY-SA-4.0
Name: ptrules/open
  Vendor: Positive Technologies
  Summary: Positive Technologies Open Ruleset
  License: Custom
Name: scwx/enhanced
  Vendor: Secureworks
  Summary: Secureworks suricata-enhanced ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
```



```
[root@server2asir /]$sudo suricata-update enable-source sslbl/ja3-fingerprints
7/11/2025 -- 09:32:02 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2025 -- 09:32:02 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
7/11/2025 -- 09:32:02 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
7/11/2025 -- 09:32:02 - <Info> -- Found Suricata version 8.0.2 at /usr/bin/suricata.
7/11/2025 -- 09:32:02 - <Warning> -- Source index does not exist, will use bundled one.
7/11/2025 -- 09:32:02 - <Warning> -- Please run suricata-update update-sources.
7/11/2025 -- 09:32:02 - <Info> -- Creating directory /var/lib/suricata/update/sources
7/11/2025 -- 09:32:02 - <Info> -- Enabling default source et/open
7/11/2025 -- 09:32:02 - <Info> -- Source sslbl/ja3-fingerprints enabled
```

Tenemos que hacer otro update o explota

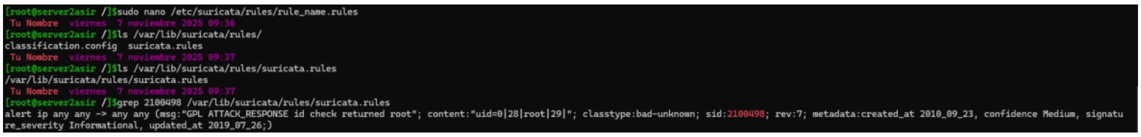


```
[root@server2asir /]$sudo suricata-update
```

Y luego reiniciar

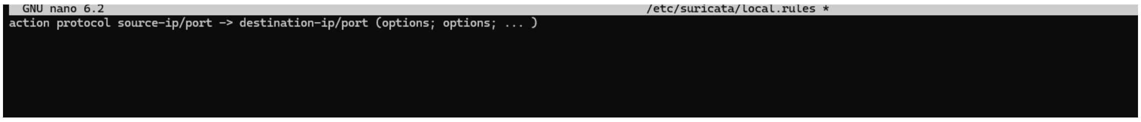
sudo systemctl restart suricata

Donde dice el ejercicio no se encuentra por lo que haremos las reglas en otro sitio



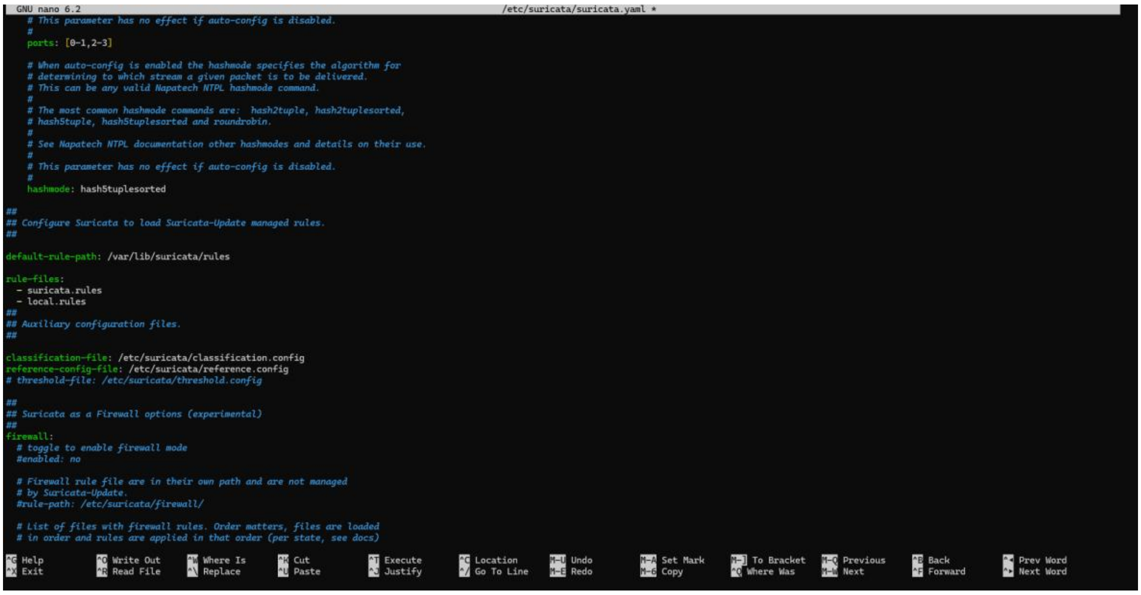
```
[root@server2asir /]$sudo nano /etc/suricata/rules/rule_name.rules
 Tu Nombre  viernes  7 noviembre 2025 09:36
[root@server2asir /]$ls /var/lib/suricata/rules/
classification.config  suricata.rules
 Tu Nombre  viernes  7 noviembre 2025 09:37
[root@server2asir /]$ls /var/lib/suricata/rules/suricata.rules
/var/lib/suricata/rules/suricata.rules
 Tu Nombre  viernes  7 noviembre 2025 09:37
[root@server2asir /]$grep 2100498 /var/lib/suricata/rules/suricata.rules
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; classtype:bad-unknown; sid:2100498; rev:7; metadata:created_at 2010_09_23, confidence Medium, signatu
re_severity Informational, updated_at 2019_07_26;)
```

Creamos la regla personalizada



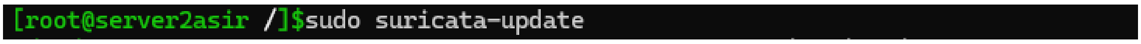
```
  GNU nano 6.2                                                      /etc/suricata/local.rules *
action protocol source-ip/port -> destination-ip/port (options; options; ... )
```

Y modificamos en .yaml añadiendo local.rules



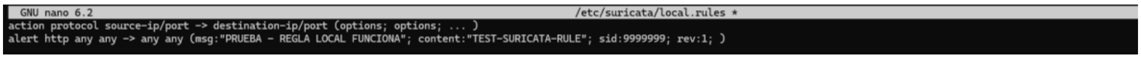
```
  GNU nano 6.2                                                      /etc/suricata/suricata.yaml *
    # This parameter has no effect if auto-config is disabled.
    #
    ports: [0-1,2-3]

    # When auto-config is enabled the hashmode specifies the algorithm for
    # determining to which stream a given packet is to be delivered.
    # This can be any valid Napatech NTPL hashmode command.
    #
    # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
    # hash5tuple, hash5tuplesorted and roundrobin.
    #
    # See Napatech NTPL documentation other hashmodes and details on their use.
    #
    # This parameter has no effect if auto-config is disabled.
    #
    hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - local.rules
##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config

##
## Suricata as a Firewall options (experimental)
##
firewall:
  # toggle to enable firewall mode
  #enabled: no

  # Firewall rule file are in their own path and are not managed
  # by Suricata-Update.
  #rule-path: /etc/suricata/firewall/

  # List of files with firewall rules. Order matters, files are loaded
  # in order and rules are applied in that order (per state, see docs)
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location    M-U Undo  M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back     ^◂ Prev Word
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy      ^Q Where Was    M-W Next      ^F Forward  ^▸ Next Word
```

Hacemos update o explota



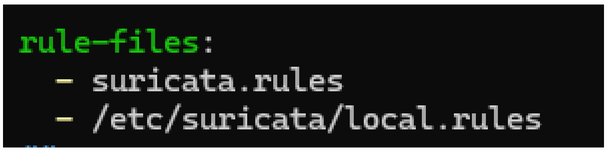
```
[root@server2asir /]$sudo suricata-update
```

Vamos a generar trafico añadiendo otra reglita en local.rules para comprobar que funciona



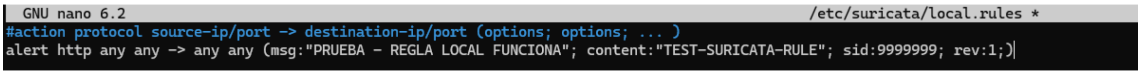
```
 GNU nano 6.2                                                        /etc/suricata/local.rules *
action protocol source-ip/port -> destination-ip/port (options; options; ... )
alert http any any -> any any (msg:"PRUEBA - REGLA LOCAL FUNCIONA"; content:"TEST-SURICATA-RULE"; sid:9999999; rev:1; )
```

Hacemos update y restart y luego vemos un error que era que había puesto local.rules en vez de la dirección completa



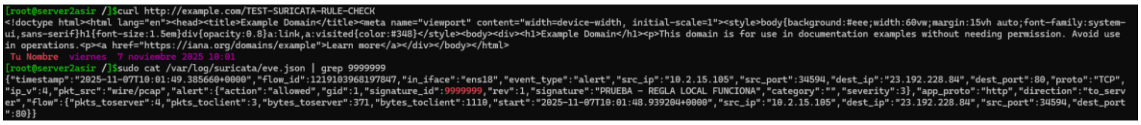
```
rule-files:
  - suricata.rules
  - /etc/suricata/local.rules
```

Ademas modifico el archivo y pongo almohadilla porque no carga las dos reglas juntas por lo que voy a probar que funciona el archivo con la generación de trafico que es mas fácil comprobar el funcionamiento



```
 GNU nano 6.2                                                        /etc/suricata/local.rules *
#action protocol source-ip/port -> destination-ip/port (options; options; ... )
alert http any any -> any any (msg:"PRUEBA - REGLA LOCAL FUNCIONA"; content:"TEST-SURICATA-RULE"; sid:9999999; rev:1;)
```

Generamos trafico con curl y luego hacemos un grep con 999999 de la regla nueva y vemos su funcionamiento



```
[root@server2asir /]$curl http://example.com/TEST-SURICATA-RULE-CHECK
<!doctype html><html lang="en"><head><title>Example Domain</title><meta name="viewport" content="width=device-width, initial-scale=1"><style>body{background:#eee;width:60vw;margin:15vh auto;font-family:system-
ui,sans-serif}h1{font-size:1.5em}div{opacity:0.8}a:link,a:visited{color:#348}</style><body><div><h1>Example Domain</h1><p>This domain is for use in documentation examples without needing permission. Avoid use
in operations.<p><a href="https://iana.org/domains/example">Learn more</a></div></body></html>
 Tu Nombre  viernes  7 noviembre 2025 10:01
[root@server2asir /]$sudo cat /var/log/suricata/eve.json | grep 9999999
{"timestamp":"2025-11-07T10:01:49.385660+0000","flow_id":1219103968197847,"in_iface":"ens18","event_type":"alert","src_ip":"10.2.15.105","src_port":34594,"dest_ip":"23.192.228.84","dest_port":80,"proto":"TCP",
"ip_v":4,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":9999999,"rev":1,"signature":"PRUEBA - REGLA LOCAL FUNCIONA","category":"","severity":3},"app_proto":"http","direction":"to_serv
er","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":371,"bytes_toclient":1110,"start":"2025-11-07T10:01:48.939204+0000","src_ip":"10.2.15.105","dest_ip":"23.192.228.84","src_port":34594,"dest_port
":80}}
```

Para dejarlo bien borramos la línea de alert en /etc/suricata/local.rules y lo dejamos con solo la primera línea que es lo que pide la practica, actualizando y reiniciando ya estaría en marcha