Detecting Suspicious Network Traffic using Suricata

Contents

Install and configure Suricata

1. Install Suricata

```
sudo apt install suricata -y
```

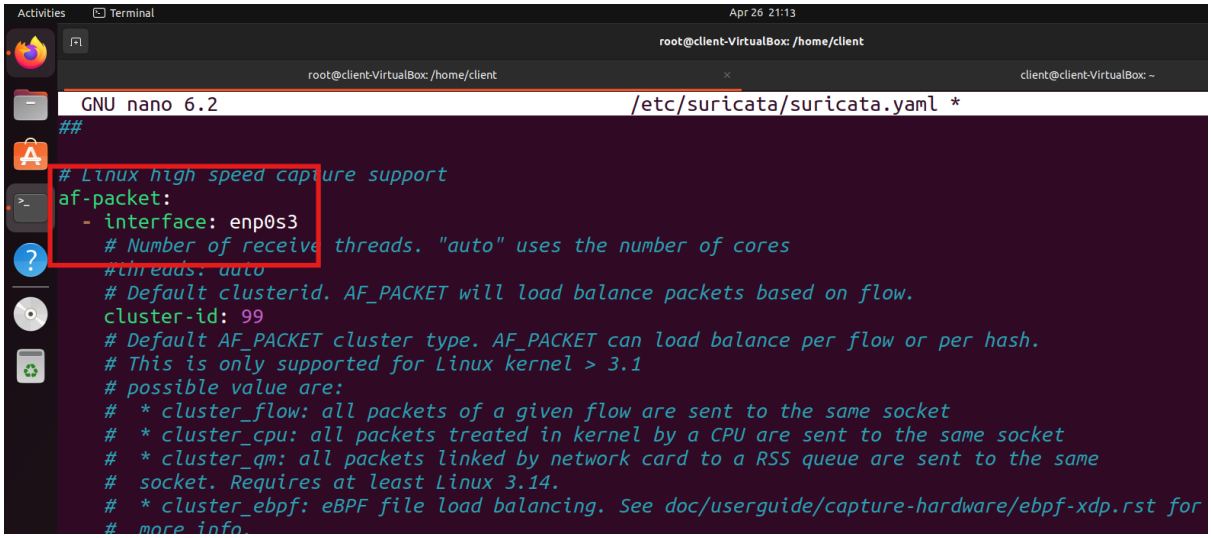
2. Update and install rules

```
sudo suricata-update
```

3. Start Suricata

```
sudo systemctl enable suricata
sudo systemctl start suricata
```

4. Edit /etc/suricata/suricata.yaml and change the interface. Check your interface using ip a command.



5. Adding custom rule to detect networking scaning. Edit suricata.rules file.

```
nano /var/lib/suricata/rules/local.rules
```

6. Add the custom rule to suricata.rules file.

```
alert tcp any any -> any any (msg:"Possible TCP Port Scan Detected";
flags:S; threshold:type threshold, track by_src, count 20, seconds 10;
sid:1000001; rev:1;)
```

7. Update and install rules

```
sudo suricata-update
```

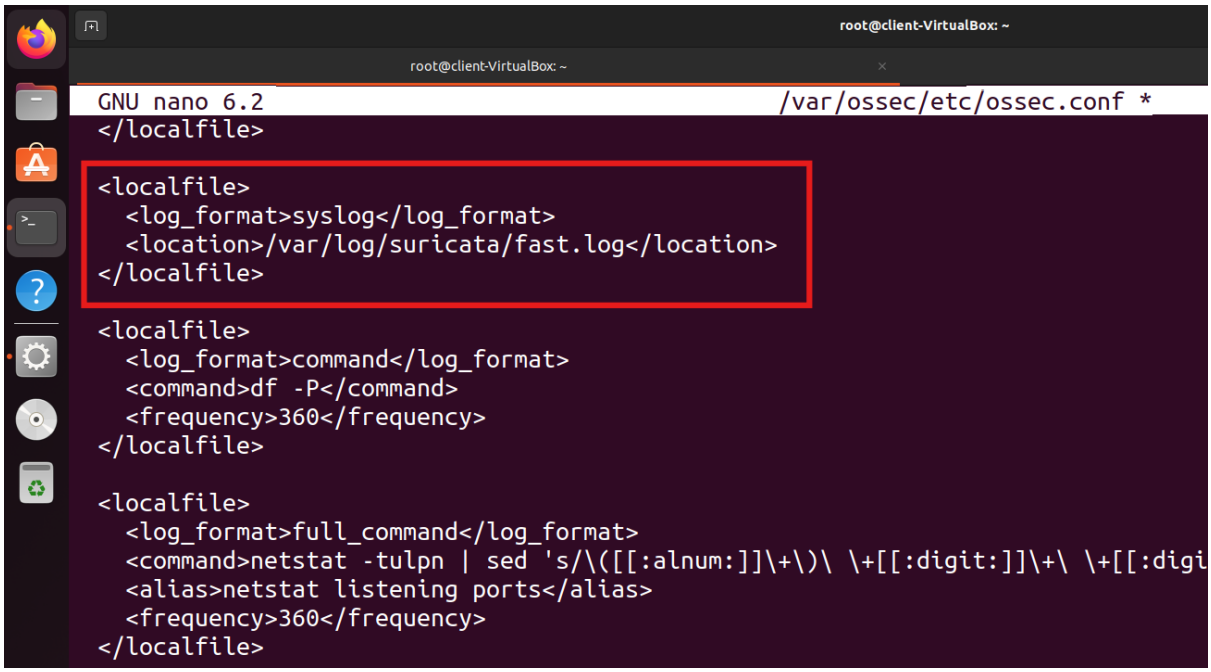
8. Restart suricata

```
sudo systemctl restart suricata
```

Send Suricata Alerts to Wazuh

1. Add this to Wazuh agent /var/ossec/etc/ossec.conf

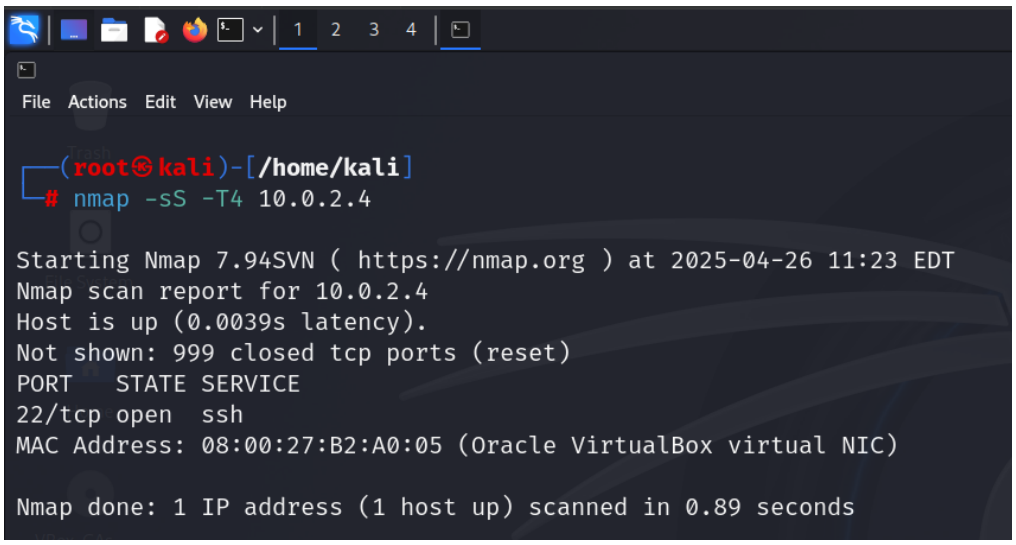
```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/suricata/fast.log</location>
</localfile>
```



Simulate Attack using Kali Linux

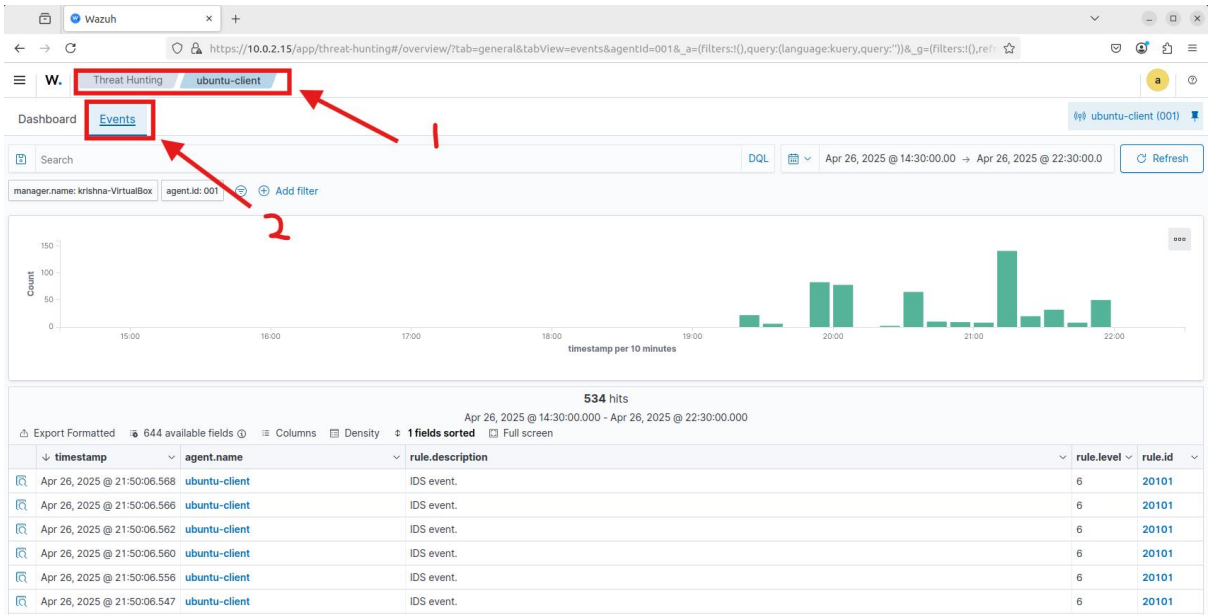
1. Run an nmap scan in kali linux

```
nmap -sS -T4 <target-ip>
```

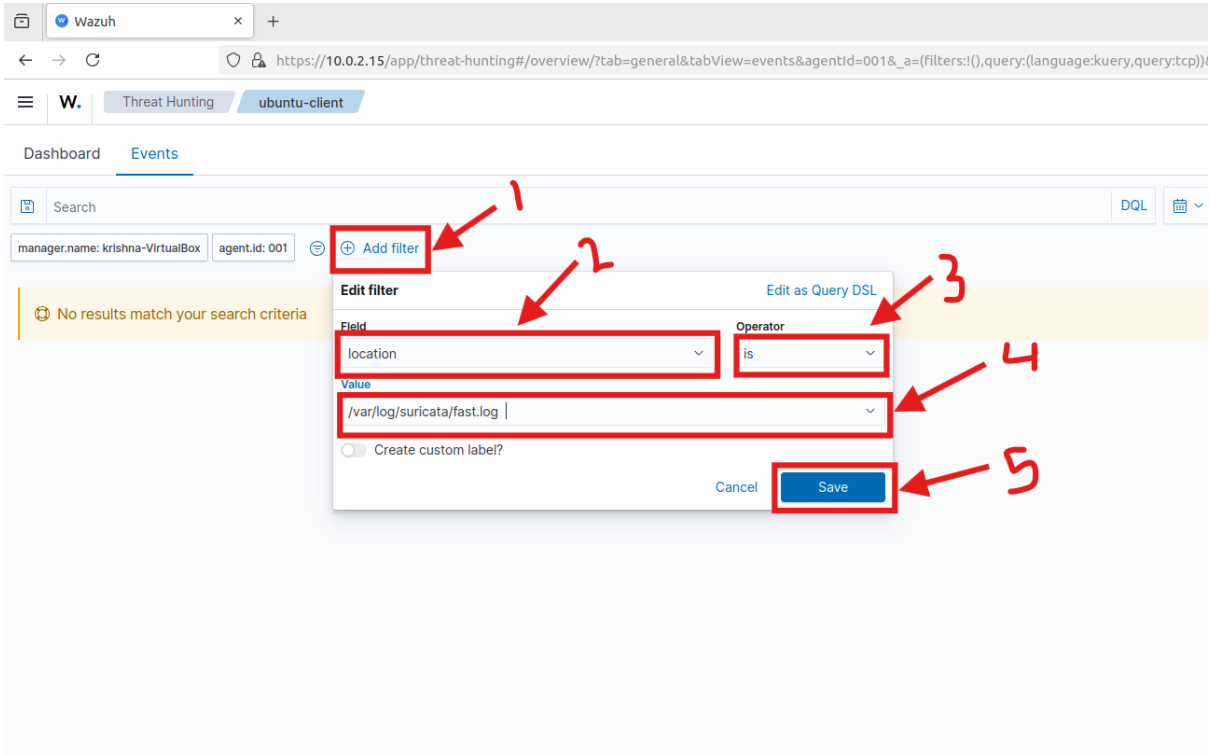


View Alerts in Wazuh Dashboard

1. Login to wazuh dashboard.
2. Navigate to Threat hunting → Choose agent → Events



3. Filter suricata logs using location value



4. These are the alerts generated.