

Detecting Suspicious Network Traffic using Suricata

Contents

Install and configure Suricata	1
Send Suricata Alerts to Wazuh	2
Simulate Attack using Kali Linux	3
View Alerts in Wazuh Dashboard	3

Install and configure Suricata

1. Install Suricata

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

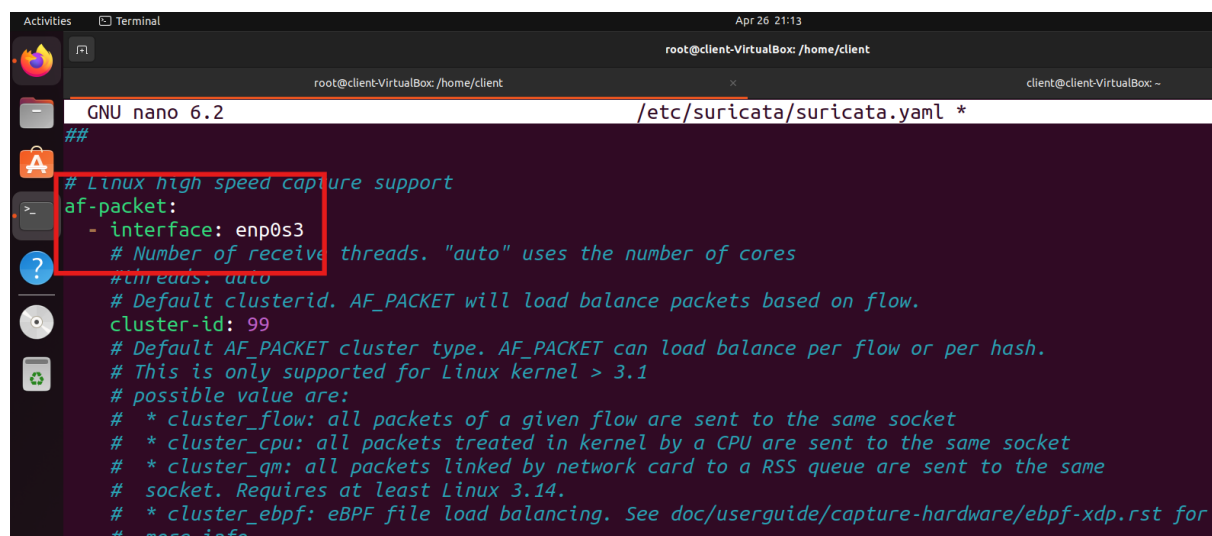
2. Update and install rules

```
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.



```
GNU nano 6.2 /etc/suricata/suricata.yaml *  
##  
# Linux high speed capture support  
af-packet:  
- interface: enp0s3  
  # 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.
```

5. Adding custom rule to detect networking scanning. 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
```

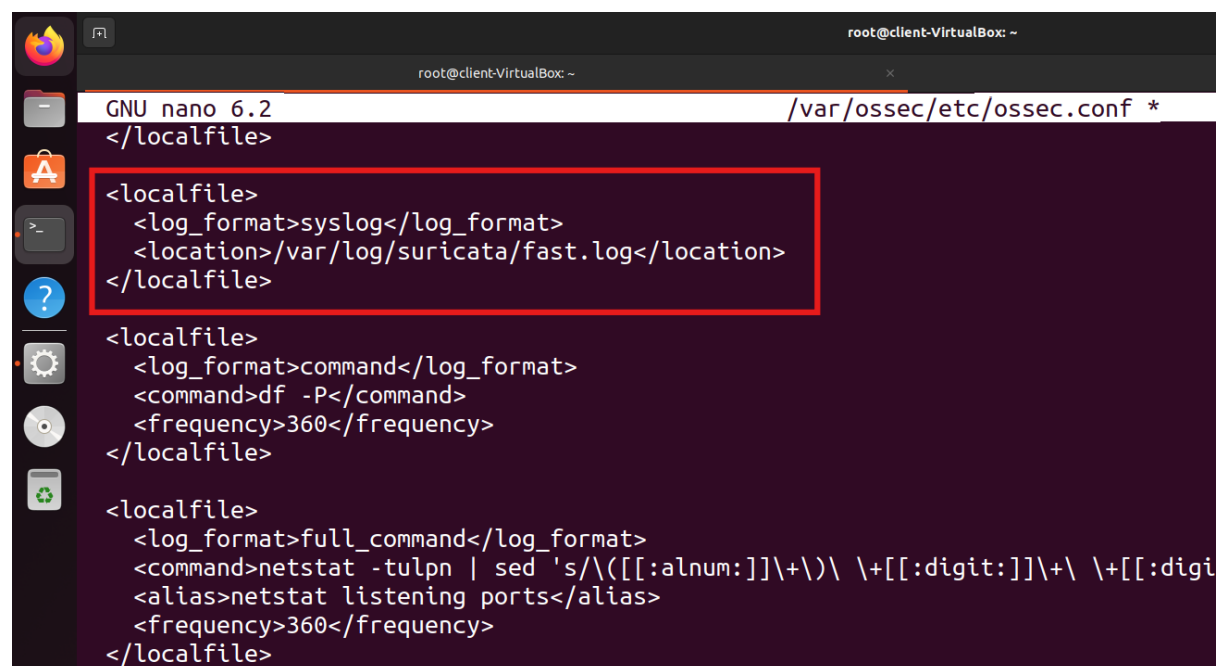
8. Restart suricata

```
sudo systemctl restart suricata
```

Send Suricata Alerts to Wazuh

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

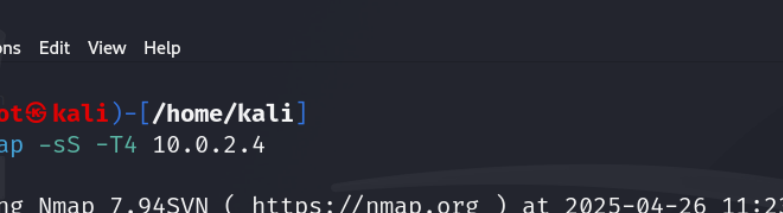
```
<localfile>  
  <log_format>syslog</log_format>  
  <location>/var/log/suricata/fast.log</location>  
</localfile>
```



Simulate Attack using Kali Linux

1. Run an nmap scan in kali linux

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



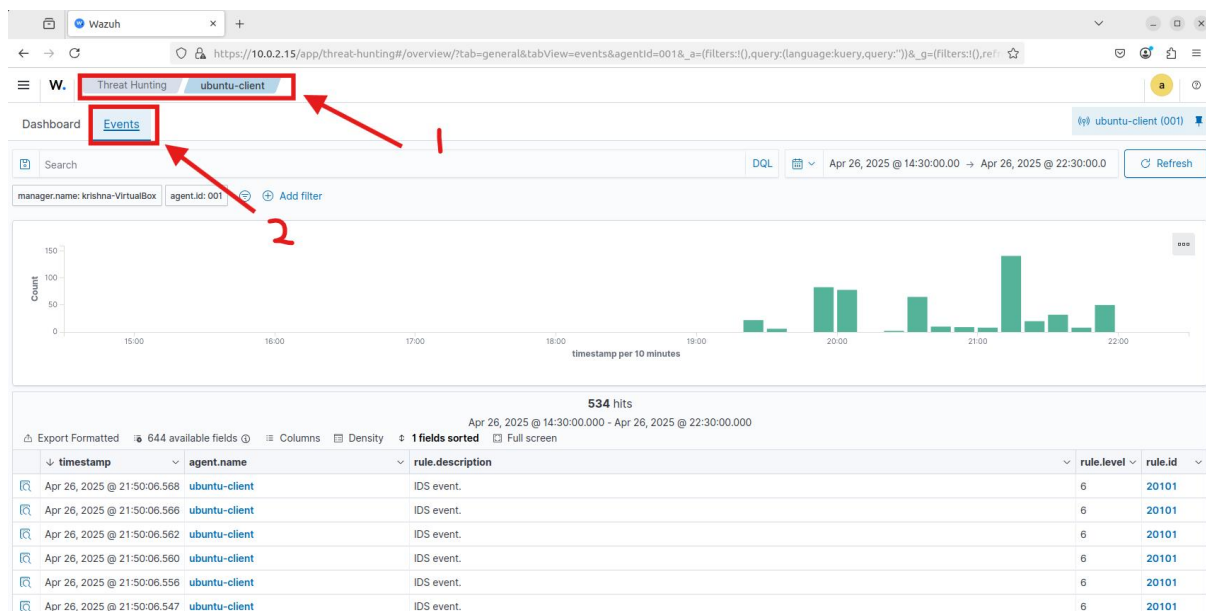
```
(root@kali)-[/home/kali]
# nmap -sS -T4 10.0.2.4

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 11:23 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0039s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:B2:A0:05 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

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

Wazuh Threat Hunting interface showing the 'Edit filter' dialog box. The dialog is open over a search results area that says "No results match your search criteria". The dialog has fields for 'Field' (location), 'Operator' (is), and 'Value' (/var/log/suricata/fast.log). Red arrows numbered 1 to 5 point to the 'Add filter' button, the 'Field' dropdown, the 'Operator' dropdown, the 'Value' input field, and the 'Save' button respectively.

4. These are the alerts generated.

