**1. Choose a Tool: Snort or Suricata**

* **Snort**: Lightweight, flexible, widely used, rule-based NIDS.
* **Suricata**: Multi-threaded, high-performance, supports more protocols, better JSON output for visualization.

For modern setups, **Suricata** is recommended due to speed, protocol support, and log formats.

**2. Install Suricata**

**For Ubuntu/Debian:**

sudo apt update

sudo apt install suricata -y

**Verify version:**

suricata --build-info

A computer screen shot of a computer

AI-generated content may be incorrect.

**3. Configure Rules and Alerts**

**Location of config files:**

* /etc/suricata/suricata.yaml — main config
* /etc/suricata/rules/ — rule files

**Add Custom Rule:**

Create or edit a .rules file (e.g., local.rules):

alert http any any -> any any (msg:"Suspicious HTTP Request Detected"; content:"cmd="; nocase; sid:100001; rev:1;)

Update suricata.yaml to include local.rules:

yaml

CopyEdit

rule-files:

- local.rules

**Test Config:**

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

A computer screen shot of a computer screen

AI-generated content may be incorrect.

A computer screen shot of a computer code

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

**4. Monitor Network Traffic**

Start Suricata in live capture mode:

A computer screen shot

AI-generated content may be incorrect.

sudo suricata -c /etc/suricata/suricata.yaml -i eth0

Replace eth0 with your actual network interface.

A screenshot of a computer

AI-generated content may be incorrect.

**Where Logs Go:**

* /var/log/suricata/eve.json (main log with alerts)

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* /var/log/suricata/fast.log (summary of alerts)

A screen shot of a computer screen

AI-generated content may be incorrect.