

## 5. Network Defense with Open-Source Tools

## Activities:

- **Tools:** Suricata, Elastic SIEM, CrowdSec.
- **Task:** Configure Suricata to block malicious IPs and map alerts to MITRE ATT&CK.

[illegible]

The screenshot shows a VMware Workstation window titled "kali-linux-2025.2-vmware-amd64 - VMware Workstation". Inside the VM, the terminal is running Metasploit Meterpreter. The prompt is `j@tcshuricata/rules/drop-malicious-ips.rules - Mousepad`. A red warning banner reads: "Warning: you are using the root account. You may harm your system." Below this, the command `1 drop ip [192.168.1.100,10.10.10.10] any -> any any (msg:"Blocked Malicious IP"; sid:100000; rev:1;)` has been entered, and the prompt is now `2|`. The bottom of the screen shows the Windows taskbar with the time 09:01 and date 22-08-2023.



```
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.

1 SYNTAX 1.1
2 ---
3
4 # Suricata configuration file. In addition to the comments describing all
5 # options in this file, full documentation can be found at:
6 # https://docs.suricata.io/en/latest/configuration/suricata-yaml.html
7
8 # This configuration file generated by Suricata 7.0.10.
9 suricata-version: "7.0"
10 alert http any any -> any any {
11   msg:"Possible Command and Control via HTTP";
12   flow:to_server,established;
13   content:"User-Agent[!a] Mozilla";
14   metadata:attack_technique_id=T1071.001, attack_tactic=Command and Control;
15   sid:1000002;
16   rev:1;
17 }
18 ##
19 ## Step 1: Inform Suricata about your network
20 ##
21
22 vars:
23   # More specific is better for alert accuracy and performance
24   address-group:
25     HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
26     EXTERNAL_NET: "[!192.168.0.0/16]"
27     HOME_NET: "[10.0.0.0/8]"
28     EXTERNAL_NET: "[!10.0.0.0/8]"
29     HOME_NET: "[172.16.0.0/12]"
30     EXTERNAL_NET: "[!172.16.0.0/12]"
31   HTTP_SERVERS: "$HOME_NET"
32   SMTP_SERVERS: "$HOME_NET"
33   SQL_SERVERS: "$HOME_NET"
34   DNS_SERVERS: "$HOME_NET"
35   TELNET_SERVERS: "$HOME_NET"
36   AIM_SERVERS: "$EXTERNAL_NET"
37   IRC_SERVERS: "$HOME_NET"
38   IMAP_SERVERS: "$HOME_NET"
39   NNTP_SERVERS: "$HOME_NET"
40   POP3_SERVERS: "$HOME_NET"
41   Socks_CLIENTS: "$HOME_NET"
```

## Enhanced Tasks:

- **Suricata Rule:** Create a rule to block a malicious IP:

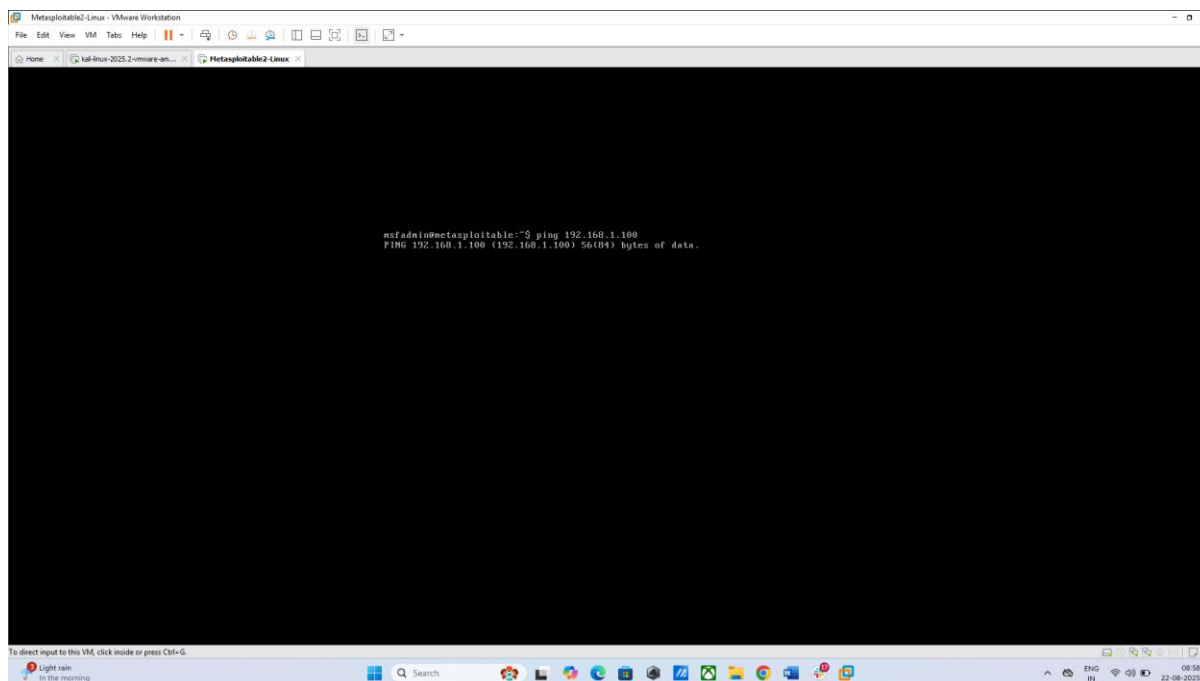
drop ip 192.168.1.100 any -> any any (msg:"Blocked Malicious IP"; sid:1000001; rev:1;)

```
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.

1 drop ip [192.168.1.100,10.10.10.10] any -> any any (msg:"Blocked Malicious IP"; sid:1000001; rev:1;)
2
```



- Test by ping from another VM.



- **ATT&CK Mapping:** Map a Suricata alert to a MITRE ATT&CK technique:

Alert	Tactic	Technique	Notes
-----	-----	-----	-----
Suspicious HTTP	Command and Control	T1071	Outbound traffic to C2

## MITRE ATT&CK Mapping Summary

Alert Name	Tactic	Technique ID	Technique Name	Notes
Suspicious HTTP	Command and control	T1071	Application Layer Protocol	Outbound traffic to C2