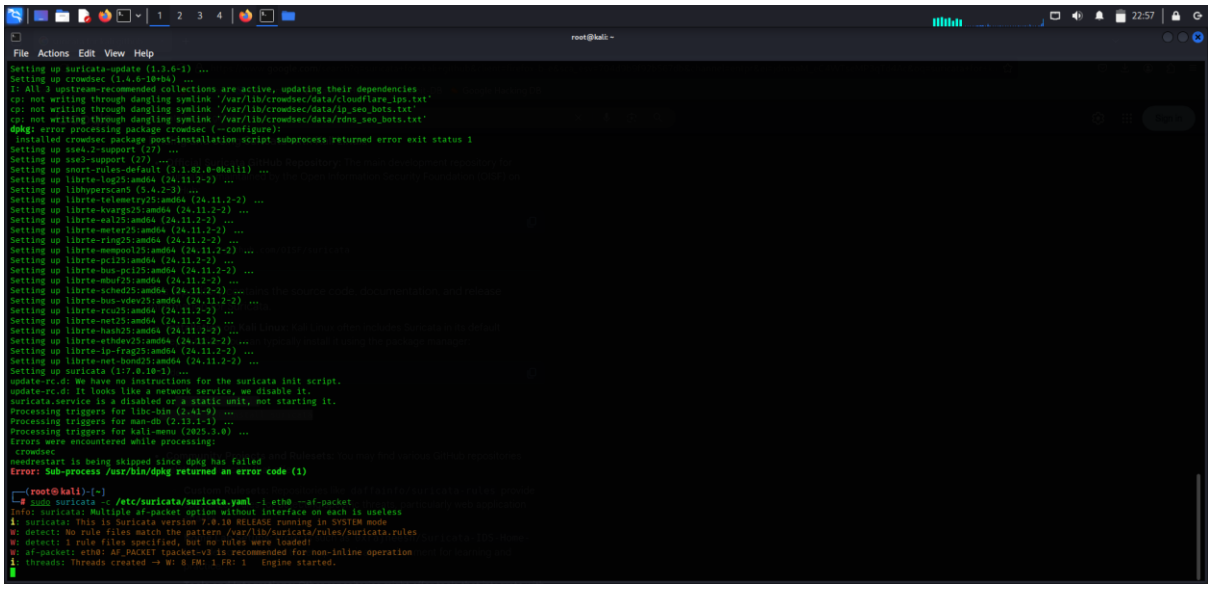
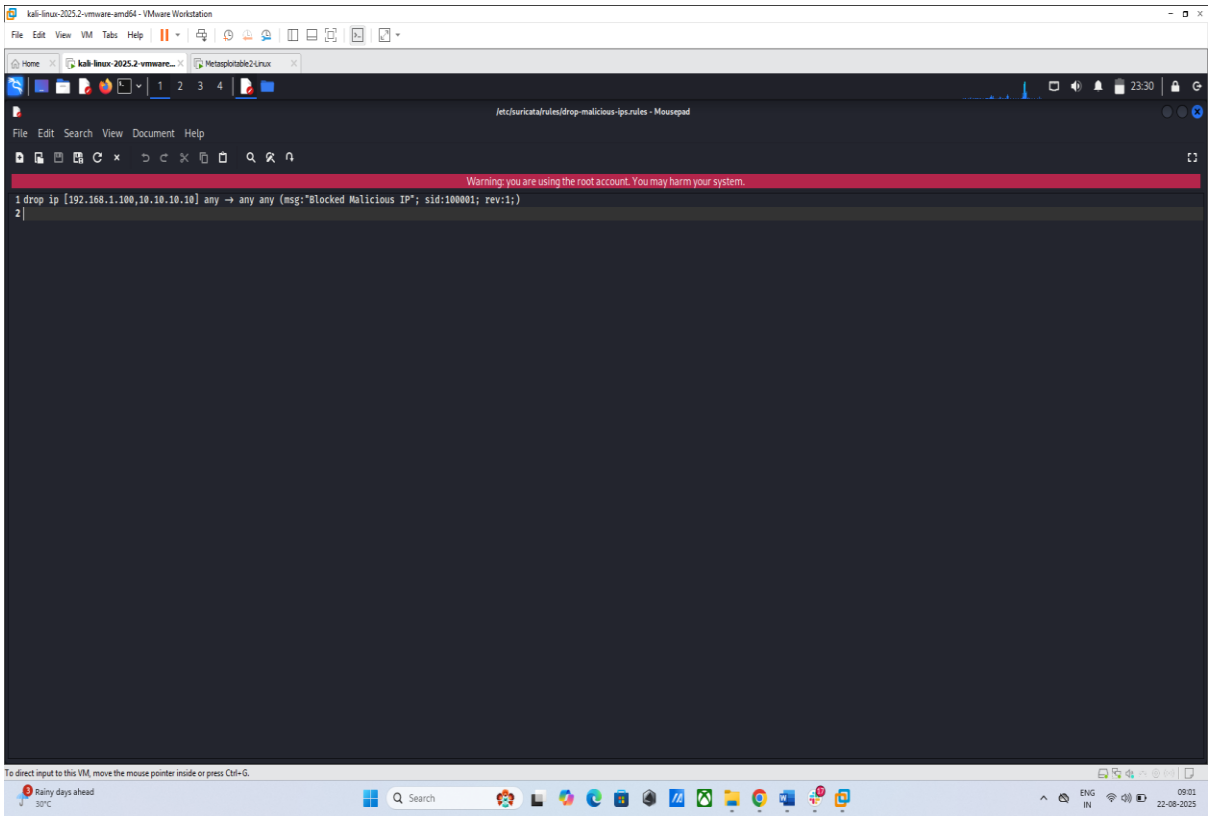
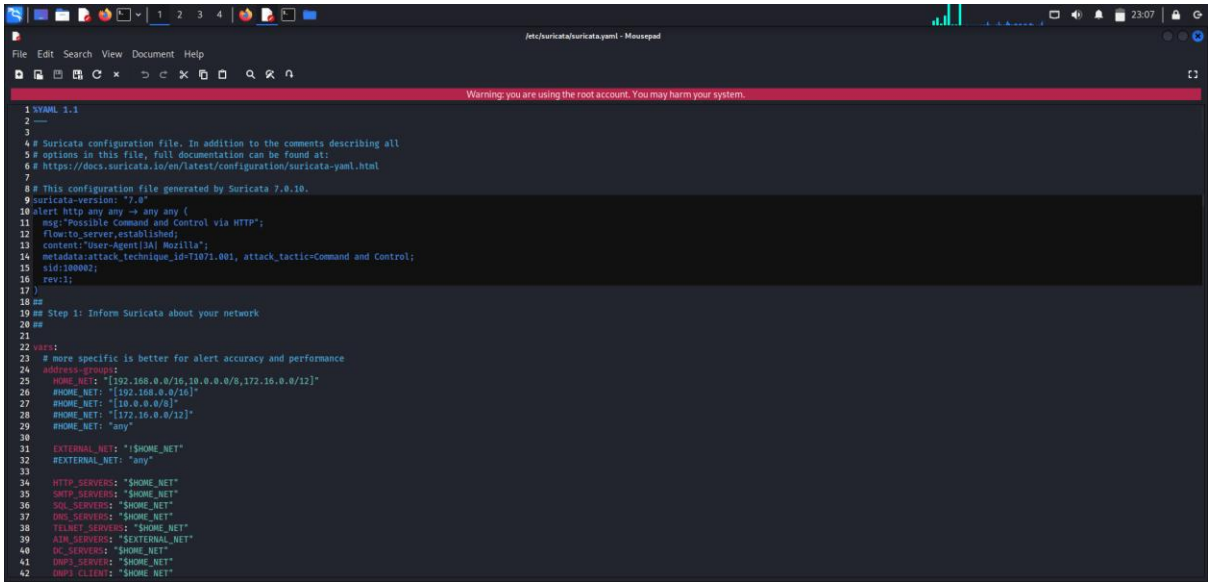
5. Network Defense with Open-Source Tools

Activities:

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



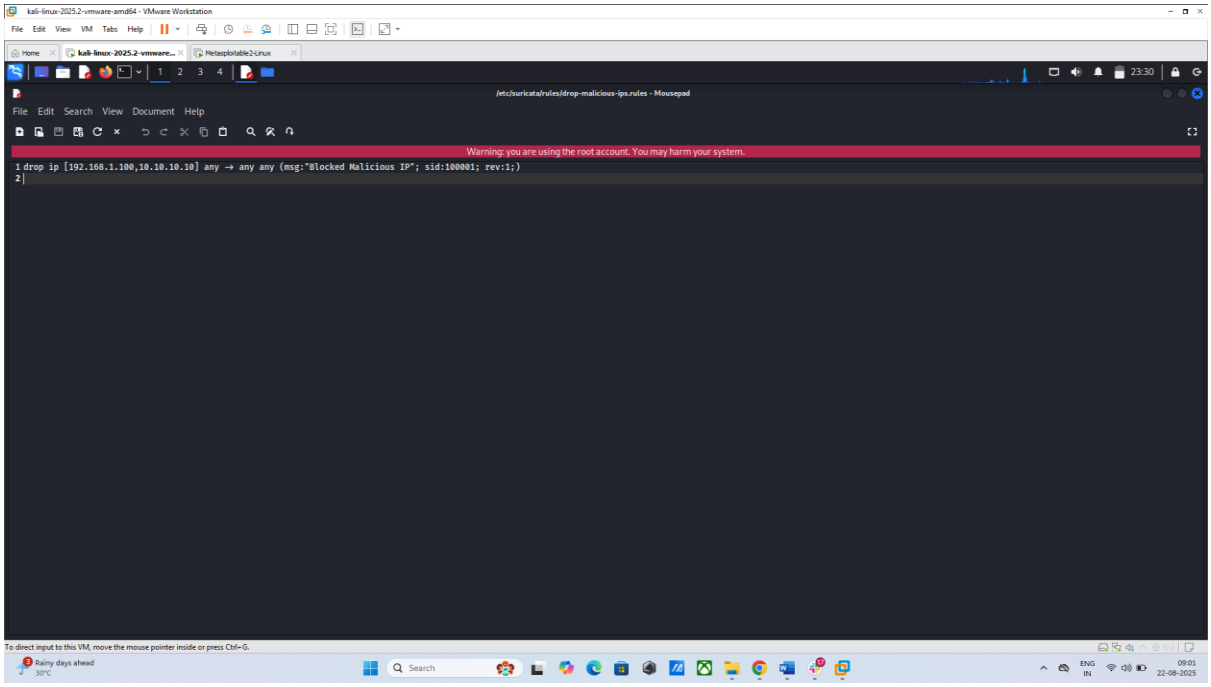




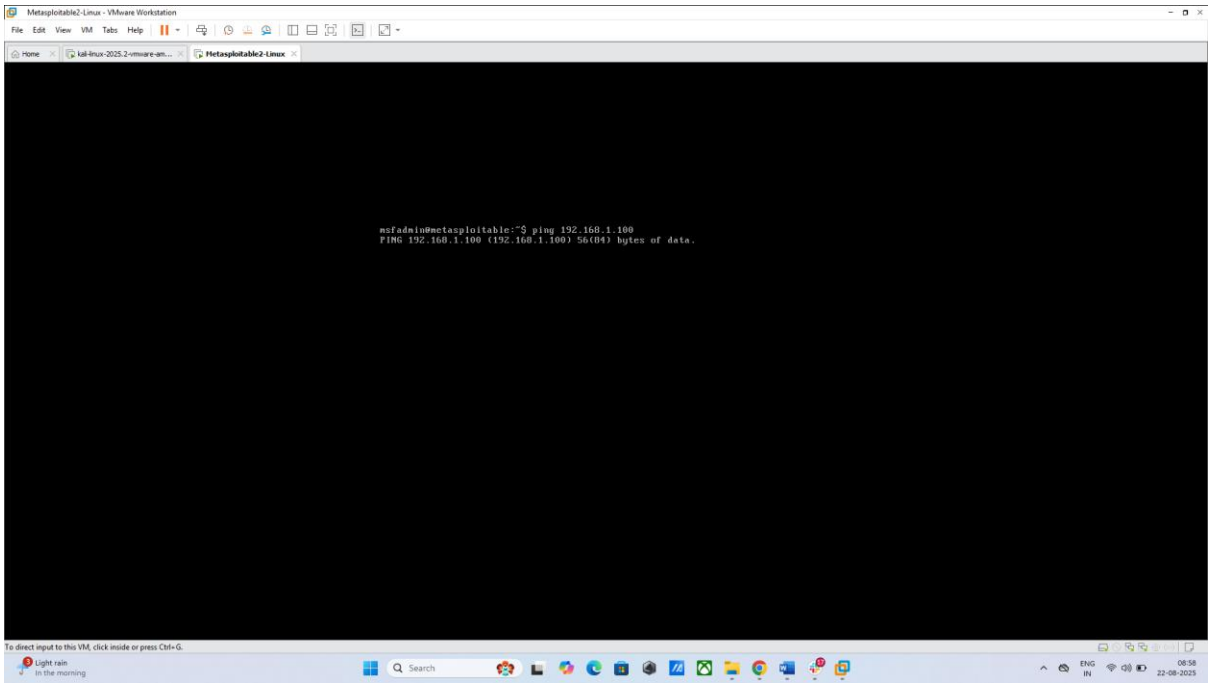
Enhanced Tasks:

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

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



- Test by pinging 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