Nids — SNORT Test Playbook & Internship Report

Company: Infotact Solution

Project: We Build Advanced Snort NIDS

Prepared by

Interns – Cyber Security Batch 9, Infotact Solutions

- **Dip Kar:** Core project development and NIDS implementation
- **Asmita Roy:** Documentation and final report preparation
- **Chhatra Rana & Ajekigbe Michael:** GitHub repository management and version control

Acknowledgement

We would like to sincerely thank **Infotact Solutions** and our mentors for their constant guidance, support, and encouragement throughout the successful completion of this project.

Date: 18.09.2025

Executive Summary

This report documents a complete set of 26 Snort IDS test cases executed in a lab environment to validate detection coverage. The tests include SQL injection, web exploits, reconnaissance scans, malware download detection, service checks, brute force attempts, and DoS/UDP checks. Each test case contains attacker and victim commands and a placeholder area for inserting Snort alert screenshots as evidence.

Content

4. 4) SQL Injection (Tautology "a"="a") — SID 2000004
5. 5) Metasploit header test — SID 2000100
6. 6) Meterpreter User-Agent test — SID 2000101
7. 7) Nmap SYN scan (ports 1-200) — SID 1000001
8. 8) Port scan (1-1024) — SID 1000013
9. 9) Nmap XMAS scan — SID 1000022
10. 10) Aggressive Nmap Scan (OS, version, scripts, traceroute) — SID 1000024
11. 11) SSH connection attempt — SID 1000002
12. 12) HTTP brute force (multiple rapid requests) — SID 1000014
13. 13) ICMP echo (ping) — SID 1000003
14. 14) HTTP access — SID 1000004
15. 15) HTTPS access — SID 1000005
16. 16) FTP / TELNET / RDP / MySQL / SMTP quick checks — SID Mixed
17. 17) DNS query — SID 1000011
18. 18) SMB check — SID 1000012
19. 19) Malware detection — EXE request/download — SID 2000301 / 400001 / 400002
20. 20) Nikto scan — SID 1000056
21. 21) Dirb scan — SID 1000057
22. 22) XSS raw — SID 1000300
23. 23) XSS encoded — SID 1000302
24. 24) Webshell upload (GET & POST) — SID 1000400 / 1000401 / 1000402
25. 25) DoS/DDoS detection — SID 1000020
26. 26) UDP packet detection — SID 1000015

1) SQL Injection (OR 1=1) — SID 2000001

Attacker (192.168.198.130):

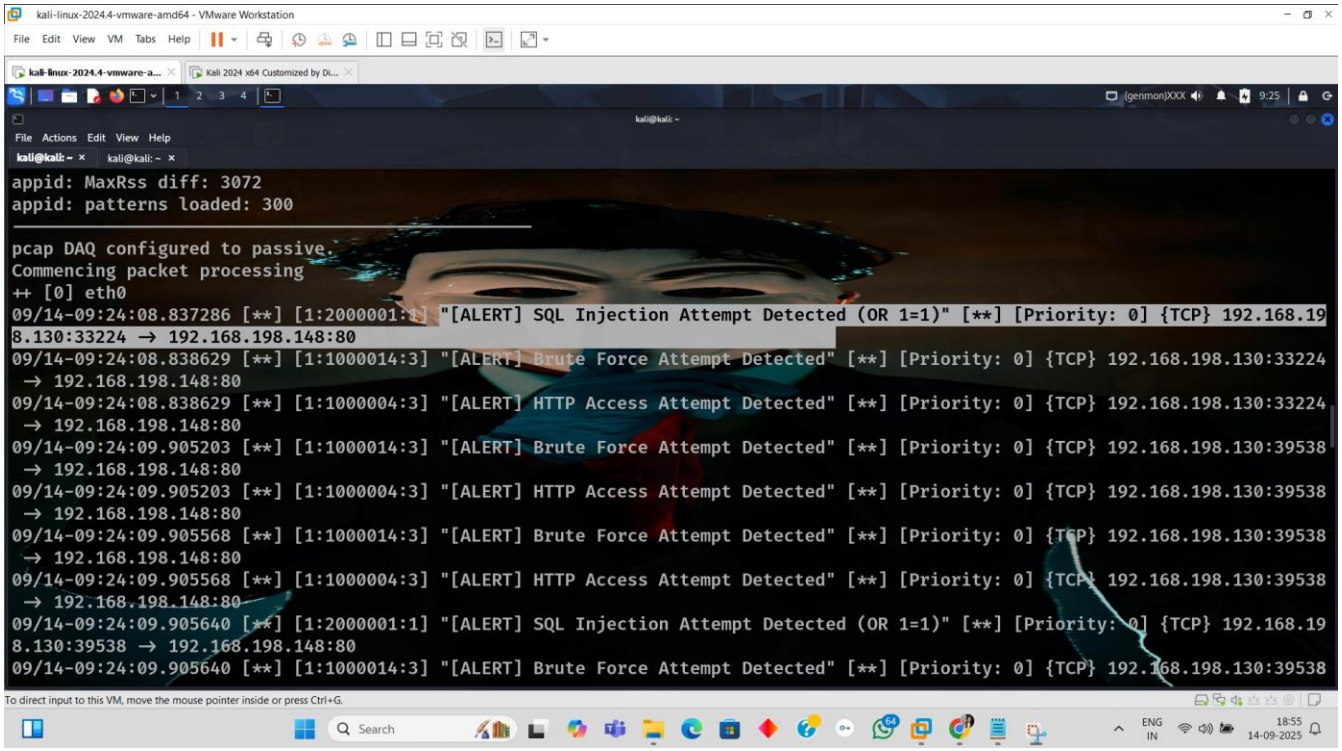
- curl -s -o /dev/null "http://192.168.198.148/page.php?id=%27%20OR%201=1--"
- for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/page.php?id=%27%20OR%201=1--"; done

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



2) SQL Injection (Encoded OR 1=1) — SID 2000002

Attacker (192.168.198.130):

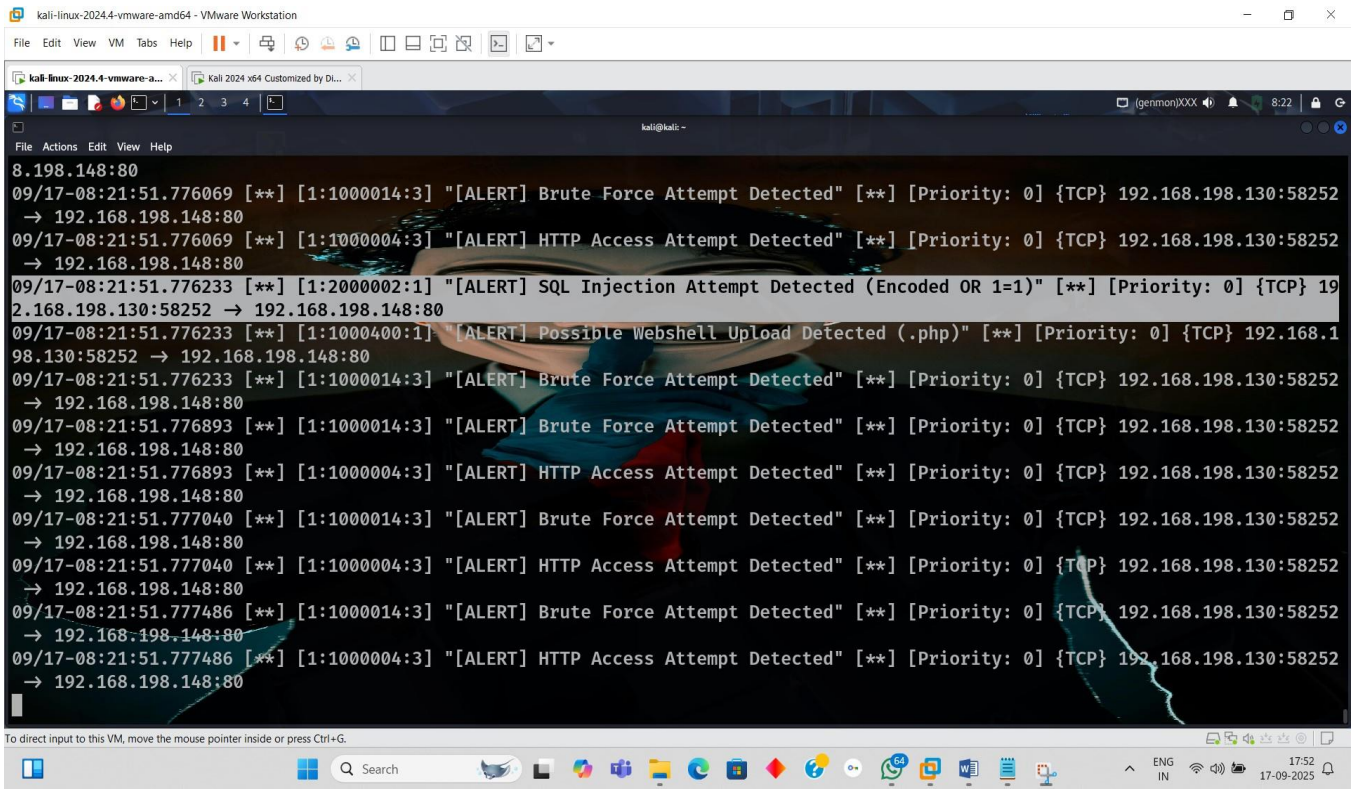
- curl -s -o /dev/null "http://192.168.198.148/page.php?id=%27+OR+1%3D1--"
- for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/page.php?id=%27+OR+1%3D1--"; done

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



3) SQL Injection (UNION SELECT) — SID 2000003

Attacker (192.168.198.130):

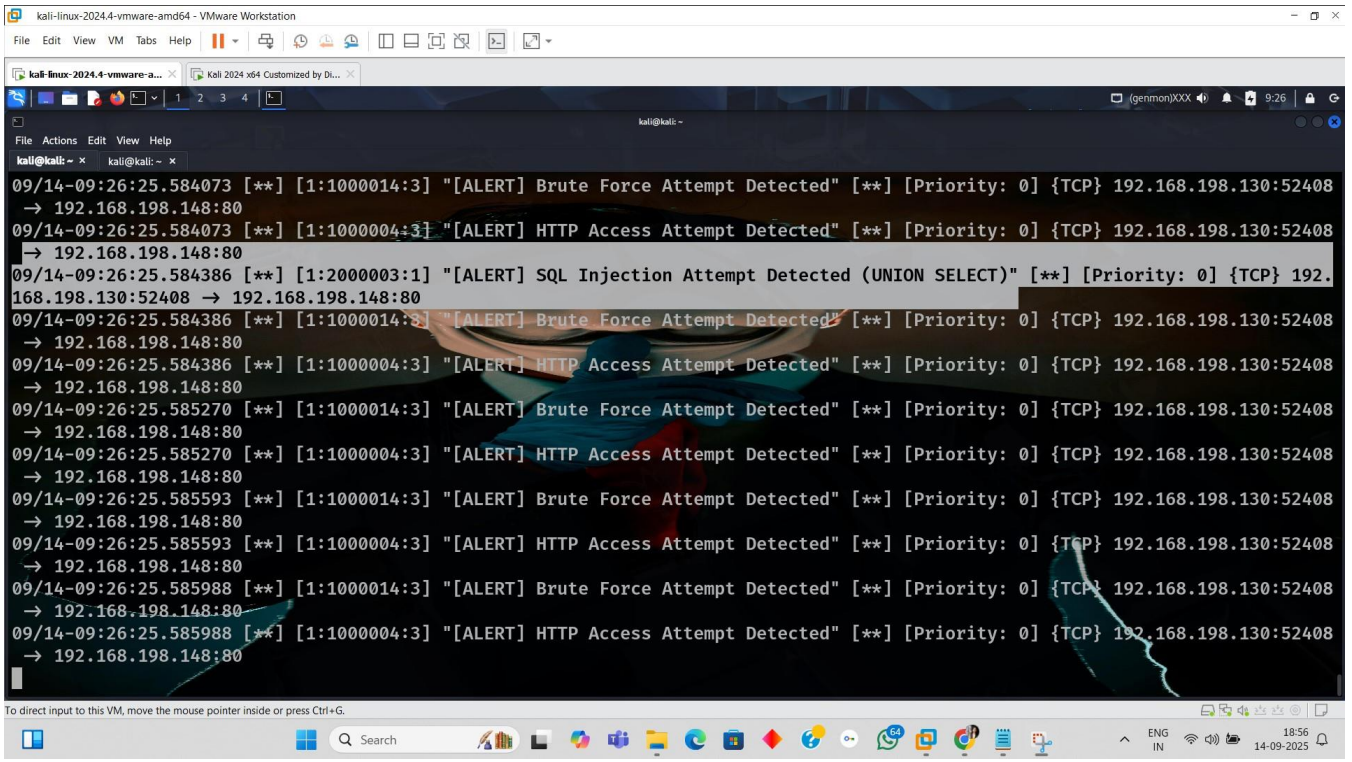
- curl -s -o /dev/null "http://192.168.198.148/search.php?q=UNION+SELECT+null"
- for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/search.php?q=UNION+SELECT+null"; done

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



4) SQL Injection (Tautology "a"="a") — SID 2000004

Attacker (192.168.198.130):

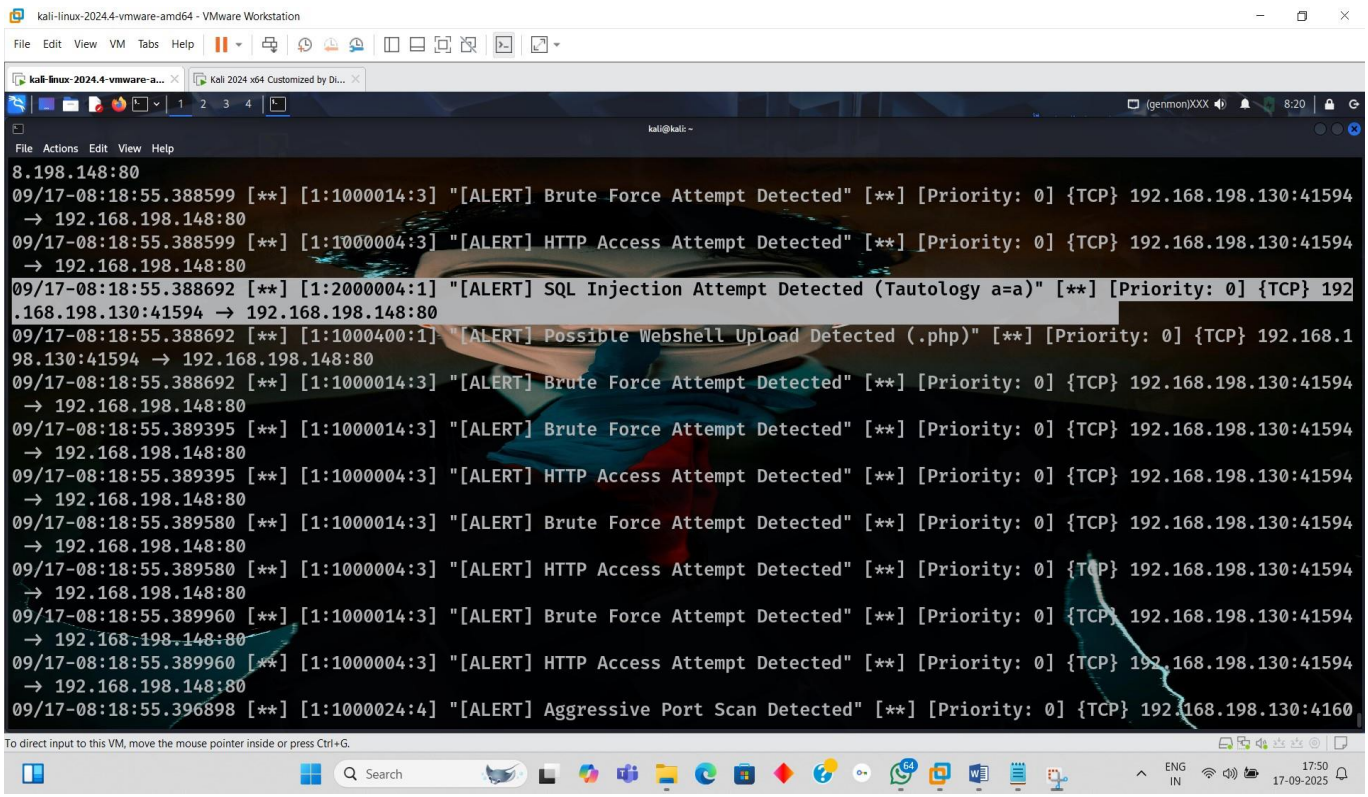
- curl -s -o /dev/null "http://192.168.198.148/index.php?id=%22a%22=%22a%22"
- for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/index.php?id=%22a%22=%22a%22"; done

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



5) Metasploit header test — SID 2000100

Attacker (192.168.198.130):

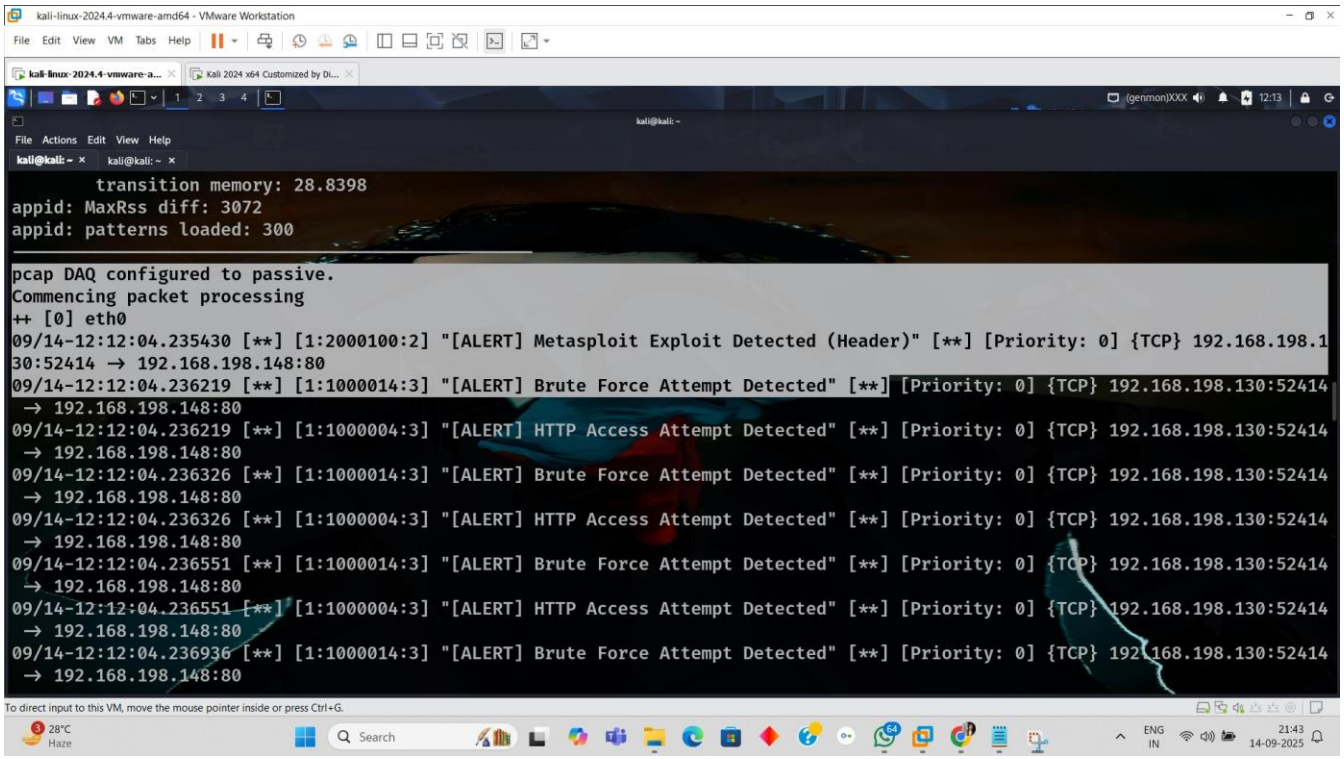
- curl -s -o /dev/null -H "X-Test: Metasploit" http://192.168.198.148/

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



6) Meterpreter User-Agent test — SID 2000101

Attacker (192.168.198.130):

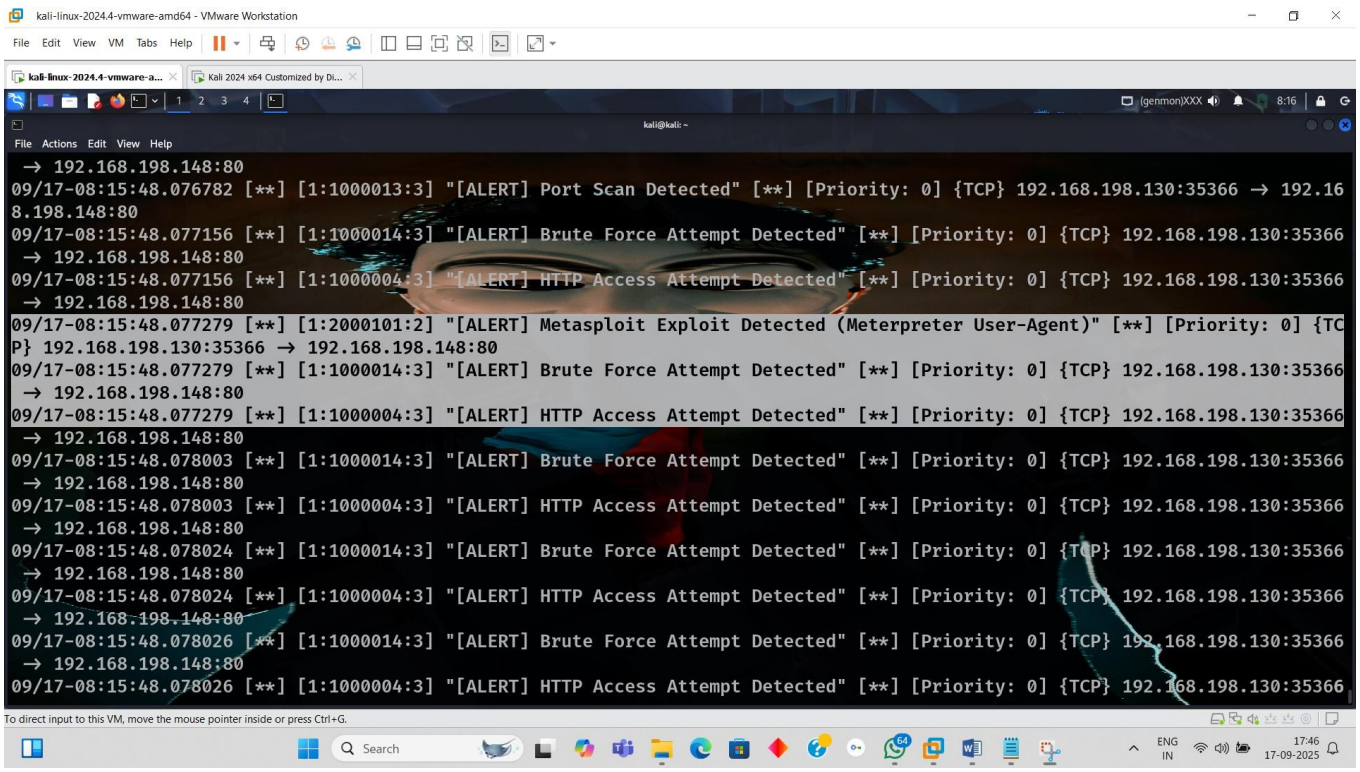
- curl -s -o /dev/null -A "Meterpreter" http://192.168.198.148/

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



7) Nmap SYN scan (ports 1-200) — SID 1000001

Attacker (192.168.198.130):

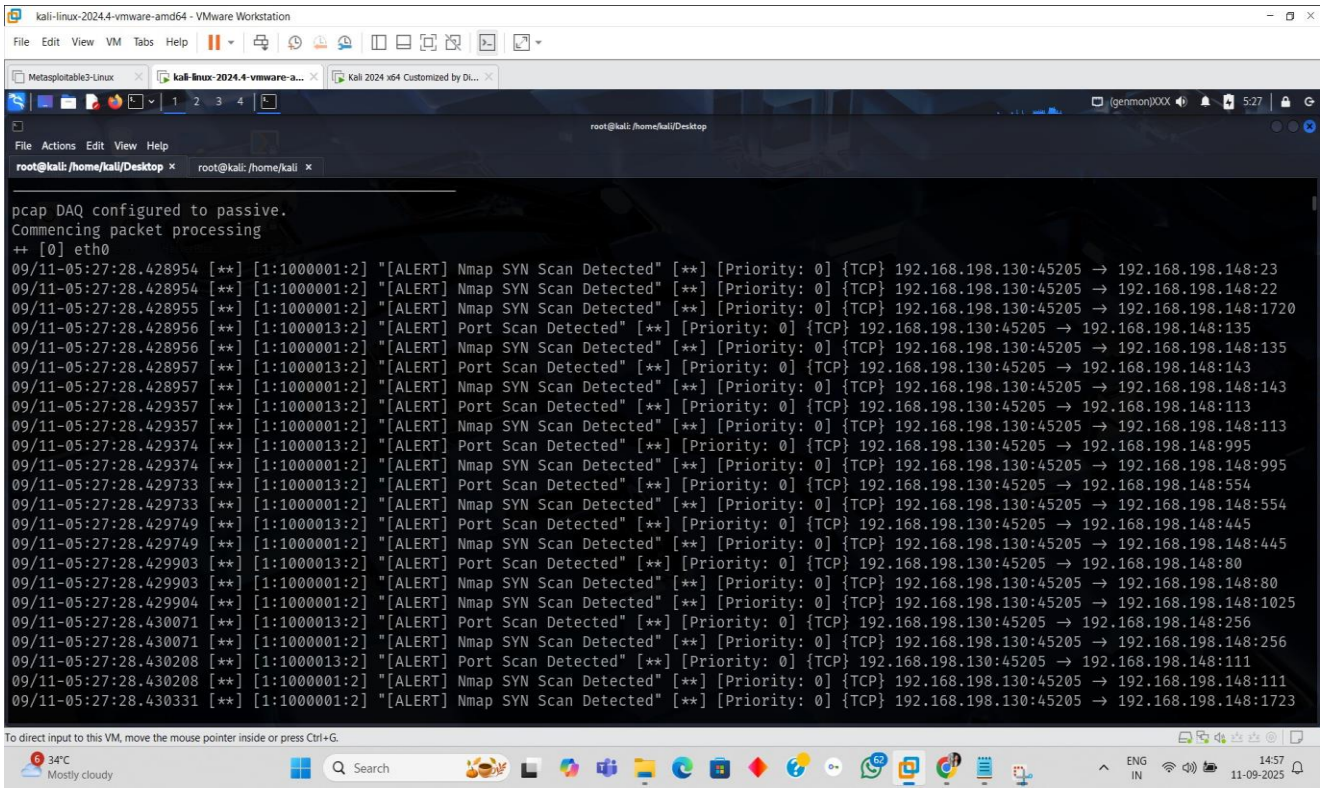
- sudo nmap -sS -p 1-200 192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



8) Port scan (1-1024) — SID 1000013

Attacker (192.168.198.130):

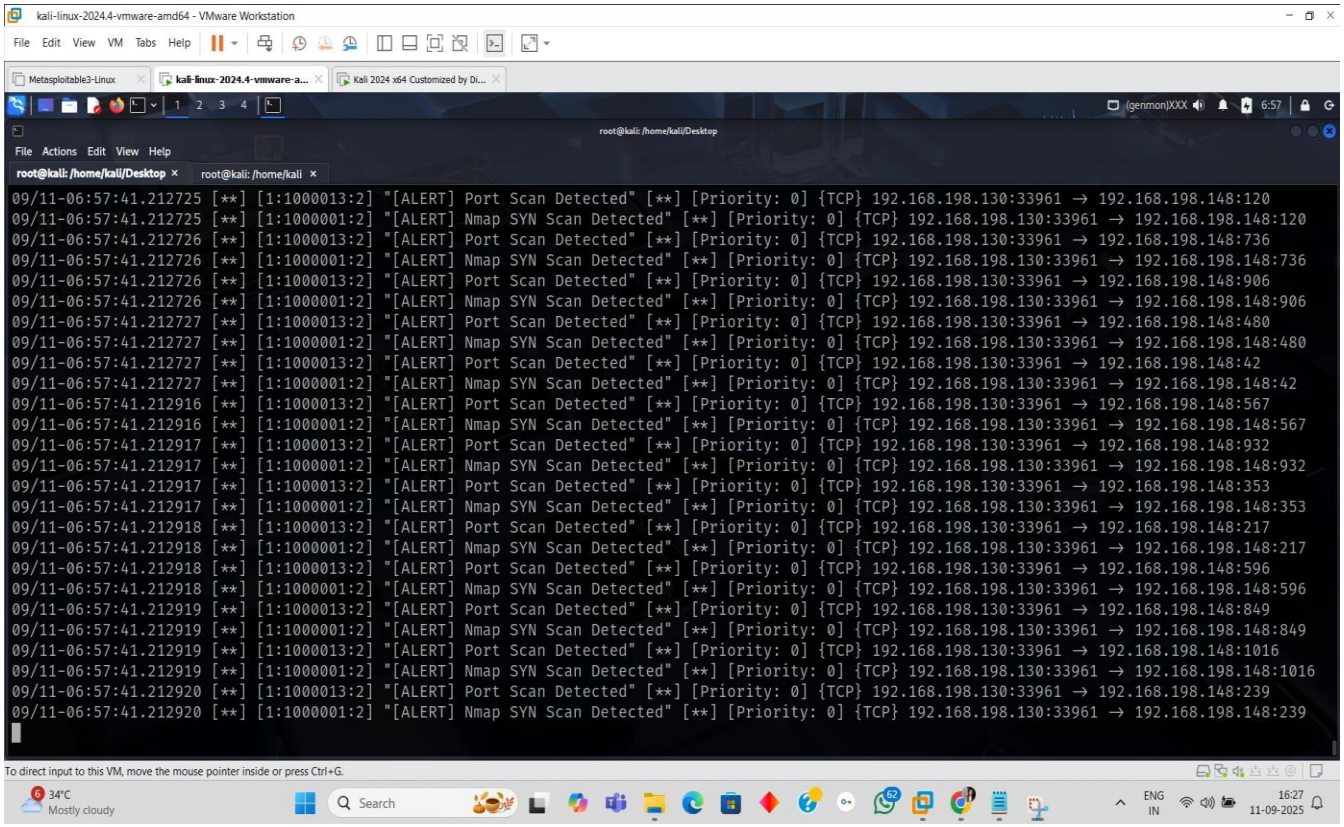
- sudo nmap -sS -p1-1024 192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



9) Nmap XMAS scan — SID 1000022

Attacker (192.168.198.130):

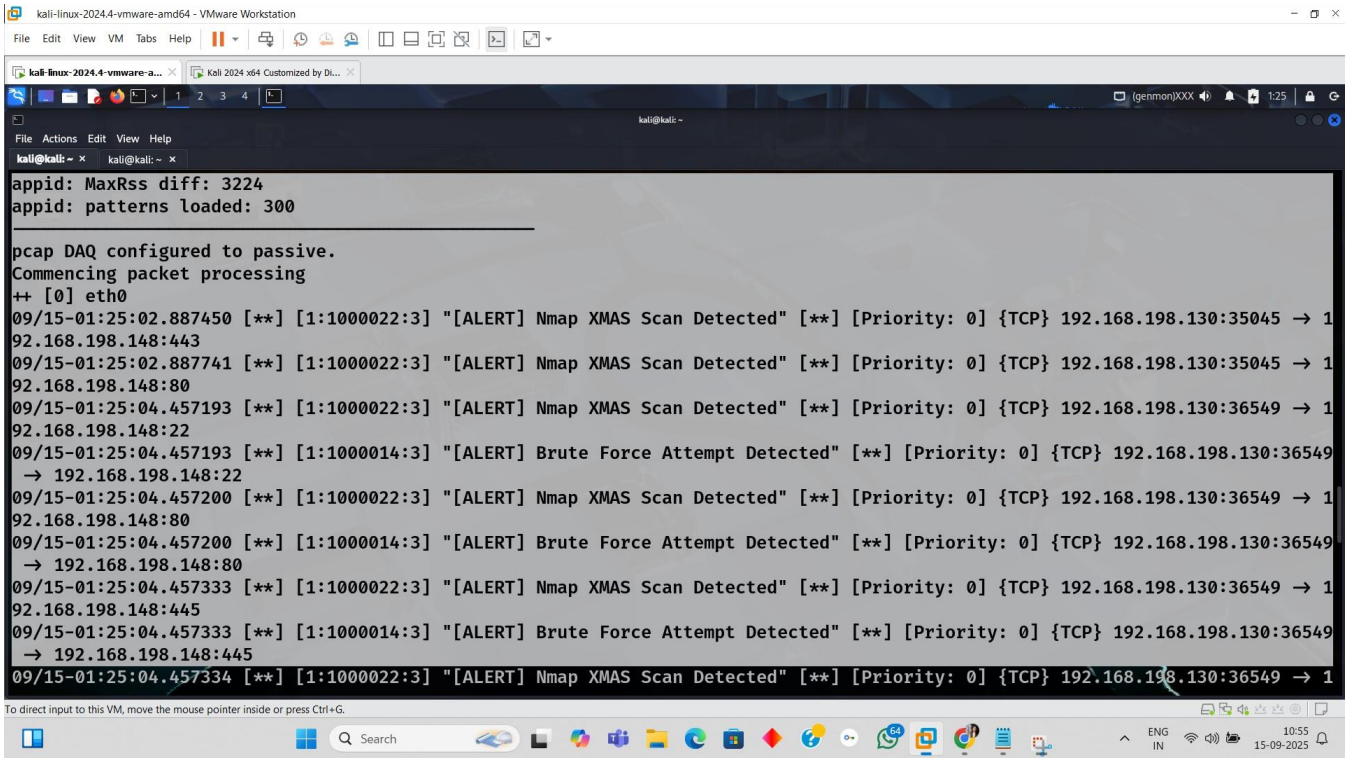
- sudo nmap -sX -p1-200 192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



10) Aggressive Nmap Scan (OS, version, scripts, traceroute) — SID 1000024

Attacker (192.168.198.130):

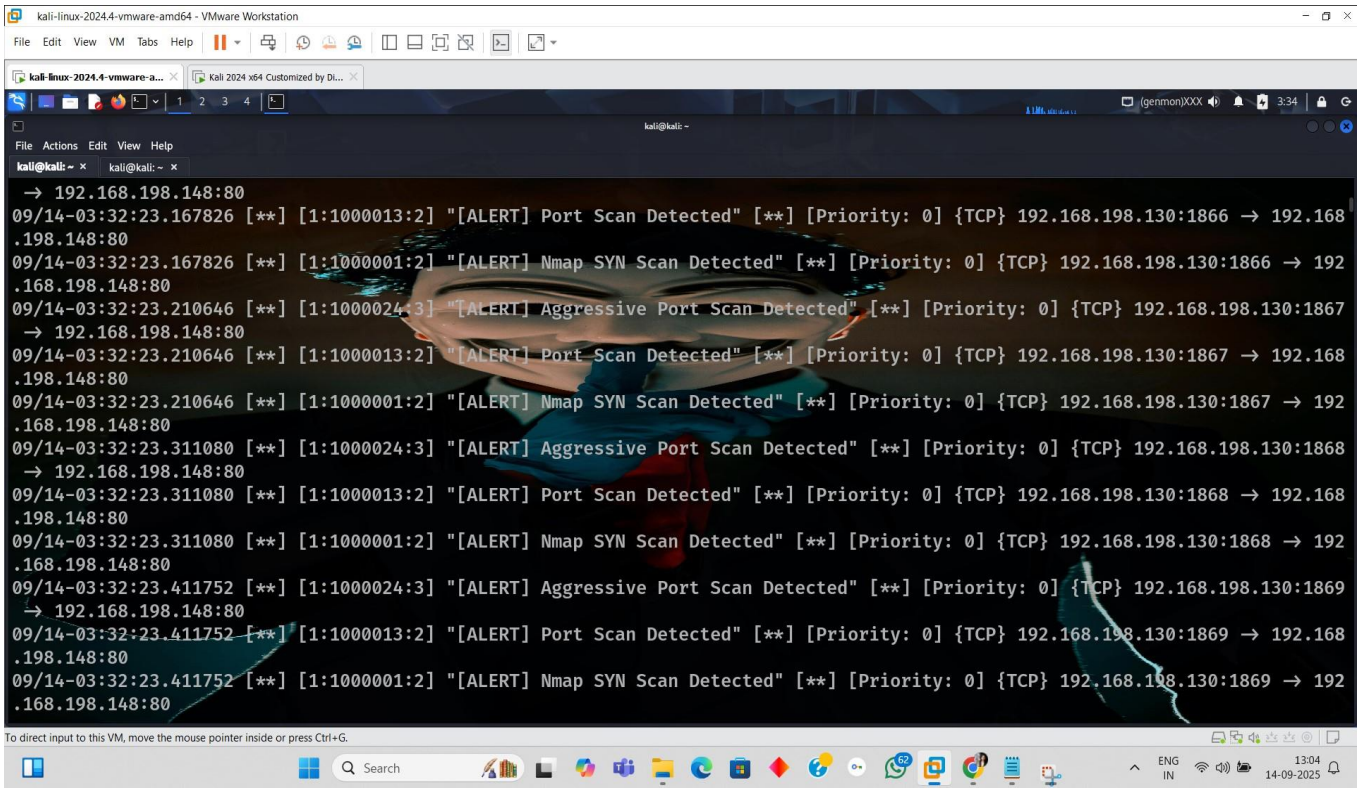
- sudo nmap -A 192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



11) SSH connection attempt — SID 1000002

Attacker (192.168.198.130):

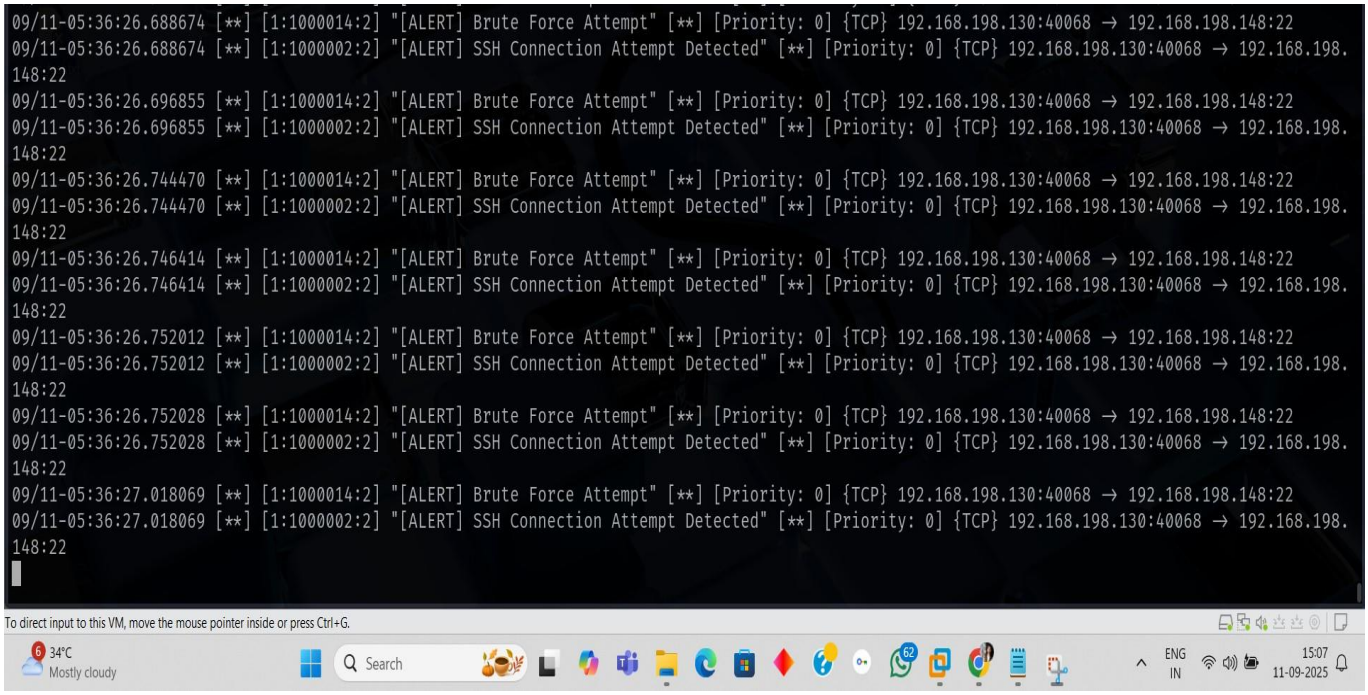
- nc -vz 192.168.198.148 22 || true

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



12) HTTP brute force (multiple rapid requests) — SID 1000014

Attacker (192.168.198.130):

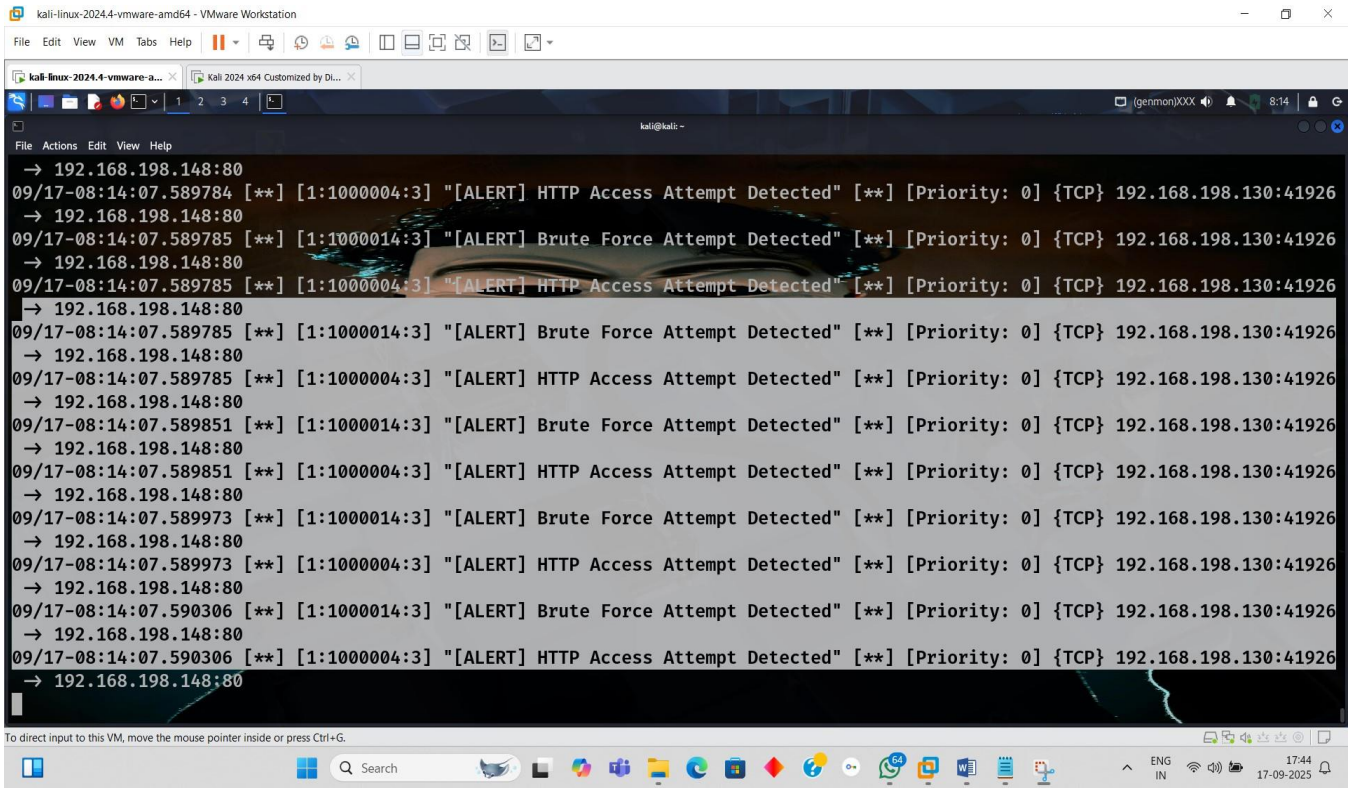
- for i in {1..7}; do curl -s -o /dev/null http://192.168.198.148/; done

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



13) ICMP echo (ping) — SID 1000003

Attacker (192.168.198.130):

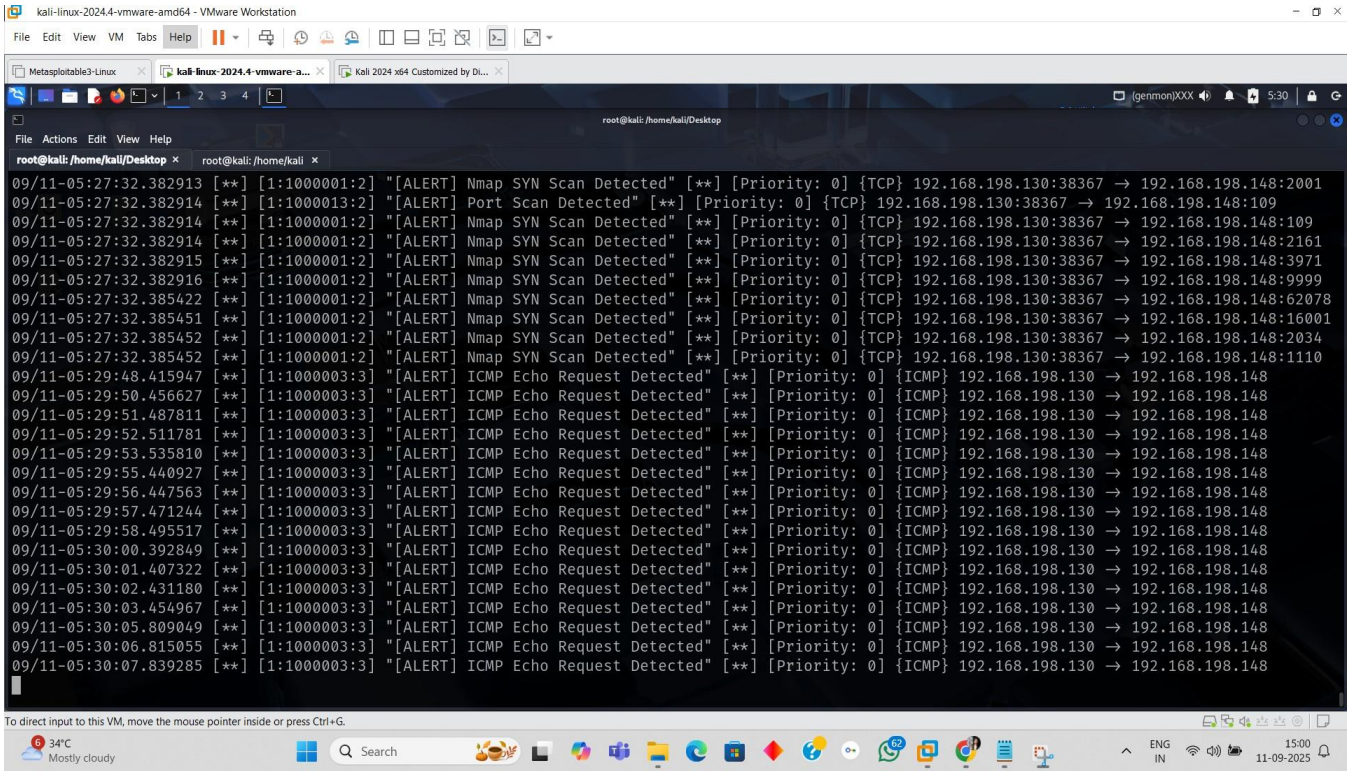
- ping -c 8 192.168.198.148
- sudo hping3 --icmp -i u1000 -c 10 192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



14) HTTP access — SID 1000004

Attacker (192.168.198.130):

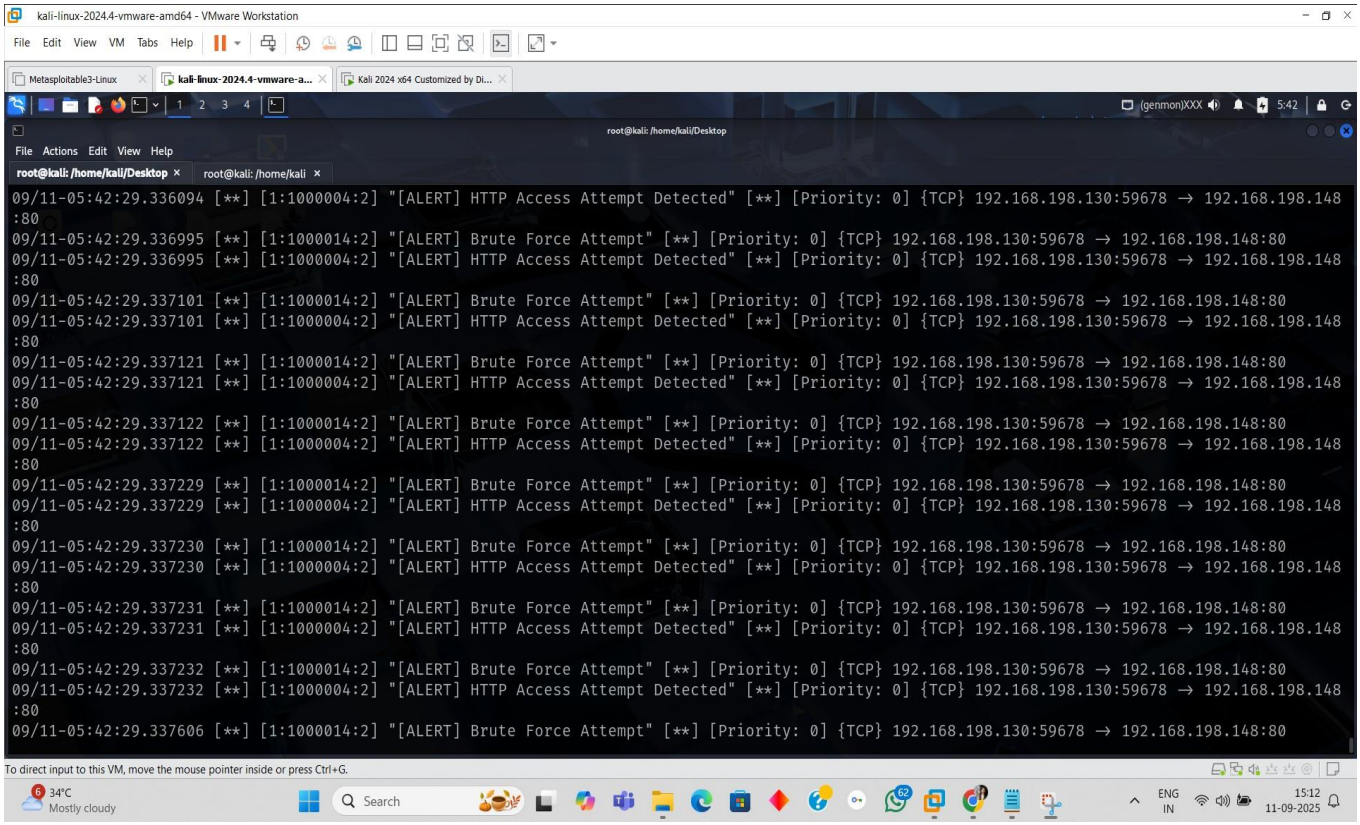
- curl -s -o /dev/null http://192.168.198.148/

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



15) HTTPS access — SID 1000005

Attacker (192.168.198.130):

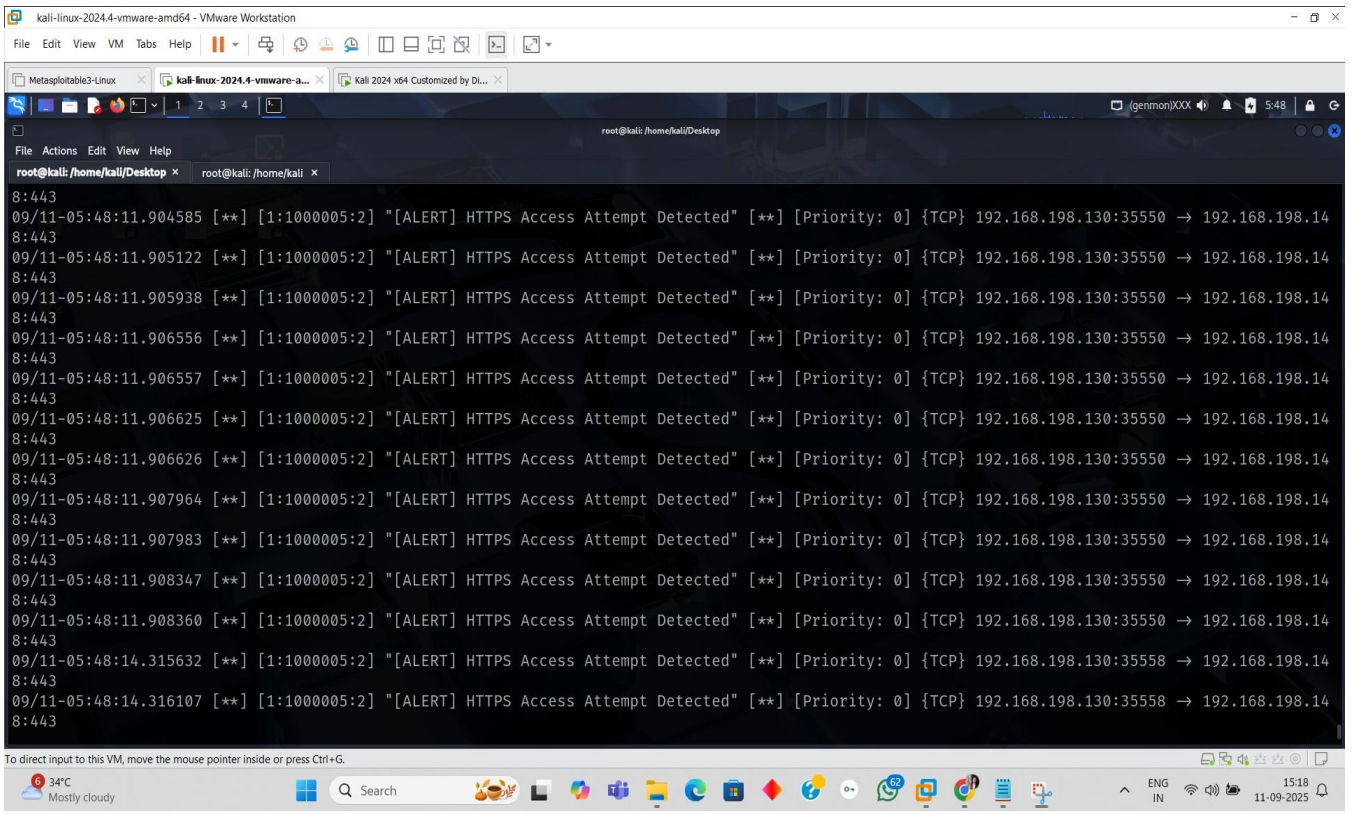
- nc -vz 192.168.198.148 443
- curl -k -s -o /dev/null https://192.168.198.148/

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



16) FTP / TELNET / RDP / MySQL / SMTP quick checks — SID Mixed

Attacker (192.168.198.130):

- nc -vz 192.168.198.148 21 # FTP
- nc -vz 192.168.198.148 23 # TELNET
- nc -vz 192.168.198.148 3389 # RDP
- mysql -h 192.168.198.148 -u testuser -ptestpass || true
- nc -vz 192.168.198.148 25 # SMTP

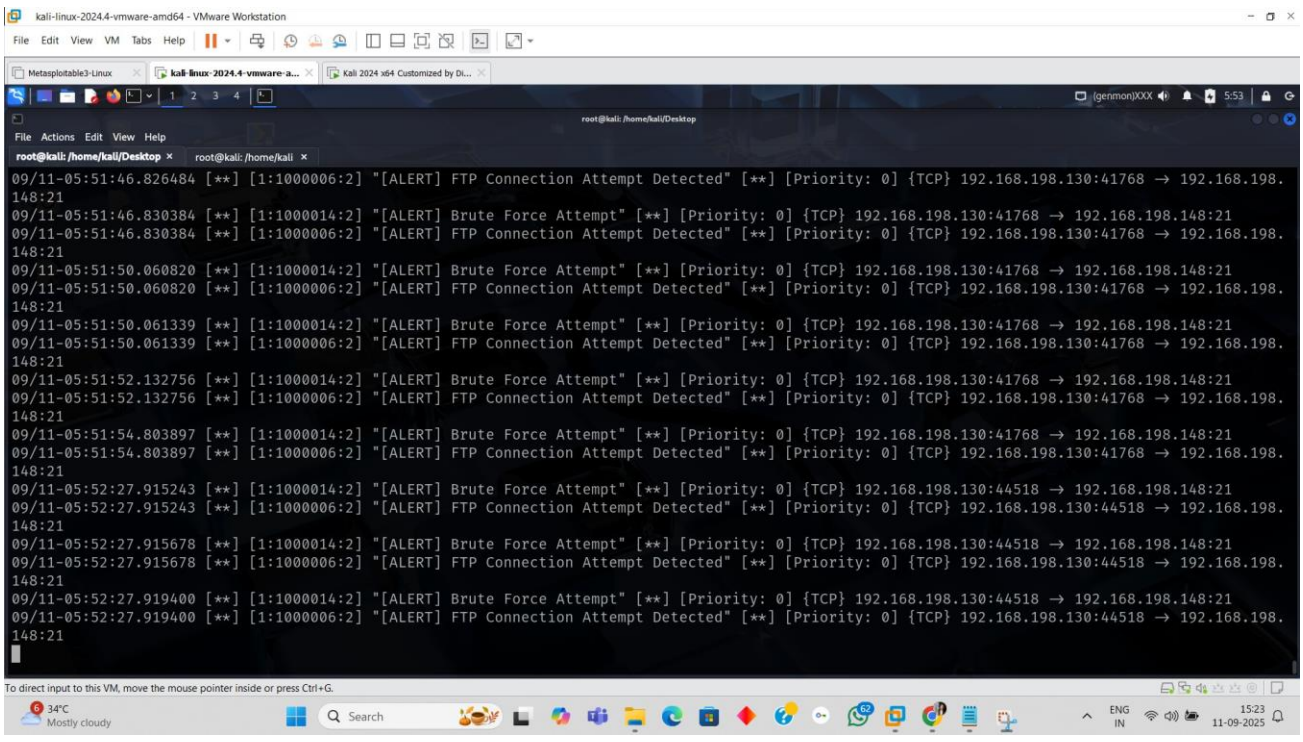
Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

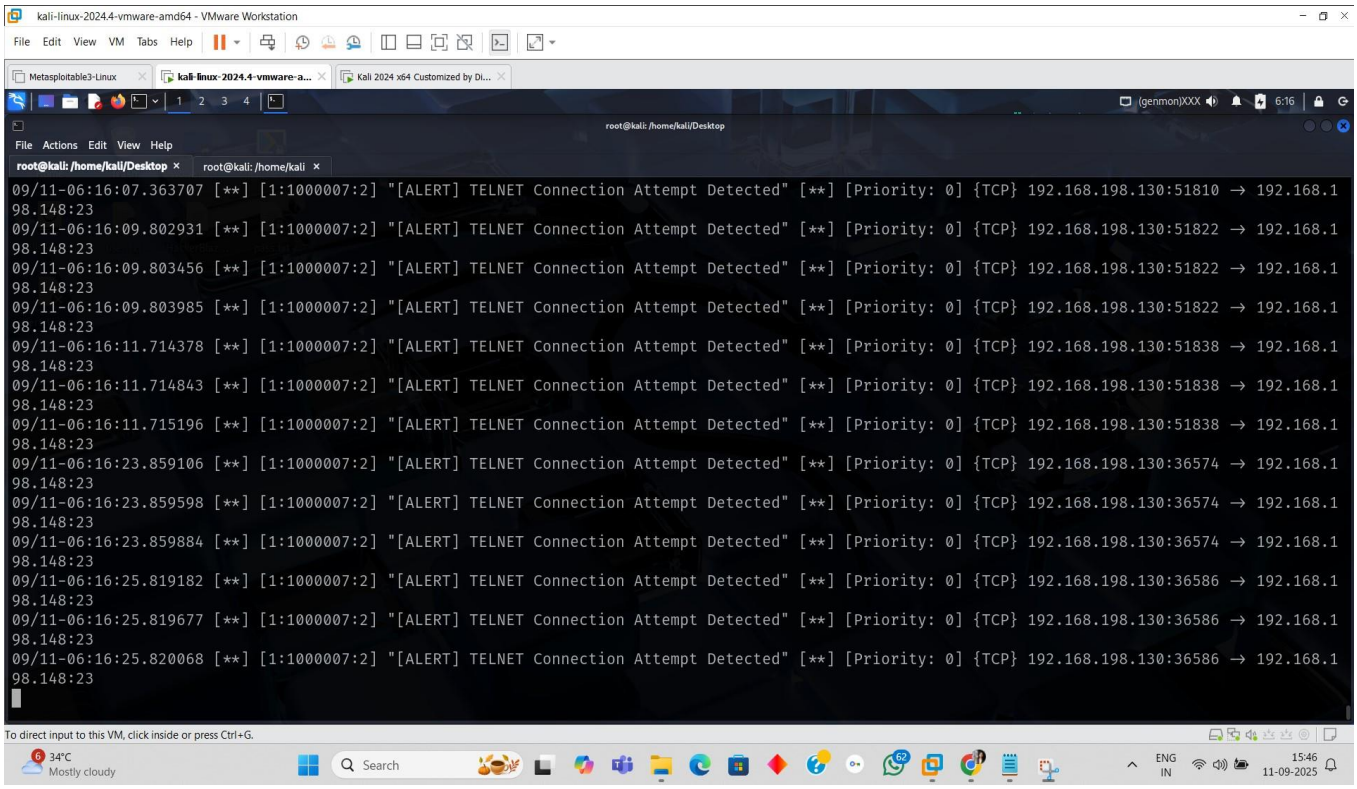
Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):

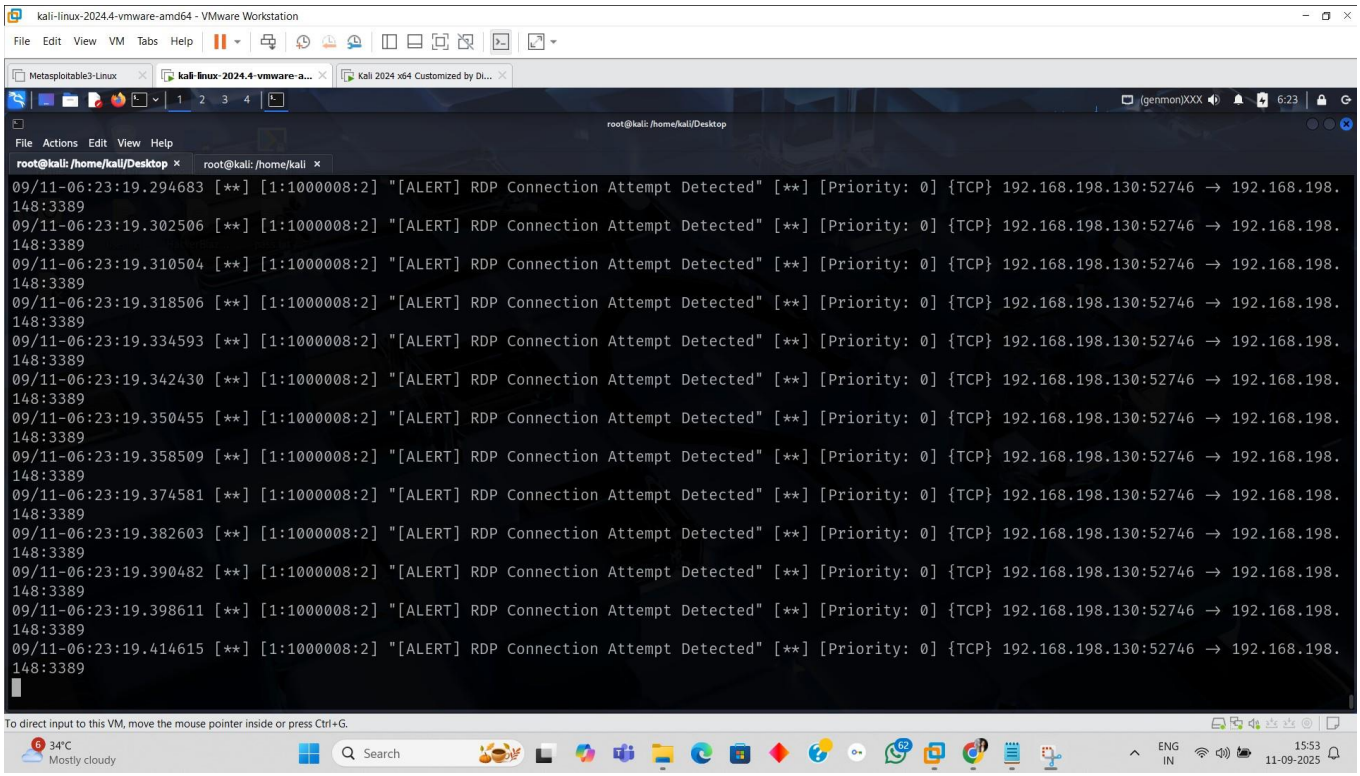
Ftp Detected Poc –



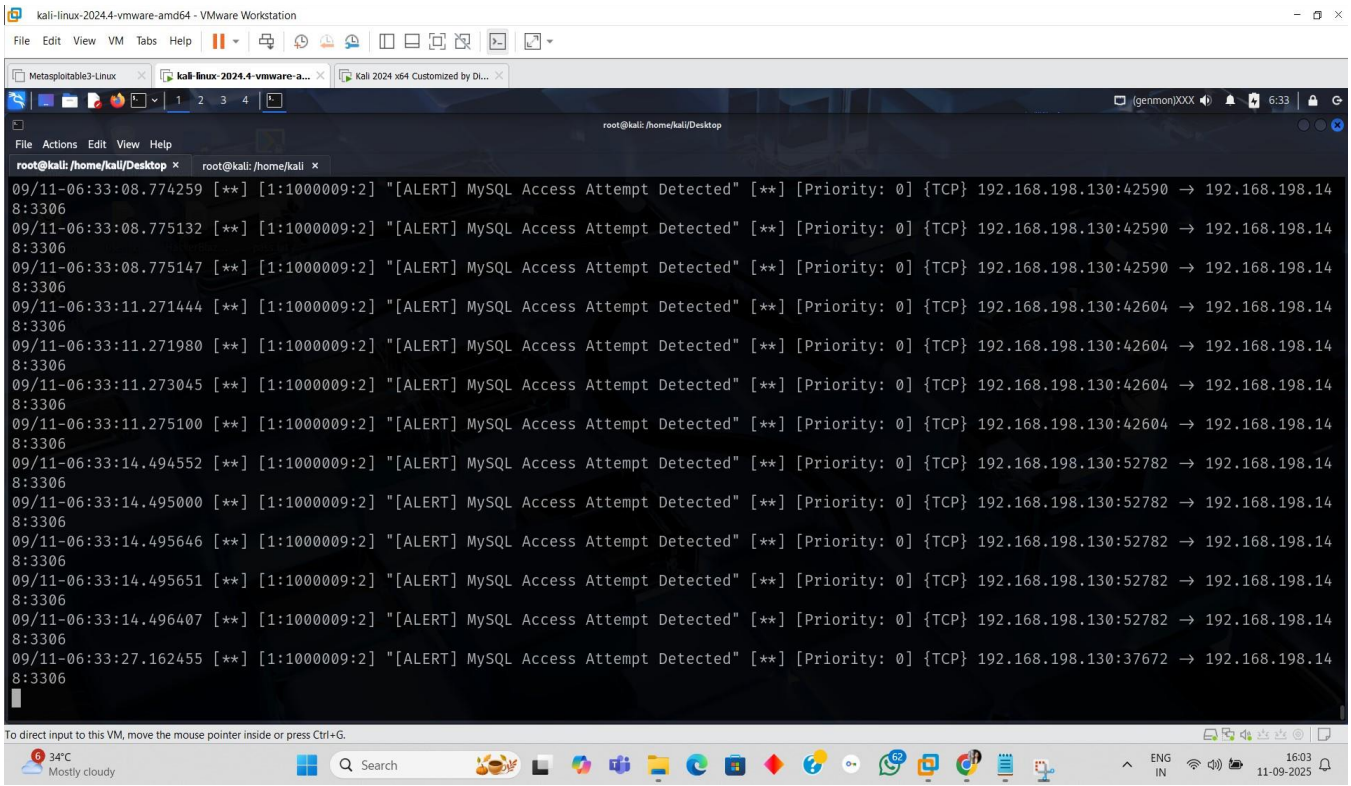
Telnet Detected Poc –



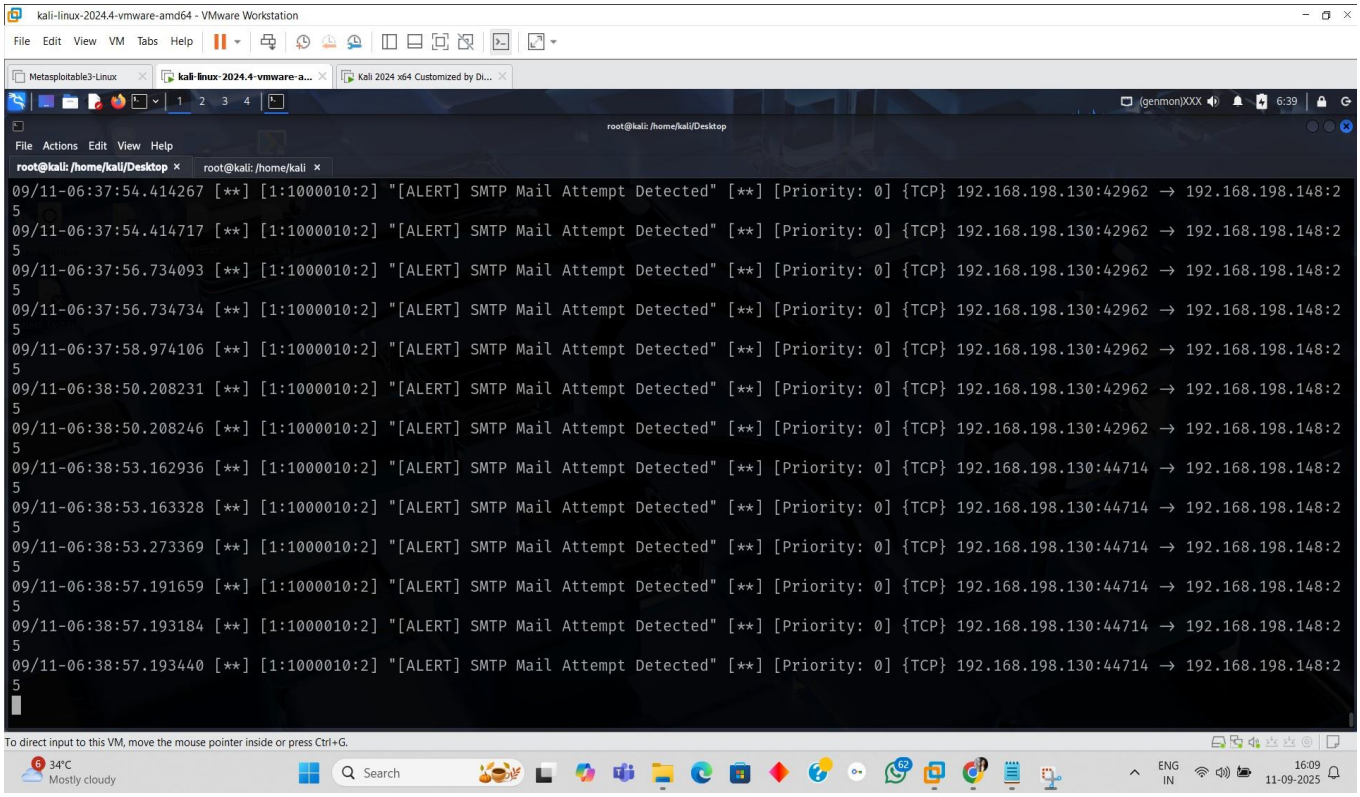
Rdp detected Poc –



Mysql detected Poc –



Smtp Detected Poc –



17) DNS query — SID 1000011

Attacker (192.168.198.130):

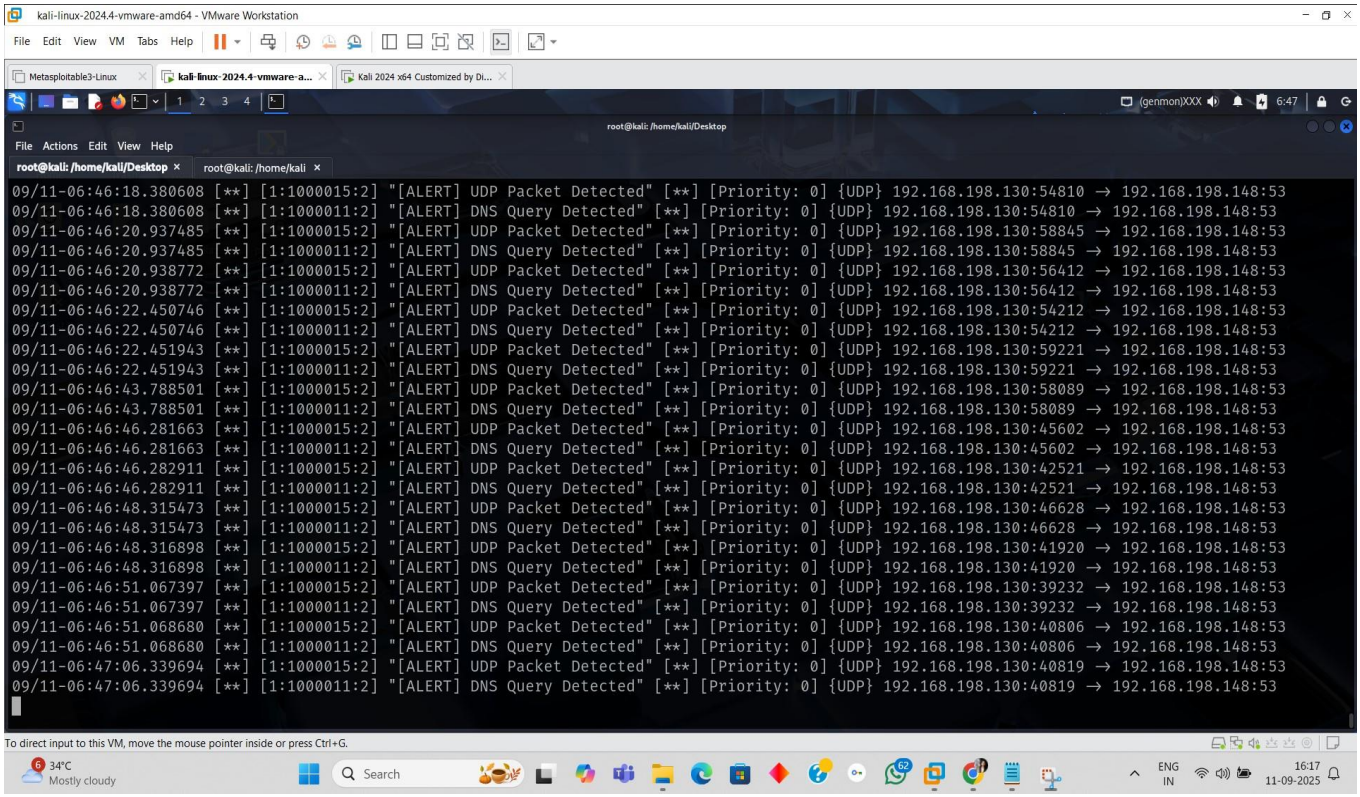
- dig @8.8.8.8 example.com || true

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (insert Snort alert screenshot here):



18) SMB check — SID 1000012

Attacker (192.168.198.130):

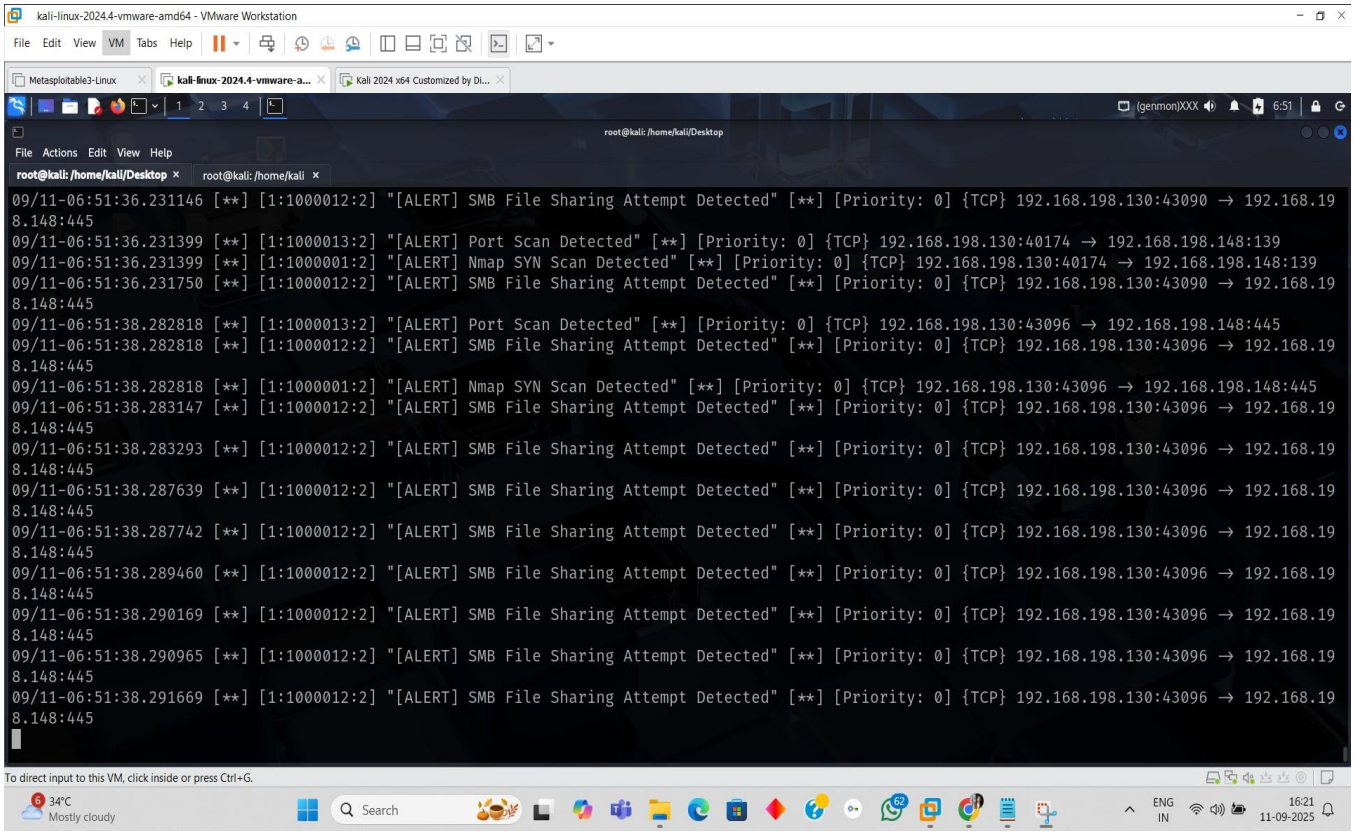
- nc -vz 192.168.198.148 445
- smbclient -L //192.168.198.148 -N || true

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



19) Malware detection — EXE request — SID 2000301

Attacker (192.168.198.130):

- Attacker (prepare & serve):
- dd if=/dev/zero of=/home/attacker/bigtest.exe bs=1K count=50
- printf 'MZ' | dd of=/home/attacker/bigtest.exe conv=notrunc
- cd /home/attacker
- python3 -m http.server 80 &
- Victim (download):

- curl -s -o /dev/null http://192.168.198.130/bigtest.exe
- curl -I http://192.168.198.130/bigtest.exe
- Expected alerts: SID 2000301 (EXE Request), SID 400001 (MIME header), SID 400002 (MZ payload)

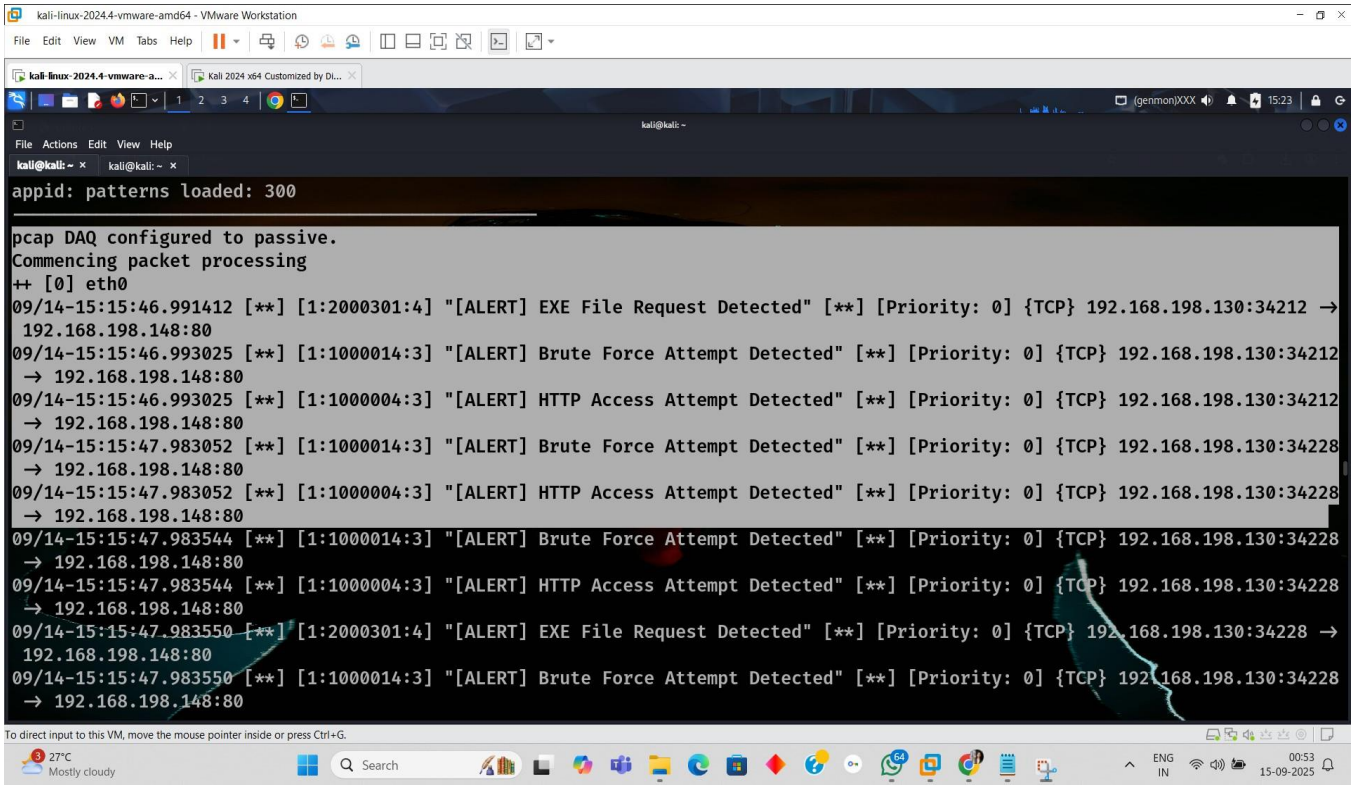
Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):

EXE Request Detected Poc –



20) Nikto scan — SID 1000056

Attacker (192.168.198.130):

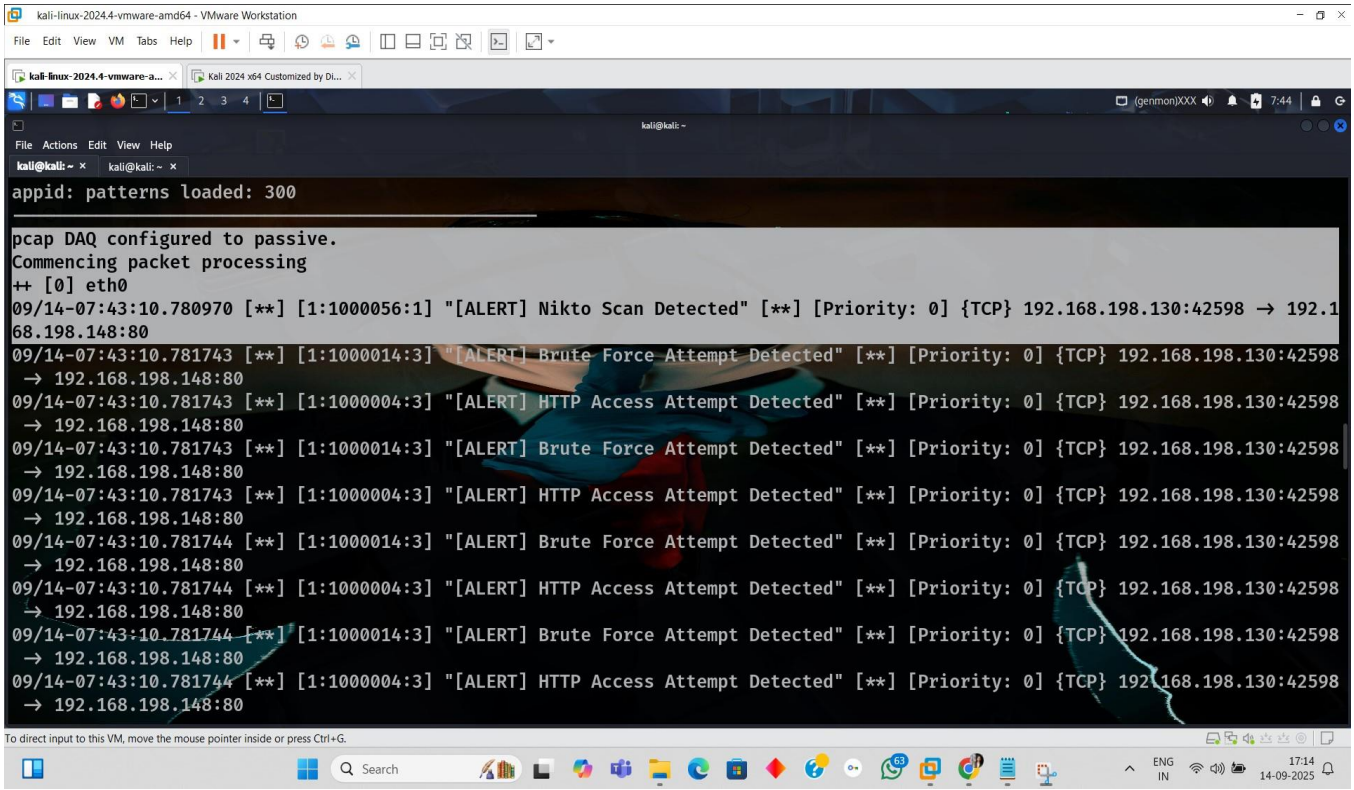
- curl -s -o /dev/null -A "Nikto/2.1.6" http://192.168.198.148/
- nikto -h http://192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



21) Dirb scan — SID 1000057

Attacker (192.168.198.130):

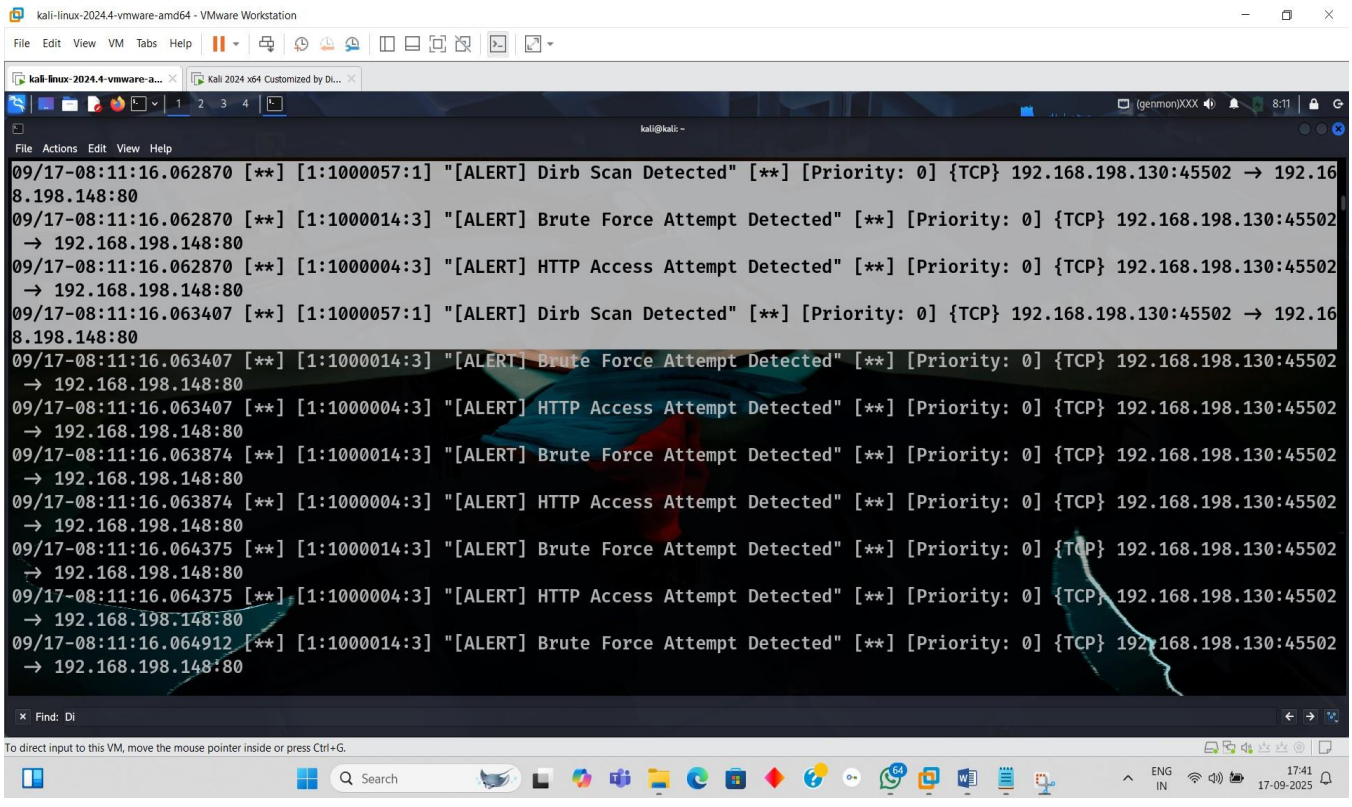
- curl -s -o /dev/null -A "dirb/2.22" http://192.168.198.148/
- dirb http://192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



22) XSS raw — SID 1000300

Attacker (192.168.198.130):

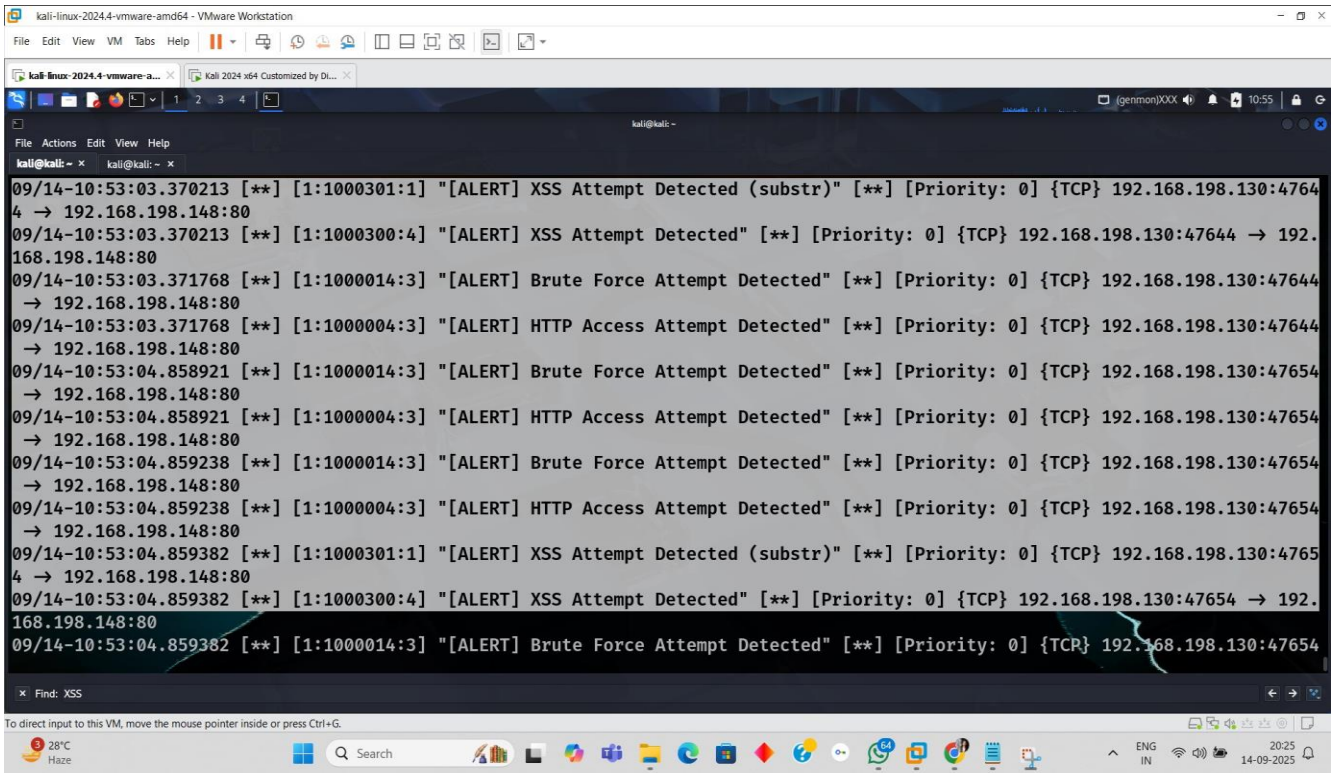
- curl -s -o /dev/null "http://192.168.198.148/index.php?q=<script>alert(1)</script>"
- for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/index.php?q=<script>alert(1)</script>"; done

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



23) XSS encoded — SID 1000302

Attacker (192.168.198.130):

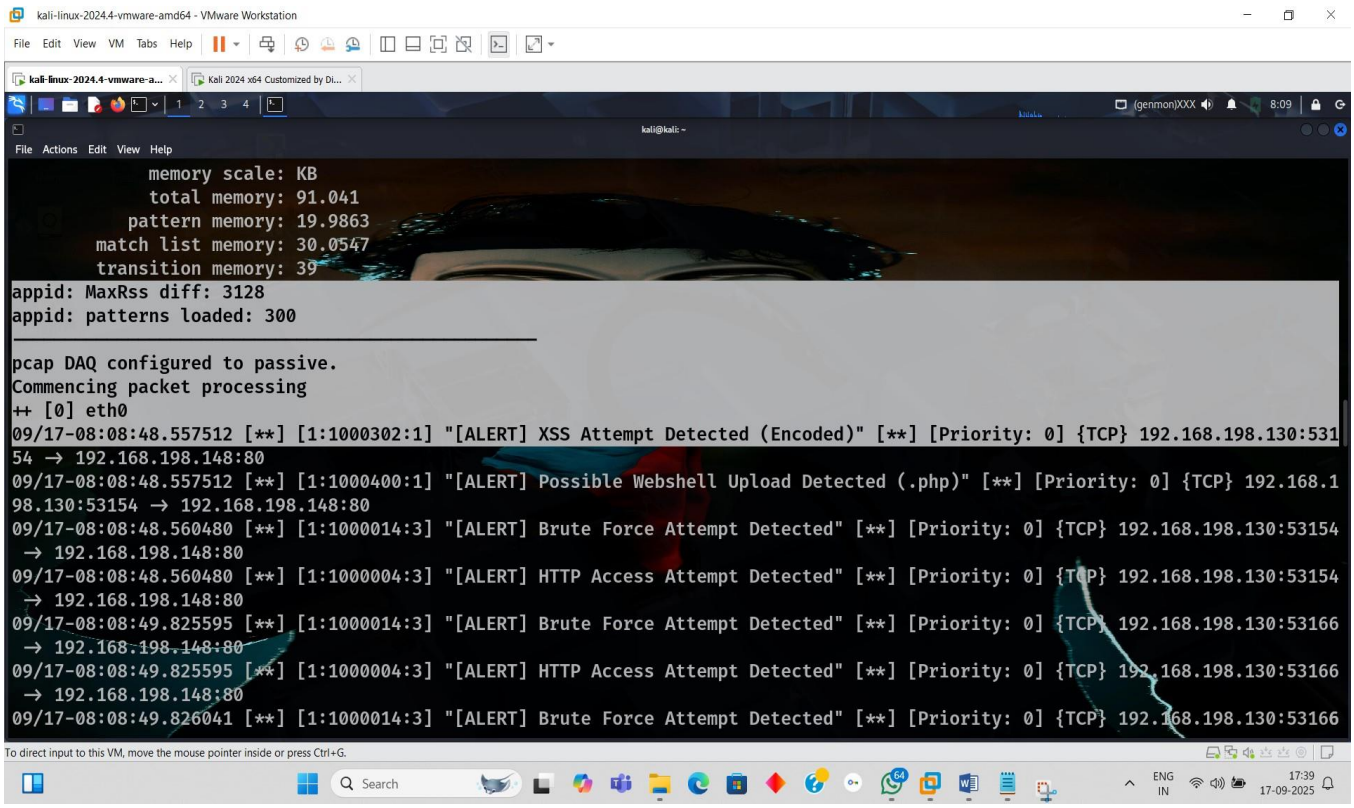
- curl -s -o /dev/null "http://192.168.198.148/index.php?q=%3Cscript%3Ealert(1)%3C%2Fscript%3E"
- for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/index.php?q=%3Cscript%3Ealert(1)%3C%2Fscript%3E"; done

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



24) Webshell upload (GET & POST) — SID 1000400 / 1000401 / 1000402

Attacker (192.168.198.130):

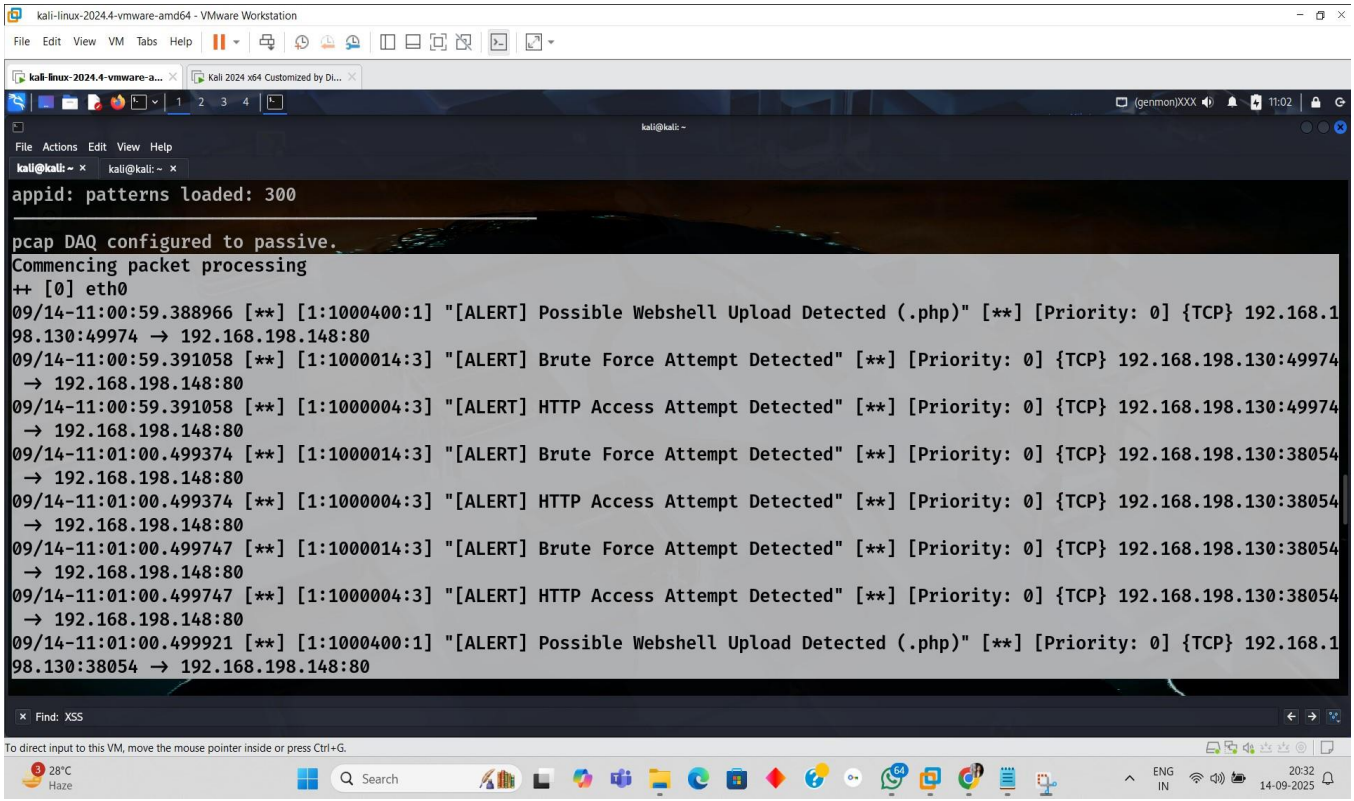
- curl -s -o /dev/null "http://192.168.198.148/upload.php?file=shell.php"
- printf "<?php echo 'ok';?>" > shell.php
- curl -s -o /dev/null -F "file=@shell.php" http://192.168.198.148/upload.php

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



25) DoS/DDoS detection — SID 1000020

Attacker (192.168.198.130):

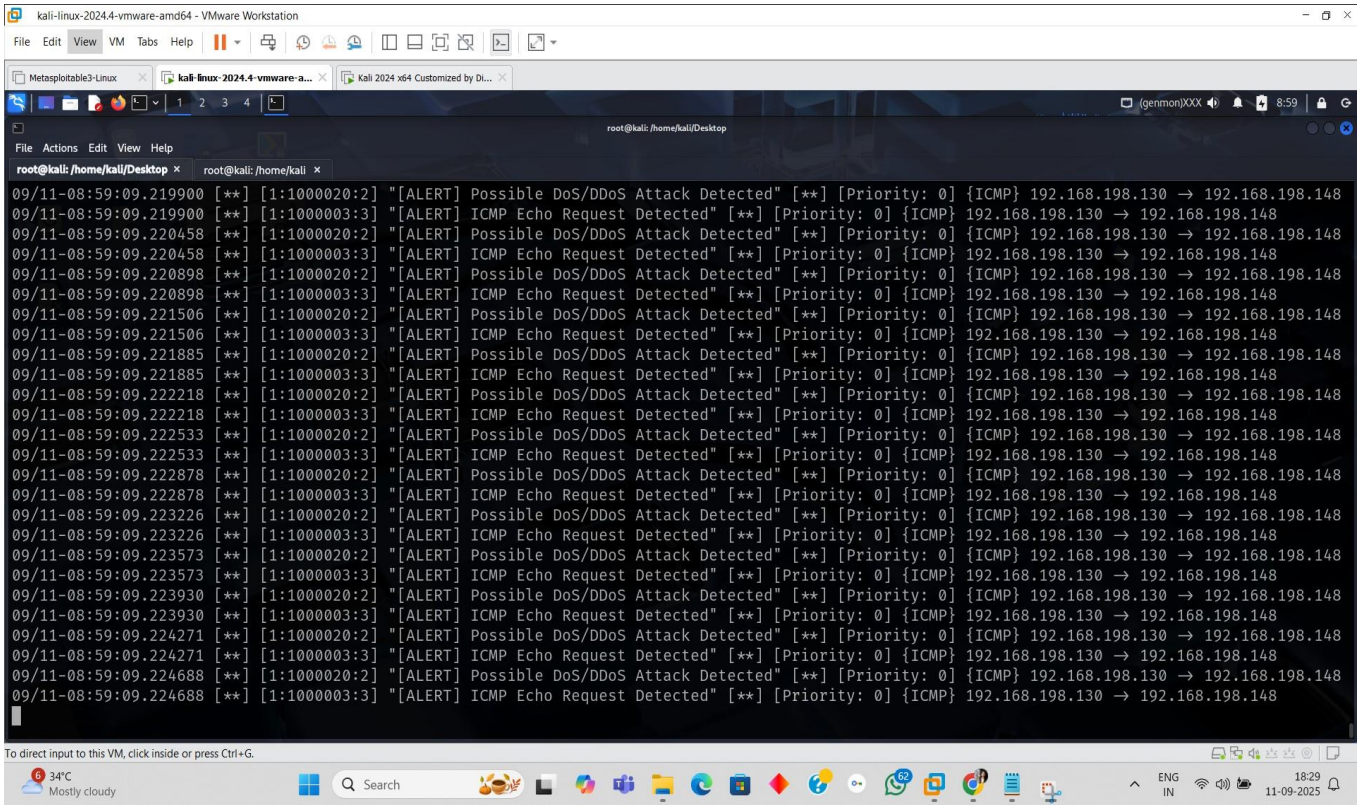
- ping -c 10 192.168.198.148
- sudo hping3 --icmp -i u1000 -c 10 192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



26) UDP packet detection — SID 1000015

Attacker (192.168.198.130):

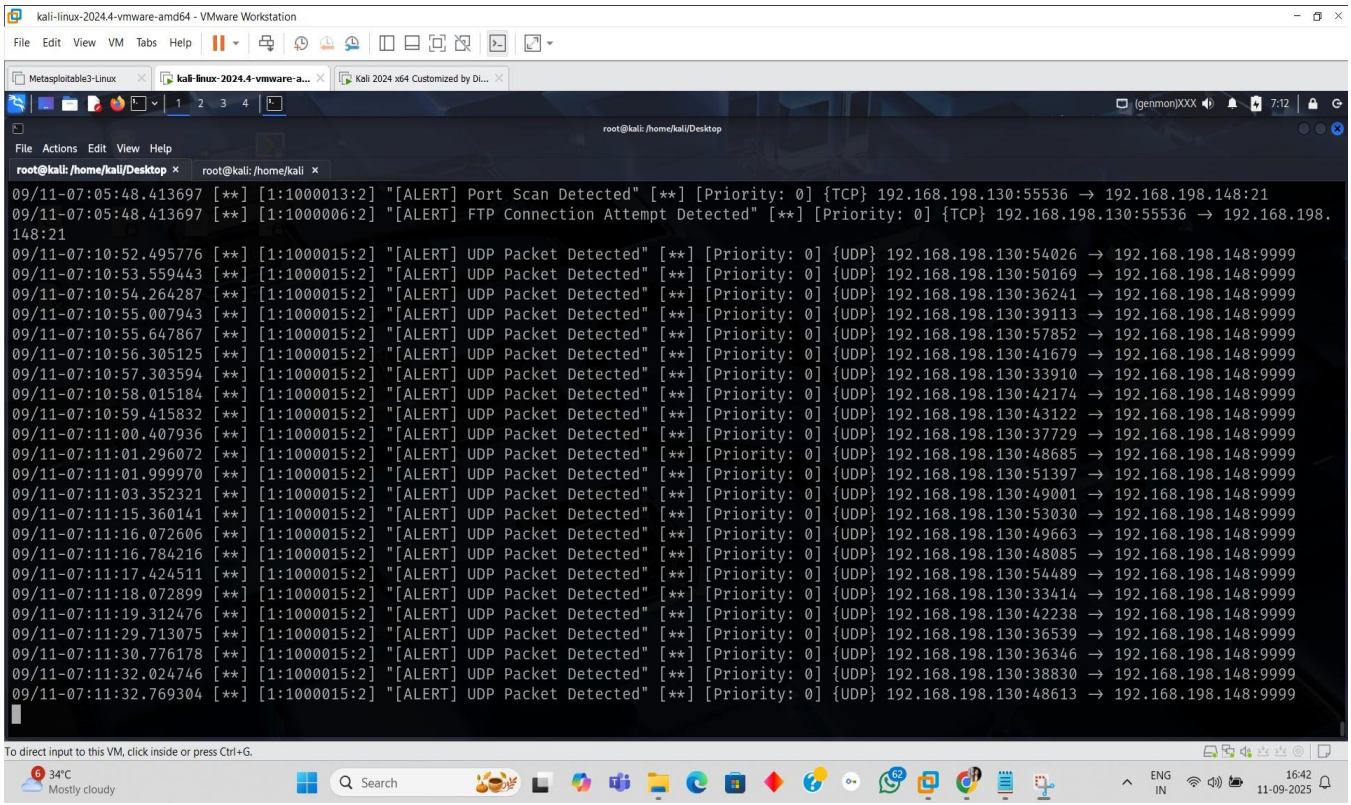
- sudo hping3 --udp -p 12345 -c 20 -i u1000 192.168.198.148

Victim / Snort host (192.168.198.148):

- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast

Note: If alert does not appear on first attempt, run the command 5–6 times continuously to ensure detection.

Screenshot placeholder (Snort alert screenshot here):



Conclusion

This project involved building and testing an advanced Snort NIDS playbook for Infotact Solution. A total of 26 rules were validated covering SQL injection, XSS, reconnaissance scans, brute force, service exploitation attempts, malware detection, and DoS/UDP scenarios. The playbook provides clear attacker and victim commands, retry guidance, and placeholders for evidence

collection. This ensures a professional, comprehensive, and practical demonstration of Snort's detection capabilities for real-world threats in a lab environment.