Integration of the Suricata With the Wazuh

⚙️ Installing Suricata (on Ubuntu)

Suricata is a powerful open-source Intrusion Detection and Prevention System (IDS/IPS) that can monitor network traffic and raise alerts when malicious patterns are detected.

1) To install Suricata and update its rules:

a. **Install Suricata on the Ubuntu endpoint. We tested this process with version 6.0.8 and it can take some time:**

   a. **sudo add-apt-repository ppa:oisf/suricata-stable**
   b. **sudo apt-get update**
   c. **sudo apt-get install suricata -y**

b. **Download and extract the Emerging Threats Suricata ruleset:**

   a. **cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz**
      sudo tar -xvzf emerging.rules.tar.gz && sudo mkdir /etc/suricata/rules && sudo mv rules/*.rules /etc/suricata/rules/
      sudo chmod 640 /etc/suricata/rules/*.rules

---

2) Configuring Rule Files in Suricata

Once Suricata is installed, you need to configure it to use both community rules (suricata.rules) and your custom rules (local.rules).

Step 1: Open the main Suricata configuration file

```
sudo nano /etc/suricata/suricata.yaml
```

a)

Use Ctrl + W and search for rule-files: to find the correct section.

Ensure the section looks like this:

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

 -  “*.rules”   # Default rules from Emerging Threats

 - local.rules      # Your custom rules
```

Note: Ensure the rules exist in the /etc/suricata/rules folder otherwise search and configure the correct folder name with path

b) Use Ctrl + W and search HOME_NET and ensure the section looks as the following:

```
HOME_NET: "<UBUNTU_IP or Your Linux  _IP>"

EXTERNAL_NET: "any"
```

c) search the following and configure as follows:

```
# Global stats configuration

stats:

enabled: yes
```

d) Search and Configure as follows :

```
# Linux high speed capture support

af-packet:

  - interface: enp0s8  or any adapter no you find using the ifconfig command
```

e) Save and exit

Press Ctrl + O to write changes, then Ctrl + X to exit the editor.

✅ local.rules is a file where **you can write custom rules** for specific lab exercises, scans, attacks, etc.

---

3) Writing Custom Rules for DoS and Scanning Detection

Create and edit your local rules file:

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

Paste the following custom rules:

🚨 **Rule 1: Detect Nmap SYN Scan**

```
alert tcp any any -> any any (msg:"[CUSTOM] Nmap SYN Scan Detected"; flags:S; threshold:type both, track by_src, count 10, seconds 30; sid:1000001; rev:1;)
```

🚨 Rule 2: Detect ICMP Flood

```
alert icmp any any -> any any (msg:"[CUSTOM] ICMP Flood Detected"; itype:8; threshold:type both, track by_src, count 100, seconds 10; sid:1000002; rev:1;)
```

🚨 Rule 3: Detect TCP SYN Flood

```
alert tcp any any -> any any (msg:"[CUSTOM] TCP SYN Flood Detected"; flags:S; threshold:type threshold, track by_src, count 50, seconds 10; sid:1000003; rev:1;)
```

Save and exit the file.

---

4) Restart Suricata to Apply Custom Rules

```
sudo systemctl restart suricata
```

---

5) Add the following configuration to the /var/ossec/etc/ossec.conf file of the Wazuh agent. This allows the Wazuh agent to read the Suricata logs file:

```
<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</ossec_config>
```

Restart the Wazuh agent to apply the changes:

```
$ sudo systemctl restart wazuh-agent
```

6) Testing from Kali Linux (Attacker Machine)

Step 1: Nmap SYN Scan (Triggers Rule 1)

```
nmap -sS -T4 <Ubuntu-IP>
```

Step 2: ICMP Flood (Triggers Rule 2)

```
ping -f <Ubuntu-IP>
```

Or:

```
sudo hping3 --icmp --flood <Ubuntu-IP>
```

Step 3: TCP SYN Flood (Triggers Rule 3)

```
sudo hping3 -S --flood --rand-source -p 80 <Ubuntu-IP>
```

🔍 Viewing Alerts in Suricata

```
sudo tail -f /var/log/suricata/fast.log
```

Or view structured JSON logs:

```
sudo grep -i alert /var/log/suricata/eve.json
```

✅ You should see:

- [CUSTOM] Nmap SYN Scan Detected
- [CUSTOM] ICMP Flood Detected
- [CUSTOM] TCP SYN Flood Detected

With this setup, you now have a full A–Z lab on detecting DoS and scanning attacks using custom rules in Suricata.

🔄 Wazuh Agent Integration – Forward Suricata Logs to Wazuh

To monitor Suricata alerts in the Wazuh dashboard, follow these steps:

📁 Step 1: Configure Wazuh Agent to Monitor Suricata Logs (on VM2)

Edit the agent configuration file:

```
sudo nano /var/ossec/etc/ossec.conf
```

Add this block inside the <ossec_config> section:

```
<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
```

This tells the Wazuh agent to monitor Suricata's JSON log file.

🔄 Step 2.5: Restart Wazuh Agent on VM2

```
sudo systemctl restart wazuh-agent
```

✅ Wazuh will now collect Suricata logs and forward them to the Wazuh Manager. You can view alerts in the Wazuh Dashboard under **Security Events > Suricata**.