

# 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

- 1) SQL Injection (OR 1=1) — SID 2000001
- 2) SQL Injection (Encoded OR 1=1) — SID 2000002
- 3) SQL Injection (UNION SELECT) — SID 2000003

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):*

---

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window titled 'kali@kali: ~' displays Snort log output. The log shows multiple alerts for SQL Injection and Brute Force attempts. The alerts are triggered by TCP connections from various IP addresses (e.g., 192.168.198.148, 192.168.198.130) to port 80. The log entries include timestamps, source and destination IP addresses, and detailed alert descriptions.

```

appid: MaxRss diff: 3072
appid: patterns loaded: 300

pcap DAQ configured to passive
Commencing packet processing
++ [0] eth0
09/14-09:24:08.837286 [**] [1:2000001:1] "[ALERT] SQL Injection Attempt Detected (OR 1=1)" [**] [Priority: 0] {TCP} 192.168.198.130:33224 → 192.168.198.148:80
09/14-09:24:08.838629 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33224 → 192.168.198.148:80
09/14-09:24:08.838629 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33224 → 192.168.198.148:80
09/14-09:24:09.905203 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:39538 → 192.168.198.148:80
09/14-09:24:09.905203 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:39538 → 192.168.198.148:80
09/14-09:24:09.905568 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:39538 → 192.168.198.148:80
09/14-09:24:09.905568 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:39538 → 192.168.198.148:80
09/14-09:24:09.905640 [**] [1:2000001:1] "[ALERT] SQL Injection Attempt Detected (OR 1=1)" [**] [Priority: 0] {TCP} 192.168.198.130:39538 → 192.168.198.148:80
09/14-09:24:09.905640 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:39538

```

## 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):**

kali-linux-2024.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali ~

8.198.148:80

09/17-08:21:51.776069 [\*\*] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.776069 [\*\*] [1:100004:3] "[ALERT] HTTP Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.776233 [\*\*] [1:2000002:1] "[ALERT] SQL Injection Attempt Detected (Encoded OR 1=1)" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252 → 192.168.198.148:80

09/17-08:21:51.776233 [\*\*] [1:1000400:1] "[ALERT] Possible Webshell Upload Detected (.php)" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252 → 192.168.198.148:80

09/17-08:21:51.776233 [\*\*] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.776893 [\*\*] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.776893 [\*\*] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.777040 [\*\*] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.777040 [\*\*] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.777486 [\*\*] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

09/17-08:21:51.777486 [\*\*] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:58252  
→ 192.168.198.148:80

3) SQL Injection (UNION SELECT) — SID 2000003

### **Attacker (192.168.198.130):**

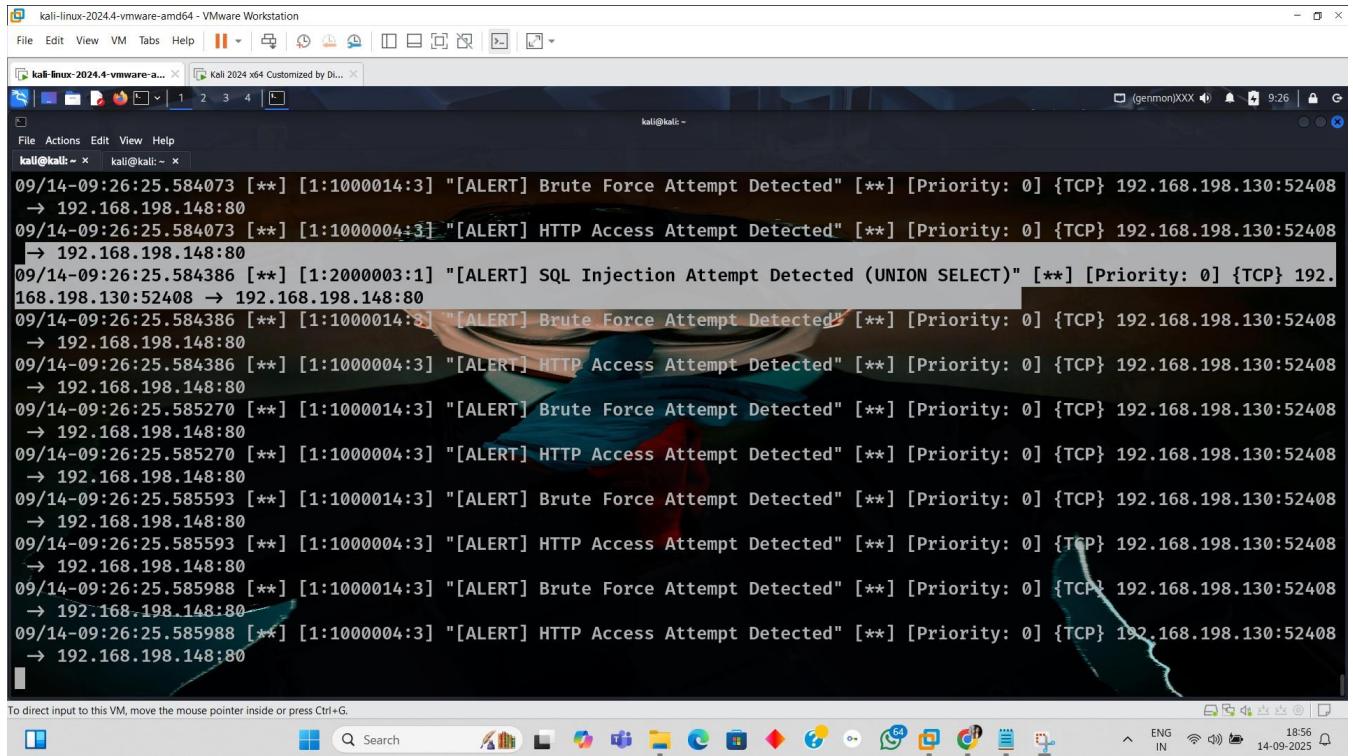
- curl -s -o /dev/null "http://192.168.198.148/search.php?q=UNION+SELECT+null"
  - for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/search.php?q=UNION+SELECT+null"; done

## **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):**

kali-linux-2024.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali: ~

```
8.198.148:80
09/17-08:18:55.388599 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.388599 [**] [1:100004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.388692 [**] [1:200004:1] "[ALERT] SQL Injection Attempt Detected (Tautology a=a)" [**] [Priority: 0] {TCP} 192.168.198.130:41594 → 192.168.198.148:80
09/17-08:18:55.388692 [**] [1:1000400:1] "[ALERT] Possible Webshell Upload Detected (.php)" [**] [Priority: 0] {TCP} 192.168.198.130:41594 → 192.168.198.148:80
09/17-08:18:55.388692 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.389395 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.389395 [**] [1:100004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.389580 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.389580 [**] [1:100004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.389960 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.389960 [**] [1:100004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41594
→ 192.168.198.148:80
09/17-08:18:55.396898 [**] [1:100024:4] "[ALERT] Aggressive Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:4160
```

## 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/

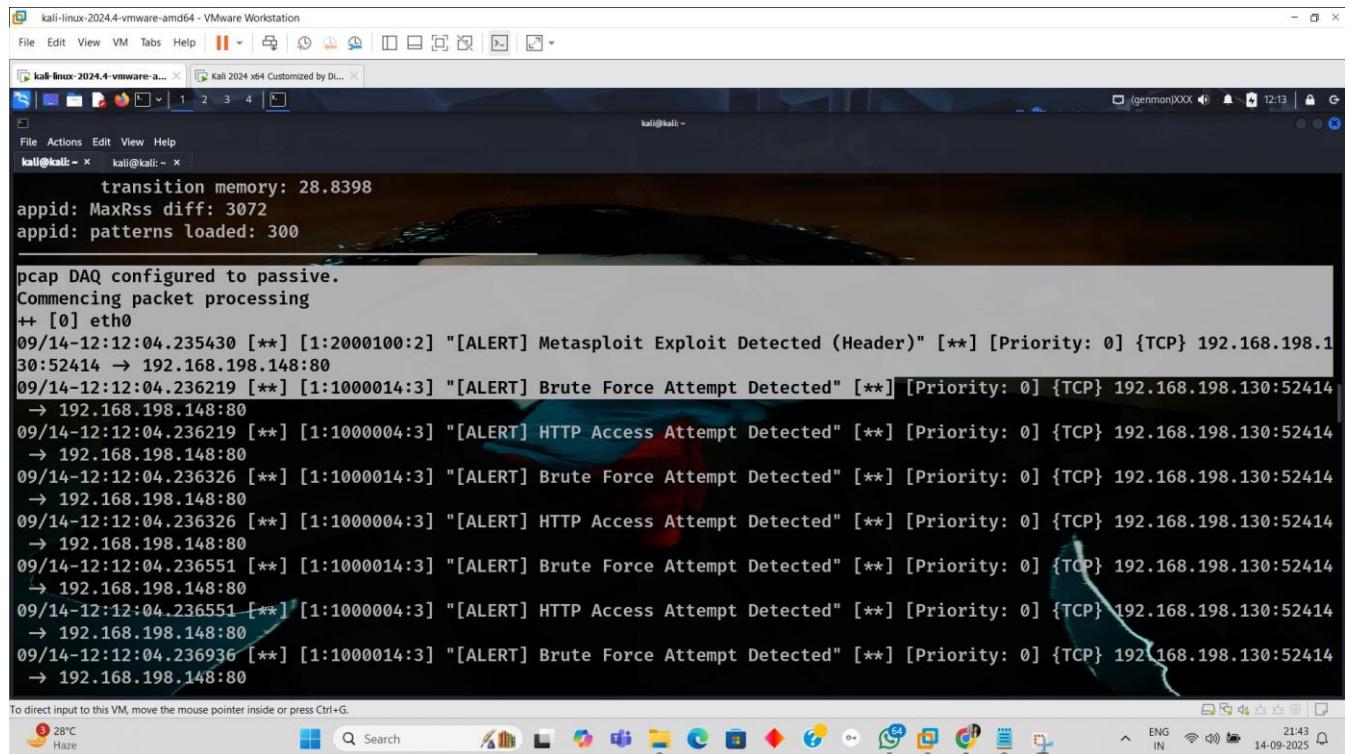
## **Victim / Snort host (192.168.198.148):**

- 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):**

---



The screenshot shows a terminal window titled "kali@kali: ~" running on Kali Linux. The window displays several Snort alerts. The alerts are as follows:

```

transition memory: 28.8398
appid: MaxRss diff: 3072
appid: patterns loaded: 300

pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
09/14-12:12:04.235430 [**] [1:2000100:2] "[ALERT] Metasploit Exploit Detected (Header)" [**] [Priority: 0] {TCP} 192.168.198.1
30:52414 → 192.168.198.148:80
09/14-12:12:04.236219 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52414
→ 192.168.198.148:80
09/14-12:12:04.236219 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52414
→ 192.168.198.148:80
09/14-12:12:04.236326 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52414
→ 192.168.198.148:80
09/14-12:12:04.236326 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52414
→ 192.168.198.148:80
09/14-12:12:04.236551 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52414
→ 192.168.198.148:80
09/14-12:12:04.236551 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52414
→ 192.168.198.148:80
09/14-12:12:04.236936 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52414
→ 192.168.198.148:80

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## 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):**

kali-linux-2024.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali: ~

```
→ 192.168.198.148:80
09/17-08:15:48.076782 [**] [1:1000013:3] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.077156 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.077156 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.077279 [**] [1:2000101:2] "[ALERT] Metasploit Exploit Detected (Meterpreter User-Agent)" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.077279 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.077279 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.078003 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.078003 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.078024 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.078024 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.078026 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366 → 192.168.198.148:80
09/17-08:15:48.078026 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35366
```

## 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):**

```
kali-linux-2024.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help || Metasploitable3-Linux | kali-linux-2024.4-vmware-a... | Kali 2024 x64 Customized by Di...
root@kali:/home/kali/Desktop ~ (genmon)XXX 5:27

File Actions Edit View Help
root@kali:/home/kali/Desktop x root@kali:/home/kali x

pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
09/11/05:27:28.428954 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:23
09/11/05:27:28.428954 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:22
09/11/05:27:28.428955 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:1720
09/11/05:27:28.428956 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:135
09/11/05:27:28.428956 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:135
09/11/05:27:28.428957 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:143
09/11/05:27:28.428957 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:143
09/11/05:27:28.428957 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:143
09/11/05:27:28.429357 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:113
09/11/05:27:28.429357 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:113
09/11/05:27:28.429374 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:95
09/11/05:27:28.429374 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:95
09/11/05:27:28.429733 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:554
09/11/05:27:28.429733 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:554
09/11/05:27:28.429749 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:445
09/11/05:27:28.429749 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:445
09/11/05:27:28.429903 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:80
09/11/05:27:28.429903 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:80
09/11/05:27:28.429904 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:1025
09/11/05:27:28.430071 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:256
09/11/05:27:28.430071 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:256
09/11/05:27:28.430208 [**] [1:1000001:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:111
09/11/05:27:28.430208 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:111
09/11/05:27:28.430331 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45205 → 192.168.198.148:1723

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

6 34°C
Mostly cloudy
ENG IN
14:57
11-09-2025
```

## 8) Port scan (1-1024) — SID 1000013

## **Attacker (192.168.198.130):**

- sudo nmap -sS -p1-1024 192.168.198.148

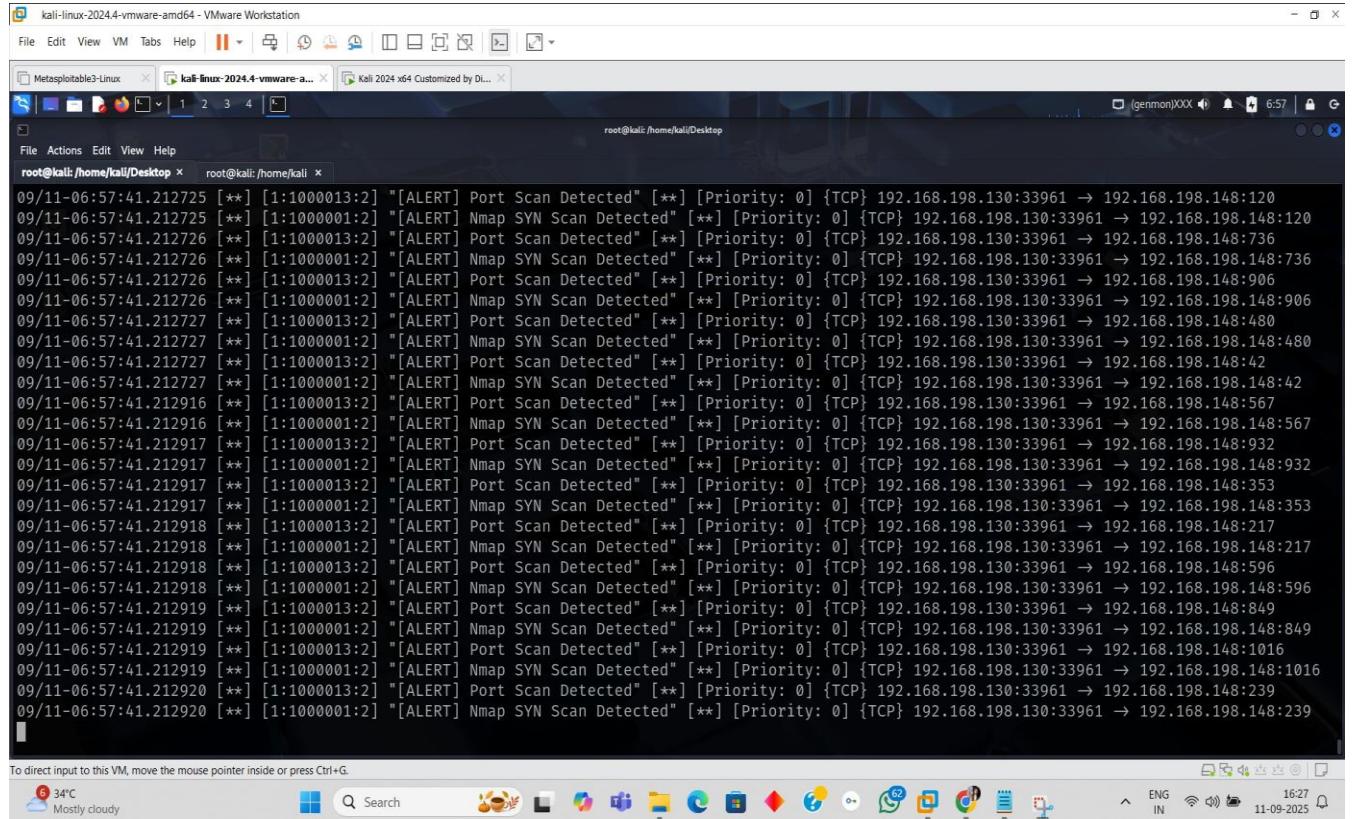
## **Victim / Snort host (192.168.198.148):**

- 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):**

---



```

root@kali:~/home/kali/Desktop x root@kali:~/home/kali x
09/11-06:57:41.212725 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:120
09/11-06:57:41.212725 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:120
09/11-06:57:41.212726 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:736
09/11-06:57:41.212726 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:736
09/11-06:57:41.212726 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:906
09/11-06:57:41.212726 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:906
09/11-06:57:41.212727 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:480
09/11-06:57:41.212727 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:480
09/11-06:57:41.212727 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:42
09/11-06:57:41.212727 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:42
09/11-06:57:41.212916 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:567
09/11-06:57:41.212916 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:567
09/11-06:57:41.212917 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:932
09/11-06:57:41.212917 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:932
09/11-06:57:41.212917 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:353
09/11-06:57:41.212917 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:353
09/11-06:57:41.212918 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:217
09/11-06:57:41.212918 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:217
09/11-06:57:41.212918 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:596
09/11-06:57:41.212918 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:596
09/11-06:57:41.212919 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:849
09/11-06:57:41.212919 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:849
09/11-06:57:41.212919 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:1016
09/11-06:57:41.212919 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:1016
09/11-06:57:41.212920 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:239
09/11-06:57:41.212920 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:33961 → 192.168.198.148:239

```

## 9) Nmap XMAS scan — SID 1000022

**Attacker (192.168.198.148):**

---

- sudo nmap -sX -p1-200 192.168.198.148

### *Victim / Snort host (192.168.198.148):*

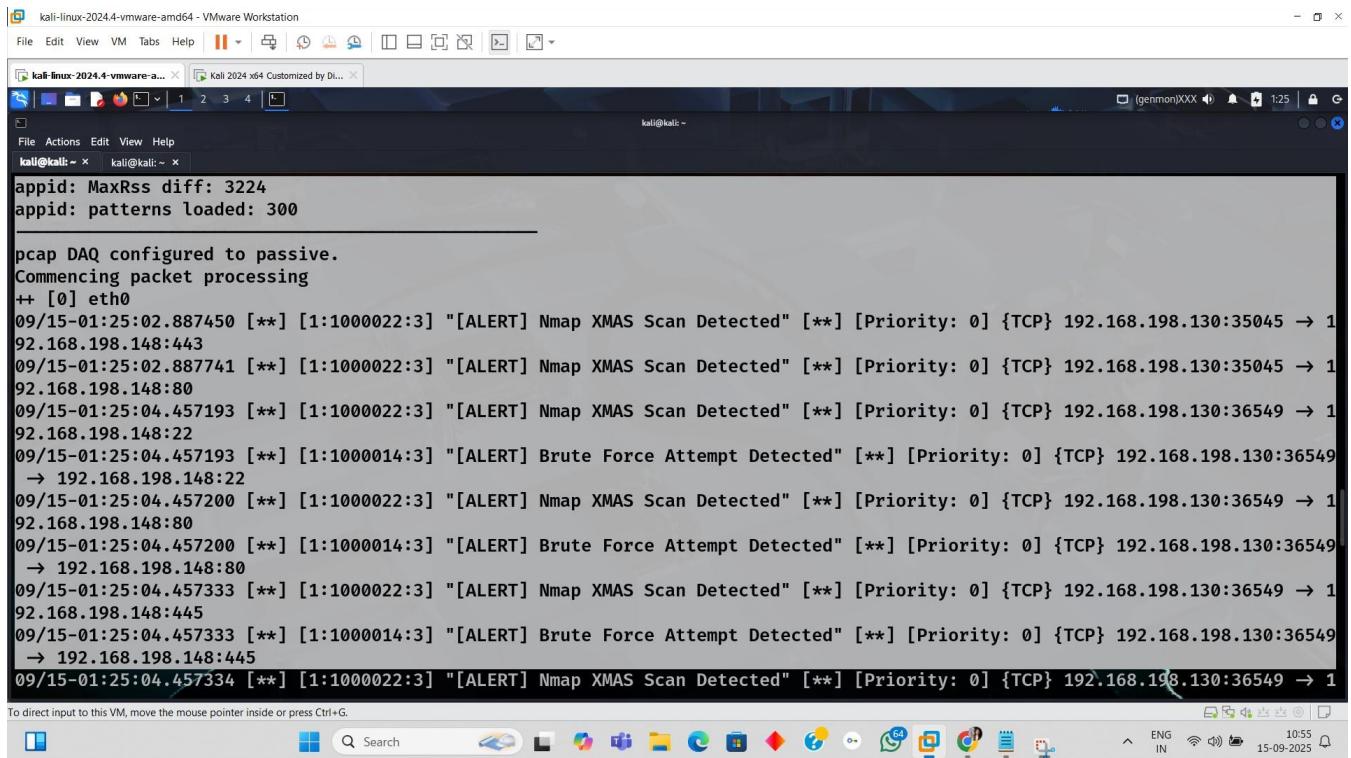
---

- 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):*

---



The screenshot shows a terminal window titled 'kali@kali: ~' running on a Kali Linux VM. The window displays several lines of Snort log output. The log entries indicate multiple instances of 'Nmap XMAS Scan Detected' and 'Brute Force Attempt Detected' alerts, primarily targeting port 135 on the IP address 192.168.198.130 from various sources, including 192.168.198.148. The log entries are timestamped from 09/15/2024 at 01:25:02 to 04:45:334.

```
kali@kali: ~
appid: MaxRss diff: 3224
appid: patterns loaded: 300

pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
09/15-01:25:02.887450 [**] [1:1000022:3] "[ALERT] Nmap XMAS Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35045 → 192.168.198.148:443
09/15-01:25:02.887741 [**] [1:1000022:3] "[ALERT] Nmap XMAS Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:35045 → 192.168.198.148:80
09/15-01:25:04.457193 [**] [1:1000022:3] "[ALERT] Nmap XMAS Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36549 → 192.168.198.148:22
09/15-01:25:04.457193 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36549 → 192.168.198.148:22
09/15-01:25:04.457200 [**] [1:1000022:3] "[ALERT] Nmap XMAS Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36549 → 192.168.198.148:80
09/15-01:25:04.457200 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36549 → 192.168.198.148:80
09/15-01:25:04.457333 [**] [1:1000022:3] "[ALERT] Nmap XMAS Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36549 → 192.168.198.148:445
09/15-01:25:04.457333 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36549 → 192.168.198.148:445
09/15-01:25:04.457334 [**] [1:1000022:3] "[ALERT] Nmap XMAS Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36549 → 192.168.198.148:445
```

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

### *Attacker (192.168.198.148):*

---

- sudo nmap -A 192.168.198.148

### *Victim / Snort host (192.168.198.148):*

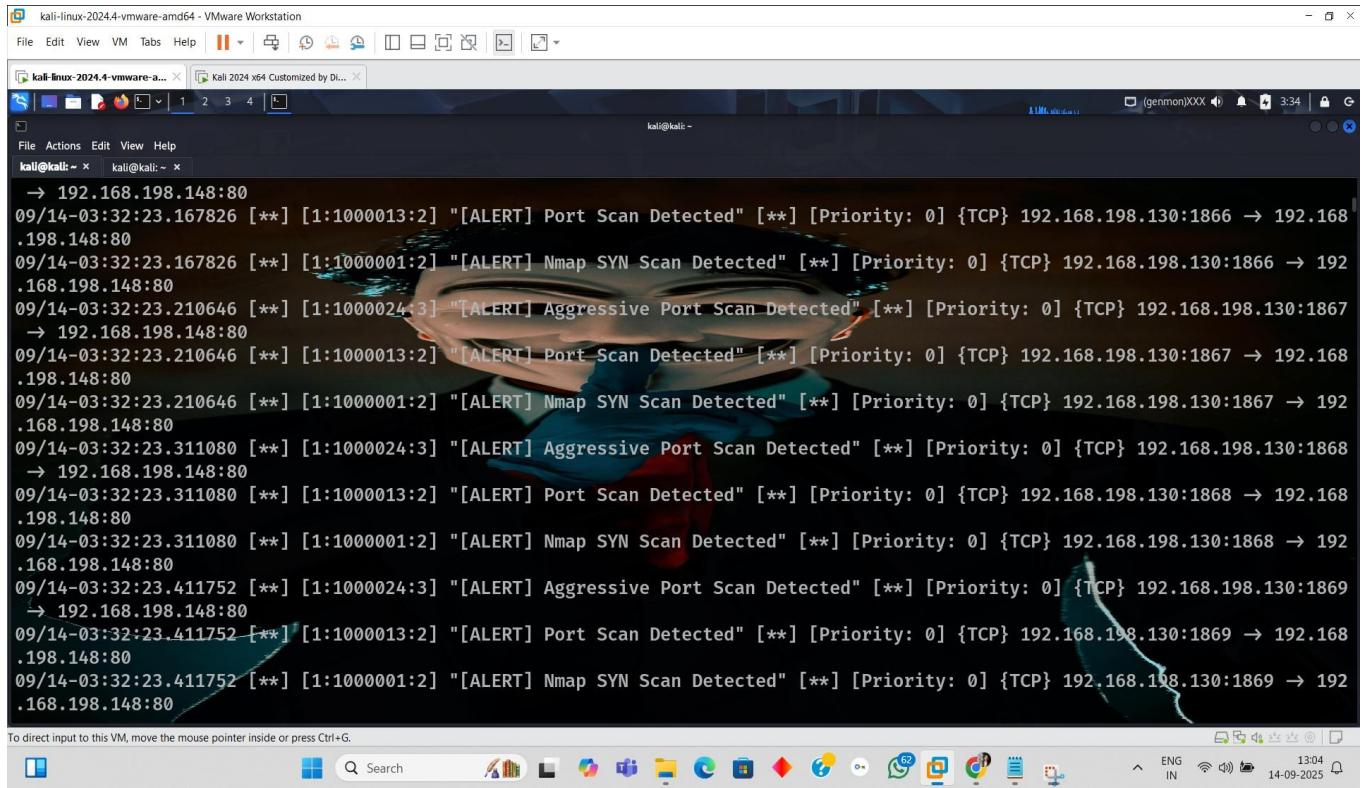
---

- 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):*

---



The screenshot shows a terminal window on a Kali Linux system. The terminal output displays numerous Snort alerts indicating various types of port scanning activity. The alerts are timestamped and show details such as the source IP (192.168.198.148), destination IP (192.168.198.130), port number (1866, 1867, 1868, 1869), and the type of scan detected (Port Scan Detected, Nmap SYN Scan Detected, Aggressive Port Scan Detected). The terminal window is titled 'kali@kali: ~' and is part of a VMware Workstation interface.

```
File Edit View VM Tabs Help | 1 2 3 4 | 
File Actions Edit View Help
kali@kali: ~ kali@kali: ~
→ 192.168.198.148:80
09/14-03:32:23.167826 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1866 → 192.168.198.148:80
09/14-03:32:23.167826 [**] [1:100001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1866 → 192.168.198.148:80
09/14-03:32:23.210646 [**] [1:1000024:3] "[ALERT] Aggressive Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1867 → 192.168.198.148:80
09/14-03:32:23.210646 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1867 → 192.168.198.148:80
09/14-03:32:23.210646 [**] [1:100001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1867 → 192.168.198.148:80
09/14-03:32:23.311080 [**] [1:1000024:3] "[ALERT] Aggressive Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1868 → 192.168.198.148:80
09/14-03:32:23.311080 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1868 → 192.168.198.148:80
09/14-03:32:23.311080 [**] [1:100001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1868 → 192.168.198.148:80
09/14-03:32:23.411752 [**] [1:1000024:3] "[ALERT] Aggressive Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1869 → 192.168.198.148:80
09/14-03:32:23.411752 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1869 → 192.168.198.148:80
09/14-03:32:23.411752 [**] [1:100001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:1869 → 192.168.198.148:80
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## 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):**

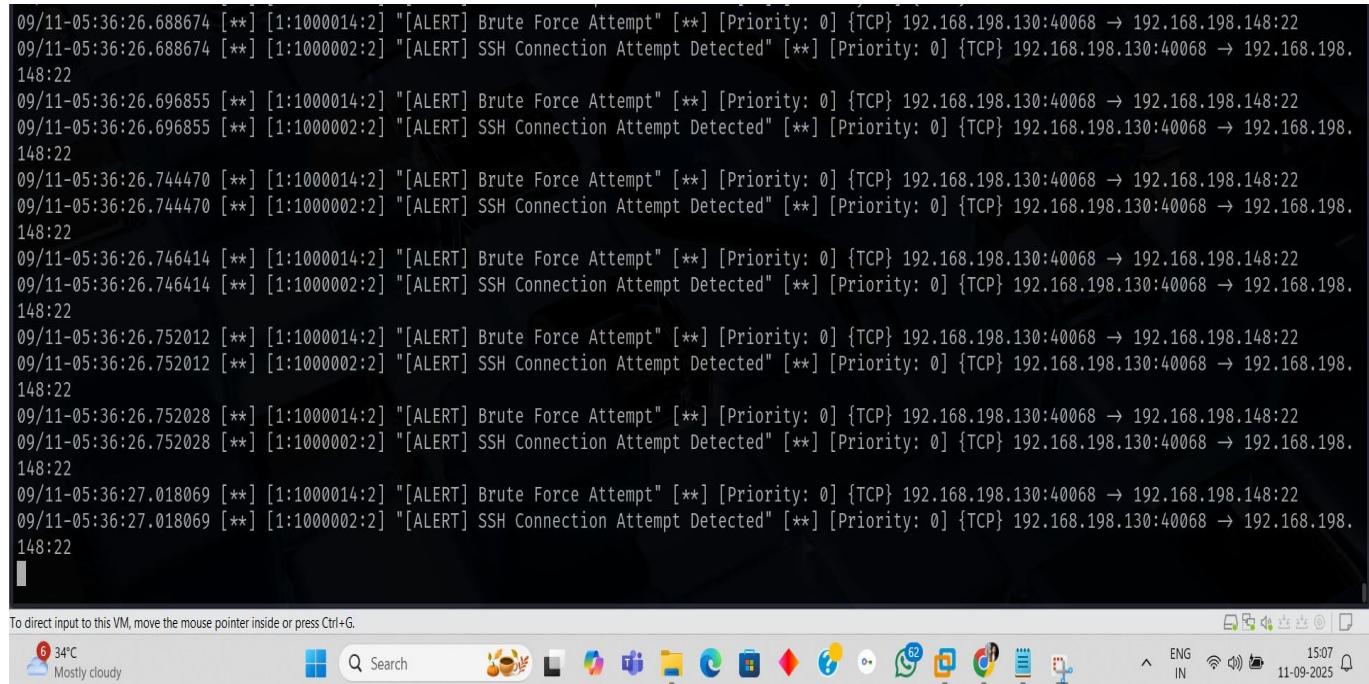
---

- 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):**

---



```

09/11-05:36:26.688674 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.688674 [**] [1:1000002:2] "[ALERT] SSH Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.696855 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.696855 [**] [1:1000002:2] "[ALERT] SSH Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.744470 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.744470 [**] [1:1000002:2] "[ALERT] SSH Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.746414 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.746414 [**] [1:1000002:2] "[ALERT] SSH Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.752012 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.752012 [**] [1:1000002:2] "[ALERT] SSH Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.752028 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:26.752028 [**] [1:1000002:2] "[ALERT] SSH Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:27.018069 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
09/11-05:36:27.018069 [**] [1:1000002:2] "[ALERT] SSH Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40068 → 192.168.198.148:22
148:22

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

34°C  
Mostly cloudy



## 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):*

---

The screenshot shows a terminal window titled "kali@kali: ~" running on a Kali Linux VM. The window displays a series of Snort alerts. The alerts are as follows:

```
→ 192.168.198.148:80
09/17-08:14:07.589784 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.589785 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.589785 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.589785 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.589785 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.589851 [**] [1:1000004:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.589973 [**] [1:1000014:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.589973 [**] [1:1000004:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.590306 [**] [1:1000014:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
09/17-08:14:07.590306 [**] [1:1000004:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41926
→ 192.168.198.148:80
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

### **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):**

kali-linux-2024.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Metasploitable3-Linux kali-linux-2024.4-vmware-a... Kali 2024 x64 Customized by Di...

1 2 3 4

File Actions Edit View Help

root@kali:/home/kali/Desktop x root@kali:/home/kali x

```
09/11-05:27:32.382913 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:2001
09/11-05:27:32.382914 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:109
09/11-05:27:32.382914 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:109
09/11-05:27:32.382914 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:109
09/11-05:27:32.382915 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:3971
09/11-05:27:32.382916 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:9999
09/11-05:27:32.385422 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:62078
09/11-05:27:32.385451 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:16001
09/11-05:27:32.385452 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:2034
09/11-05:27:32.385452 [**] [1:1000001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38367 → 192.168.198.148:1110
09/11-05:29:48.415947 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:50.456627 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:51.487811 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:52.511781 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:53.535810 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:55.440927 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:56.447563 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:57.471244 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:29:58.495517 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:30:00.392849 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:30:01.407322 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:30:02.431180 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:30:03.454967 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:30:05.809049 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:30:06.815055 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-05:30:07.839285 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
```

## 14) HTTP access — SID 1000004

**Attacker (192.168.198.130):**

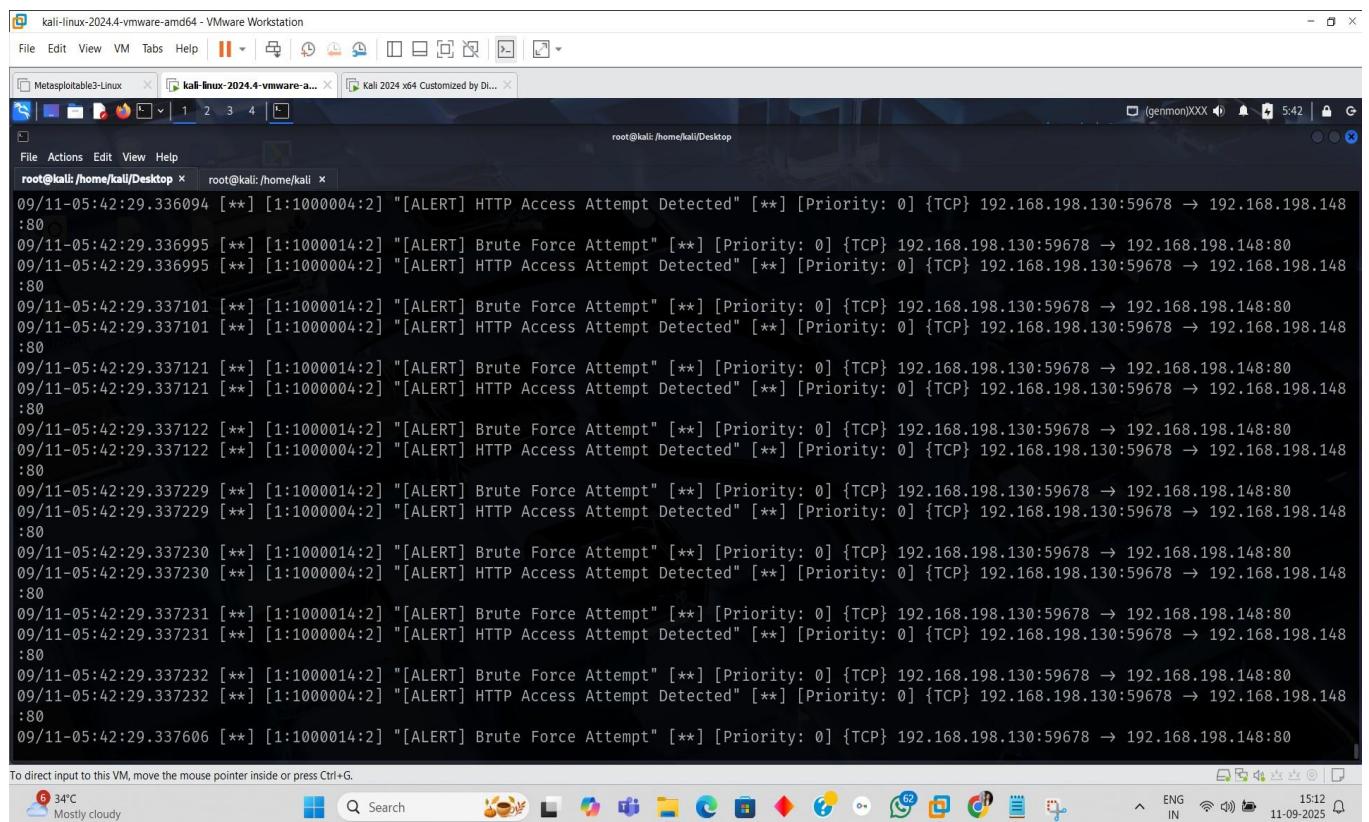
- curl -s -o /dev/null http://192.168.198.148/

**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):**



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output displays numerous Snort alerts for HTTP access attempts. The alerts are timestamped and show the source IP (192.168.198.130) connecting to port 148 on the victim host (192.168.198.148). The alerts are categorized into two types: "HTTP Access Attempt Detected" and "Brute Force Attempt". The terminal window has a title bar "root@kali:/home/kali/Desktop" and a status bar at the bottom showing system information like battery level, signal strength, and date/time.

```
09/11-05:42:29.336094 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.336995 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.336995 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337101 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337101 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337121 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337121 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337122 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337122 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337229 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337229 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337230 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337230 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337231 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337231 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337232 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337232 [**] [1:1000004:2] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
09/11-05:42:29.337606 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:59678 → 192.168.198.148:80
```

## 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):**

kali-linux-2024.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Metasploitable3-Linux kali-linux-2024.4-vmware-a... Kali 2024 x64 Customized by Di...

(genmon)XXX 5:48 5/18

File Actions Edit View Help root@kali:/home/kali/Desktop

root@kali:/home/kali/Desktop x root@kali:/home/kali x

8:443  
09/11-05:48:11.904585 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.905122 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.905938 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.906556 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.906557 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.906625 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.906626 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.907964 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.907983 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.908347 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:11.908360 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35550 → 192.168.198.14  
8:443  
09/11-05:48:14.315632 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35558 → 192.168.198.14  
8:443  
09/11-05:48:14.316107 [\*\*] [1:1000005:2] "[ALERT] HTTPS Access Attempt Detected" [\*\*] [Priority: 0] {TCP} 192.168.198.130:35558 → 192.168.198.14  
8:443

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## 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

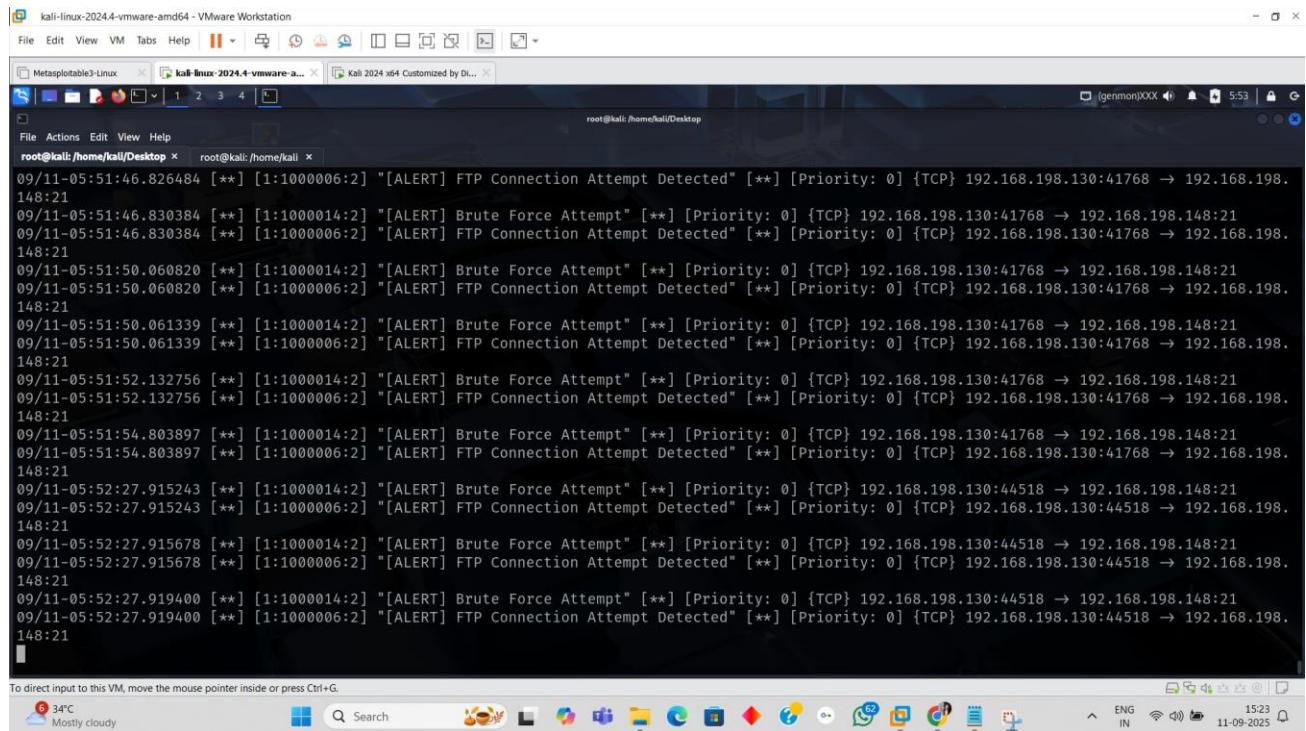
*Victim / Snort host (192.168.198.148):*

- 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):*

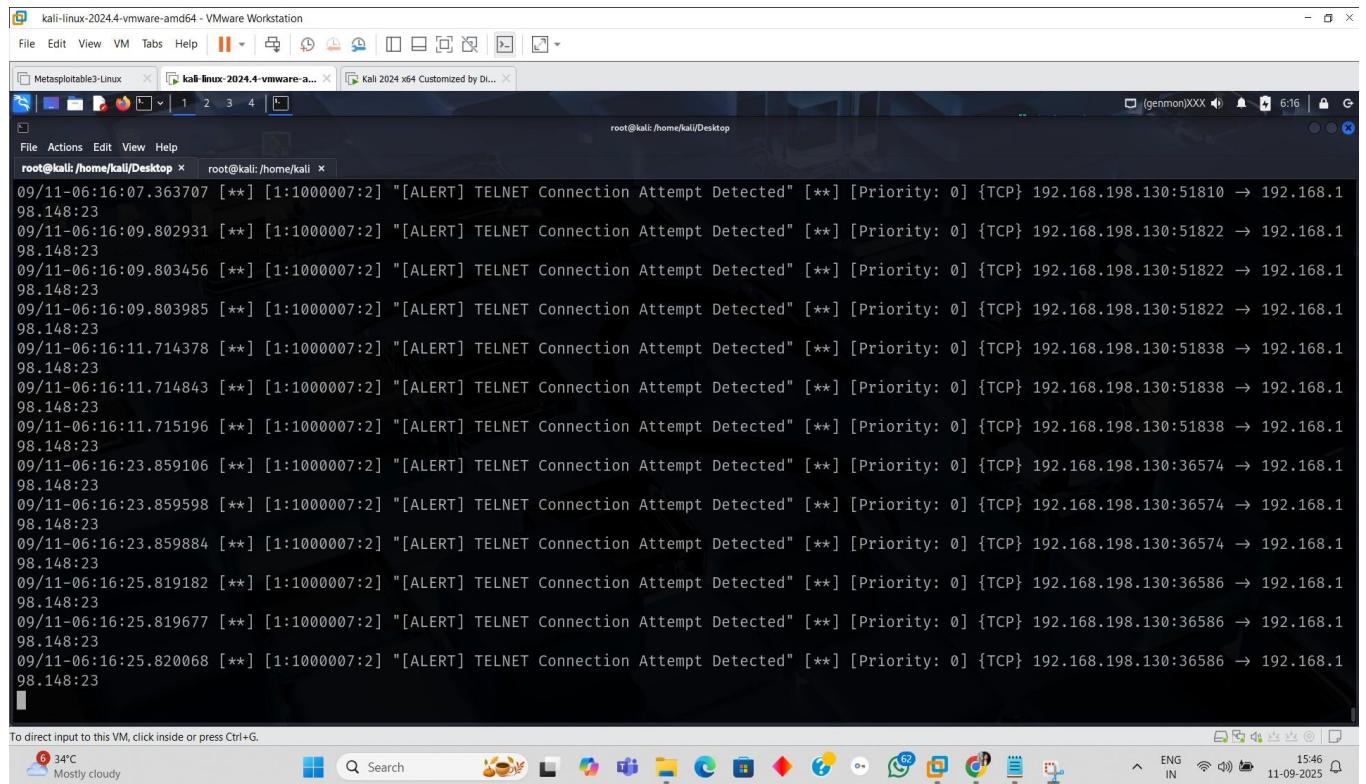
### Ftp Detected Poc –



The screenshot shows a terminal window titled 'root@kali:~\$' with several Snort alerts displayed. The alerts are related to FTP connection attempts from 192.168.198.130 to 192.168.198.148. The log entries are as follows:

```
09/11-05:51:46.826484 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:46.830384 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:46.830384 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:50.060820 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:50.060820 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:50.061339 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:50.061339 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:52.132756 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:52.132756 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:54.803897 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:51:54.803897 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:41768 → 192.168.198.148:21
09/11-05:52:27.915243 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:44518 → 192.168.198.148:21
09/11-05:52:27.915243 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44518 → 192.168.198.148:21
09/11-05:52:27.915678 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:44518 → 192.168.198.148:21
09/11-05:52:27.915678 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44518 → 192.168.198.148:21
09/11-05:52:27.919400 [**] [1:1000014:2] "[ALERT] Brute Force Attempt" [**] [Priority: 0] {TCP} 192.168.198.130:44518 → 192.168.198.148:21
09/11-05:52:27.919400 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44518 → 192.168.198.148:21
```

## Telnet Detected Poc –



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali:/home/kali/Desktop". The terminal content displays numerous log entries from a log file, all reporting "[ALERT] TELNET Connection Attempt Detected" for various IP addresses (e.g., 192.168.198.130, 192.168.198.130:51822) at different times (e.g., 09/11-06:16:07.363707, 09/11-06:16:09.802931). The log entries are timestamped with dates ranging from 09/11-06 to 09/11-06, and times from 07:23 to 11:23. The terminal window is part of a VMware Workstation interface, with other windows visible in the background.

```
root@kali:~# cat /var/log/auth.log | grep -i telnet
09/11-06:16:07.363707 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:51810 → 192.168.198.148:23
09/11-06:16:09.802931 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:51822 → 192.168.198.148:23
09/11-06:16:09.803456 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:51822 → 192.168.198.148:23
09/11-06:16:09.803985 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:51822 → 192.168.198.148:23
09/11-06:16:11.714378 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:51838 → 192.168.198.148:23
09/11-06:16:11.714843 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:51838 → 192.168.198.148:23
09/11-06:16:11.715196 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:51838 → 192.168.198.148:23
09/11-06:16:23.859106 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36574 → 192.168.198.148:23
09/11-06:16:23.859598 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36574 → 192.168.198.148:23
09/11-06:16:23.859884 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36574 → 192.168.198.148:23
09/11-06:16:25.819182 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36586 → 192.168.198.148:23
09/11-06:16:25.819677 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36586 → 192.168.198.148:23
09/11-06:16:25.820068 [**] [1:1000007:2] "[ALERT] TELNET Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:36586 → 192.168.198.148:23
```

## Rdp detected Poc –

A screenshot of a Kali Linux desktop environment within a VMware Workstation window. The desktop has a dark theme with a taskbar at the bottom containing icons for various applications like Metasploit, Firefox, and File Explorer. A terminal window is open in the foreground, showing a log of RDP connection attempts from 192.168.198.130 to 192.168.198.148. The logs are timestamped from 09/11-06:23:19 to 09/11-06:23:19. The terminal window title is 'root@kali:/home/kali/Desktop'.

```
09/11-06:23:19.294683 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.302506 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.310504 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.318506 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.334593 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.342430 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.350455 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.358509 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.374581 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.382603 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.390482 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.398611 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
09/11-06:23:19.414615 [**] [1:1000008:2] "[ALERT] RDP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52746 → 192.168.198.148:3389
```

## Mysql detected Poc –

A screenshot of a Kali Linux desktop environment within a VMware Workstation window. The desktop has a dark theme with a taskbar at the bottom containing icons for various applications like Metasploit, Firefox, and File Explorer. A terminal window is open in the foreground, showing a log of MySQL access attempts from 192.168.198.130 to 192.168.198.148. The logs are timestamped from 09/11-06:33:08 to 09/11-06:33:14. The terminal window title is 'root@kali:/home/kali/Desktop'.

```
09/11-06:33:08.774259 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42590 → 192.168.198.148:3306
09/11-06:33:08.775132 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42590 → 192.168.198.148:3306
09/11-06:33:08.775147 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42590 → 192.168.198.148:3306
09/11-06:33:11.271444 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42604 → 192.168.198.148:3306
09/11-06:33:11.271980 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42604 → 192.168.198.148:3306
09/11-06:33:11.273045 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42604 → 192.168.198.148:3306
09/11-06:33:11.275100 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42604 → 192.168.198.148:3306
09/11-06:33:14.494552 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52782 → 192.168.198.148:3306
09/11-06:33:14.495000 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52782 → 192.168.198.148:3306
09/11-06:33:14.495646 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52782 → 192.168.198.148:3306
09/11-06:33:14.495651 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52782 → 192.168.198.148:3306
09/11-06:33:14.496407 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:52782 → 192.168.198.148:3306
09/11-06:33:27.162455 [**] [1:1000009:2] "[ALERT] MySQL Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:37672 → 192.168.198.148:3306
```

## Smtp Detected Poc –

```

root@kali:~/Desktop
09/11-06:37:54.414267 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42962 → 192.168.198.148:2
5
09/11-06:37:54.414717 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42962 → 192.168.198.148:2
5
09/11-06:37:56.734093 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42962 → 192.168.198.148:2
5
09/11-06:37:56.734734 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42962 → 192.168.198.148:2
5
09/11-06:37:58.974106 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42962 → 192.168.198.148:2
5
09/11-06:38:50.208231 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42962 → 192.168.198.148:2
5
09/11-06:38:50.208246 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42962 → 192.168.198.148:2
5
09/11-06:38:53.162936 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44714 → 192.168.198.148:2
5
09/11-06:38:53.163328 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44714 → 192.168.198.148:2
5
09/11-06:38:53.273369 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44714 → 192.168.198.148:2
5
09/11-06:38:57.191659 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44714 → 192.168.198.148:2
5
09/11-06:38:57.193184 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44714 → 192.168.198.148:2
5
09/11-06:38:57.193440 [**] [1:1000010:2] "[ALERT] SMTP Mail Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:44714 → 192.168.198.148:2
5

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

34°C Mostly cloudy Search ENG IN 16:09 11-09-2025

## 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):**

```

root@kali:~/home/kali/Desktop
root@kali:~/home/kali/Desktop

09/11-06:46:18.380608 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:54810 → 192.168.198.148:53
09/11-06:46:18.380608 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:54810 → 192.168.198.148:53
09/11-06:46:20.937485 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:58845 → 192.168.198.148:53
09/11-06:46:20.937485 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:58845 → 192.168.198.148:53
09/11-06:46:20.938772 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:56412 → 192.168.198.148:53
09/11-06:46:20.938772 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:56412 → 192.168.198.148:53
09/11-06:46:22.450746 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:54212 → 192.168.198.148:53
09/11-06:46:22.450746 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:54212 → 192.168.198.148:53
09/11-06:46:22.451943 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:59221 → 192.168.198.148:53
09/11-06:46:22.451943 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:59221 → 192.168.198.148:53
09/11-06:46:43.788501 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:58089 → 192.168.198.148:53
09/11-06:46:43.788501 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:58089 → 192.168.198.148:53
09/11-06:46:46.281663 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:45602 → 192.168.198.148:53
09/11-06:46:46.281663 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:45602 → 192.168.198.148:53
09/11-06:46:46.282911 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:42521 → 192.168.198.148:53
09/11-06:46:46.282911 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:42521 → 192.168.198.148:53
09/11-06:46:48.315473 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:46628 → 192.168.198.148:53
09/11-06:46:48.315473 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:46628 → 192.168.198.148:53
09/11-06:46:48.316898 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:41920 → 192.168.198.148:53
09/11-06:46:48.316898 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:41920 → 192.168.198.148:53
09/11-06:46:51.067397 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:39232 → 192.168.198.148:53
09/11-06:46:51.067397 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:39232 → 192.168.198.148:53
09/11-06:46:51.068680 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:40806 → 192.168.198.148:53
09/11-06:46:51.068680 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:40806 → 192.168.198.148:53
09/11-06:47:06.339694 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:40819 → 192.168.198.148:53
09/11-06:47:06.339694 [**] [1:1000011:2] "[ALERT] DNS Query Detected" [**] [Priority: 0] {UDP} 192.168.198.130:40819 → 192.168.198.148:53

```

## 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):*

---

The screenshot shows a terminal window titled 'root@kali: /home/kali/Desktop' with several tabs open. The terminal is displaying a log of Snort alerts. The alerts are as follows:

```
09/11-06:51:36.231146 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43090 → 192.168.198.148:445
09/11-06:51:36.231399 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40174 → 192.168.198.148:139
09/11-06:51:36.231399 [**] [1:100001:2] "[ALERT] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:40174 → 192.168.198.148:139
09/11-06:51:36.231750 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43090 → 192.168.198.148:445
09/11-06:51:38.282818 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.282818 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.283147 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.283293 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.287639 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.287742 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.289460 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.290169 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.290965 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
09/11-06:51:38.291669 [**] [1:1000012:2] "[ALERT] SMB File Sharing Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:43096 → 192.168.198.148:445
```

To direct input to this VM, click inside or press Ctrl+G.

34°C Mostly cloudy

Search

ENG IN 16:21 11-09-2023

## 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):**

---

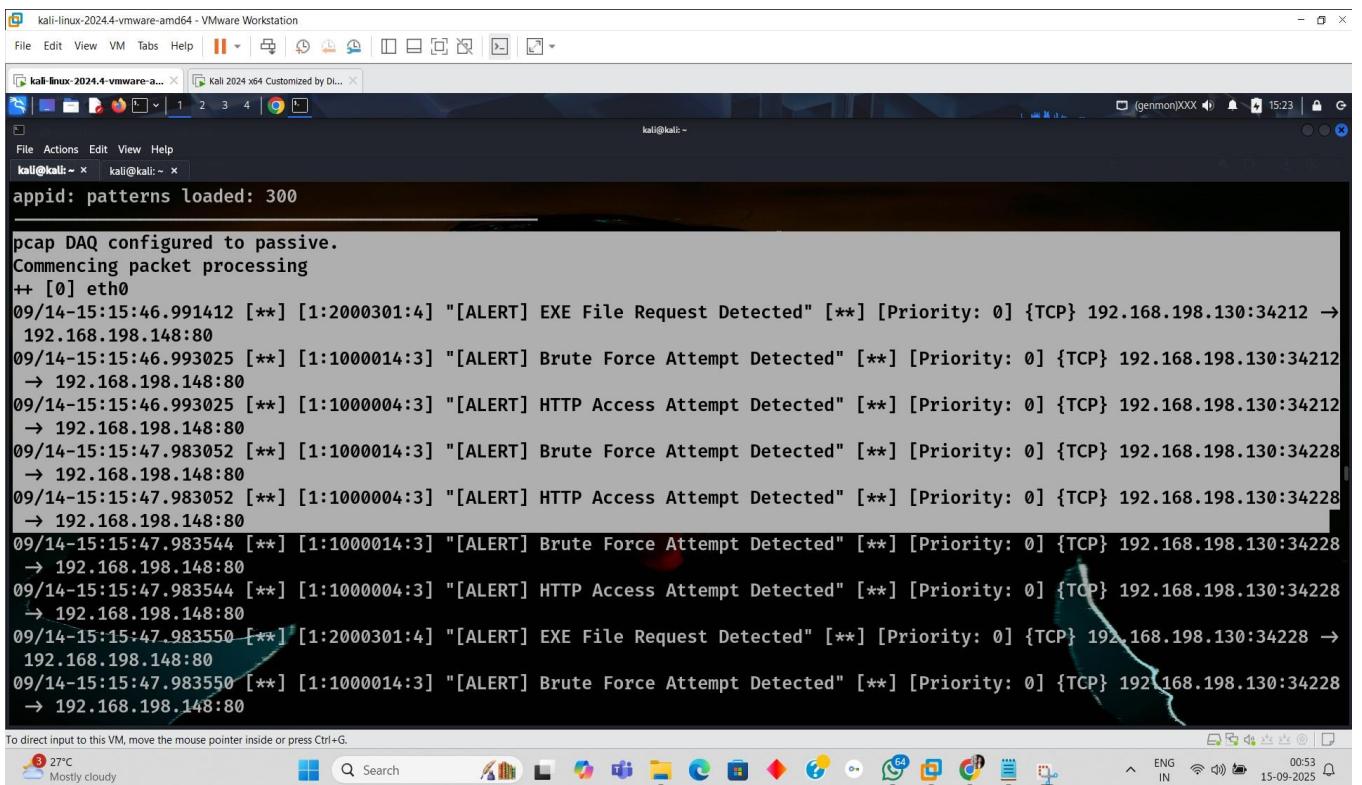
- sudo snort -c /etc/snort/snort.lua -i eth0 -A alert\_fast

**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 –**



```

kali@kali:~$ appid: patterns loaded: 300
pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
09/14-15:15:46.991412 [**] [1:2000301:4] "[ALERT] EXE File Request Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34212 → 192.168.198.148:80
09/14-15:15:46.993025 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34212 → 192.168.198.148:80
09/14-15:15:46.993025 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34212 → 192.168.198.148:80
09/14-15:15:47.983052 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34228 → 192.168.198.148:80
09/14-15:15:47.983052 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34228 → 192.168.198.148:80
09/14-15:15:47.983544 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34228 → 192.168.198.148:80
09/14-15:15:47.983544 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34228 → 192.168.198.148:80
09/14-15:15:47.983550 [**] [1:2000301:4] "[ALERT] EXE File Request Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34228 → 192.168.198.148:80
09/14-15:15:47.983550 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:34228 → 192.168.198.148:80

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## 20) Nikto scan — SID 1000056

*Attacker (192.168.198.130):*

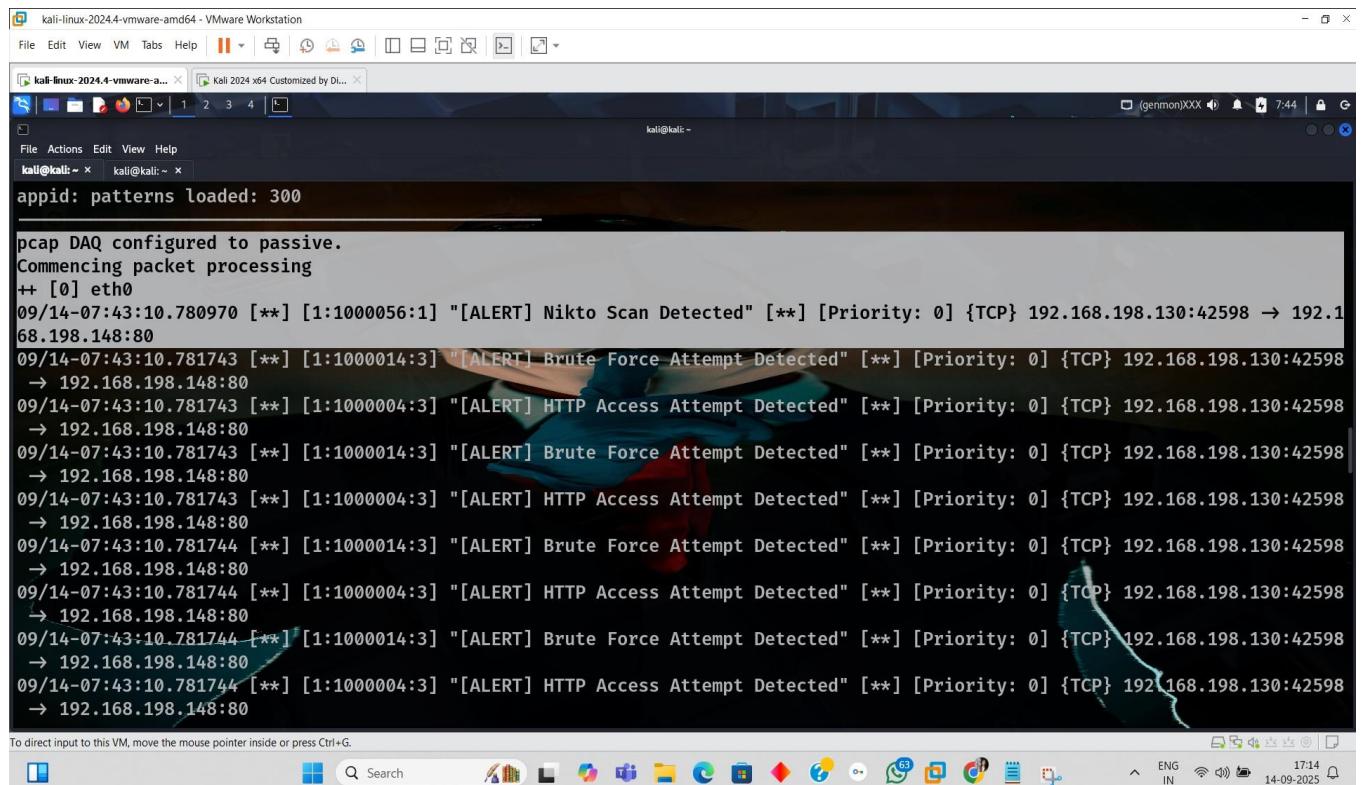
- curl -s -o /dev/null -A "Nikto/2.1.6" http://192.168.198.148/
- nikto -h http://192.168.198.148

*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):*



The screenshot shows a terminal window on a Kali Linux desktop. The terminal output is as follows:

```
appid: patterns loaded: 300
pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
09/14-07:43:10.780970 [**] [1:1000056:1] "[ALERT] Nikto Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781743 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781743 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781743 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781743 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781744 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781744 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781744 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
09/14-07:43:10.781744 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:42598 → 192.168.198.148:80
```

## 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):*

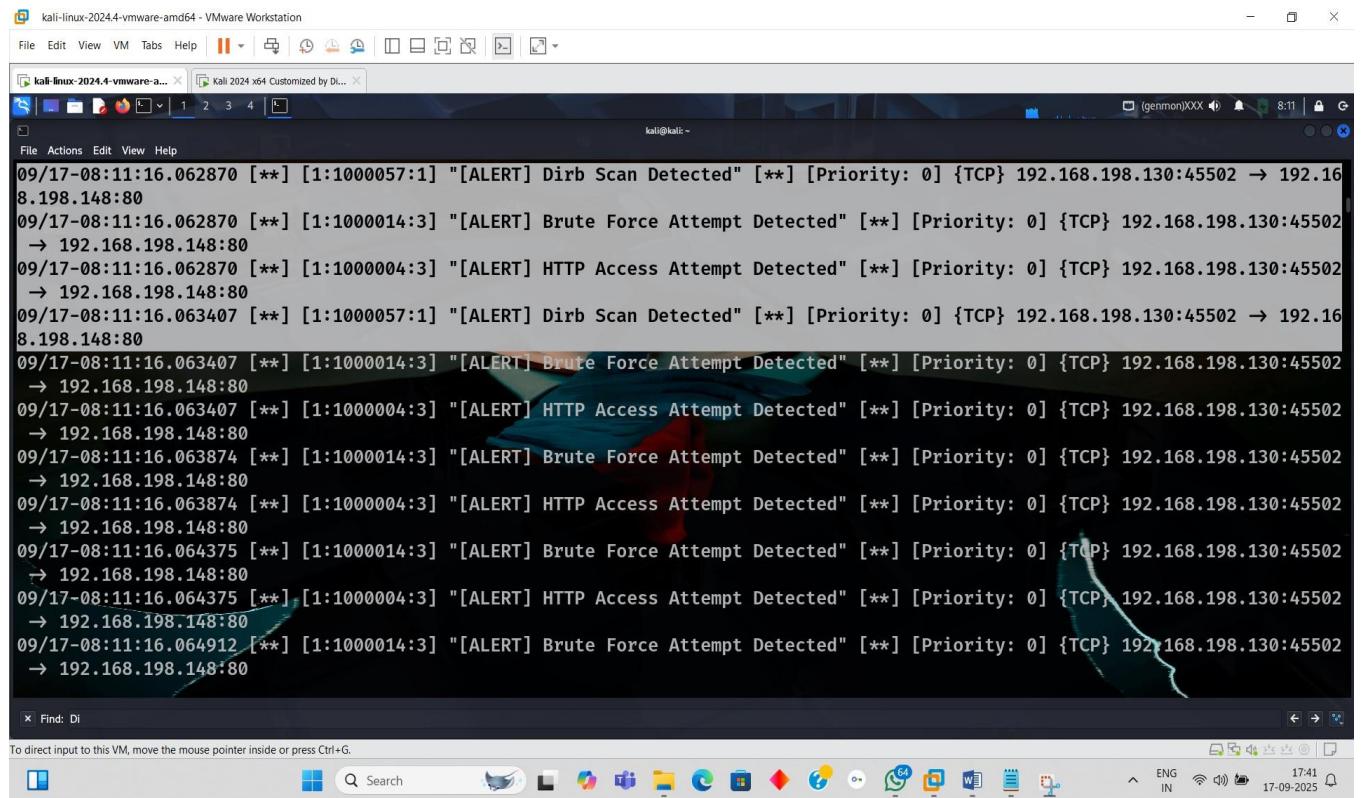
---

- 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):*

---



The screenshot shows a terminal window titled 'kali@kali: ~' running on a Kali Linux VM. The window displays a series of Snort alerts. The alerts are as follows:

```
09/17-08:11:16.062870 [**] [1:1000057:1] "[ALERT] Dirb Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.062870 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.062870 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.063407 [**] [1:1000057:1] "[ALERT] Dirb Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.063407 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.063407 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.063874 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.063874 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.064375 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.064375 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
09/17-08:11:16.064912 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:45502 → 192.168.198.148:80
```

## 22) XSS raw — SID 1000300

### Attacker (192.168.198.130):

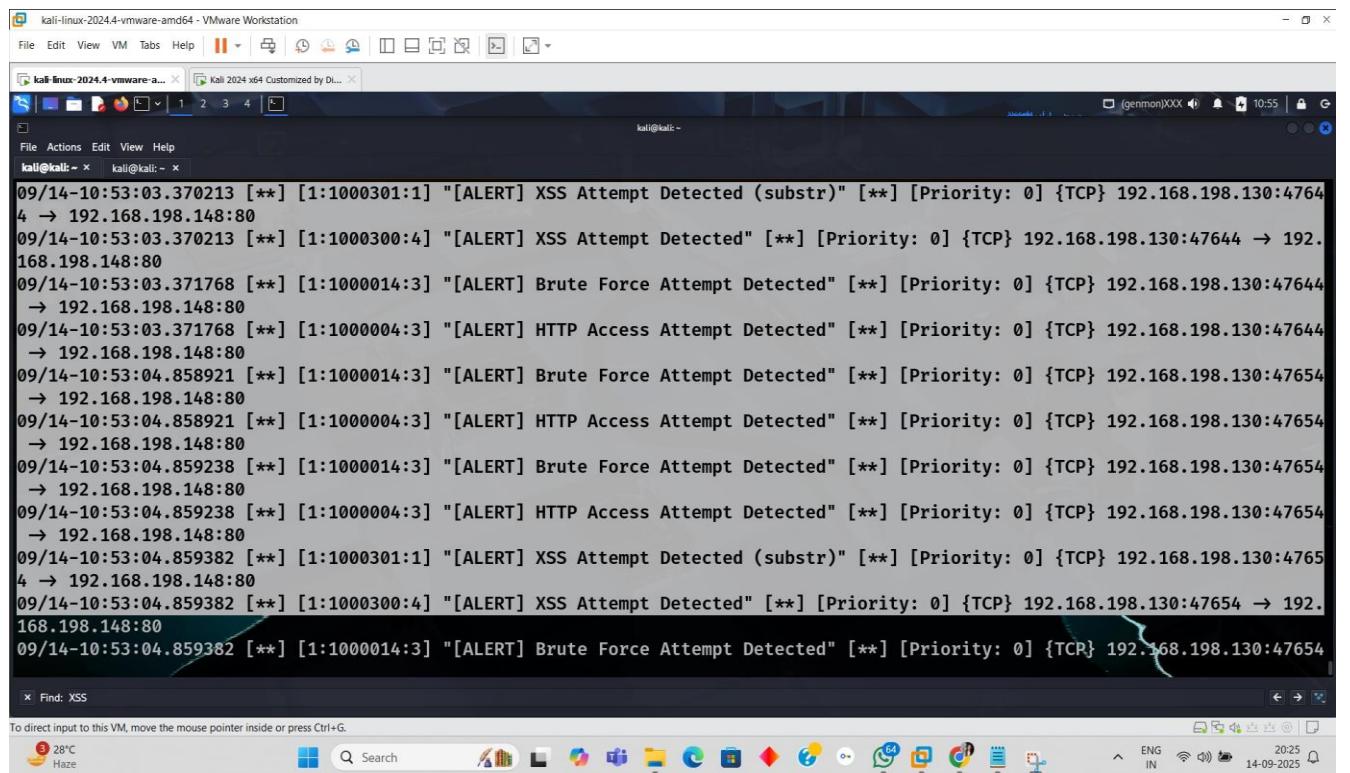
- curl -s -o /dev/null "http://192.168.198.148/index.php?q=<script>alert(1)</script>"
- for i in {1..7}; do curl -s -o /dev/null "http://192.168.198.148/index.php?q=<script>alert(1)</script>"; done

### 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):



The screenshot shows a terminal window titled 'kali@kali: ~' running on a Kali Linux VM. The window displays a series of Snort alerts for XSS attempts. The alerts are as follows:

```
09/14-10:53:03.370213 [**] [1:1000301:1] "[ALERT] XSS Attempt Detected (substr)" [**] [Priority: 0] {TCP} 192.168.198.130:47644 → 192.168.198.148:80
09/14-10:53:03.370213 [**] [1:1000300:4] "[ALERT] XSS Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47644 → 192.168.198.148:80
09/14-10:53:03.371768 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47644 → 192.168.198.148:80
09/14-10:53:03.371768 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47644 → 192.168.198.148:80
09/14-10:53:04.858921 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47654 → 192.168.198.148:80
09/14-10:53:04.858921 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47654 → 192.168.198.148:80
09/14-10:53:04.859238 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47654 → 192.168.198.148:80
09/14-10:53:04.859238 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47654 → 192.168.198.148:80
09/14-10:53:04.859382 [**] [1:1000301:1] "[ALERT] XSS Attempt Detected (substr)" [**] [Priority: 0] {TCP} 192.168.198.130:47654 → 192.168.198.148:80
09/14-10:53:04.859382 [**] [1:1000300:4] "[ALERT] XSS Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47654 → 192.168.198.148:80
09/14-10:53:04.859382 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:47654
```

The terminal also includes a 'Find: XSS' search bar at the bottom. The desktop environment at the bottom shows a taskbar with various icons and system status information.

## 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):*

---

```

kali@kali: ~
memory scale: KB
total memory: 91.041
pattern memory: 19.9863
match list memory: 30.0547
transition memory: 39
appid: MaxRss diff: 3128
appid: patterns loaded: 300

pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
09/17-08:08:48.557512 [**] [1:1000302:1] "[ALERT] XSS Attempt Detected (Encoded)" [**] [Priority: 0] {TCP} 192.168.198.130:531
54 → 192.168.198.148:80
09/17-08:08:48.557512 [**] [1:1000400:1] "[ALERT] Possible Webshell Upload Detected (.php)" [**] [Priority: 0] {TCP} 192.168.1
98.130:53154 → 192.168.198.148:80
09/17-08:08:48.560480 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:53154
→ 192.168.198.148:80
09/17-08:08:48.560480 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:53154
→ 192.168.198.148:80
09/17-08:08:49.825595 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:53166
→ 192.168.198.148:80
09/17-08:08:49.825595 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:53166
→ 192.168.198.148:80
09/17-08:08:49.826041 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:53166

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## 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

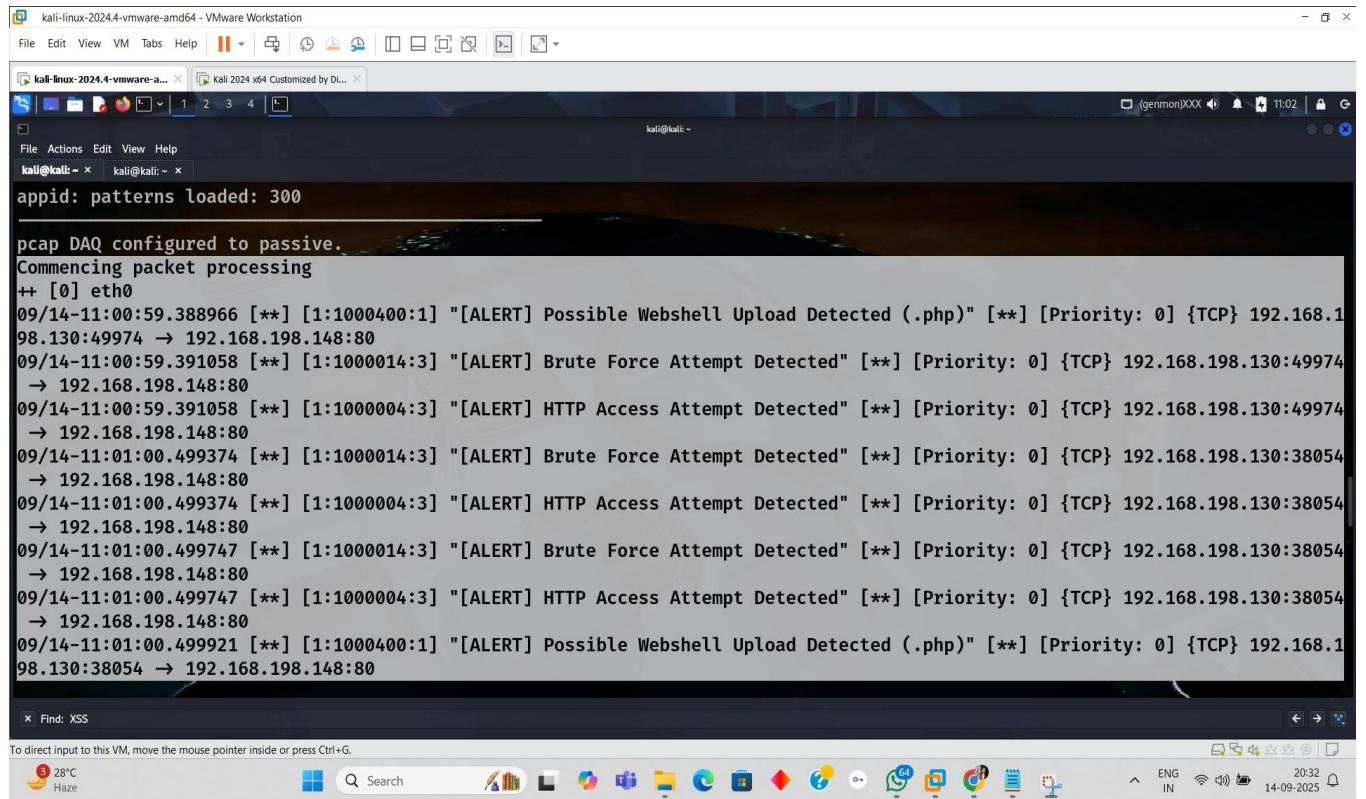
### Victim / Snort host (192.168.198.148):

- 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):*

---



The screenshot shows a terminal window on a Kali Linux desktop. The terminal output is as follows:

```
appid: patterns loaded: 300
pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
09/14-11:00:59.388966 [**] [1:1000400:1] "[ALERT] Possible Webshell Upload Detected (.php)" [**] [Priority: 0] {TCP} 192.168.198.130:49974 -> 192.168.198.148:80
09/14-11:00:59.391058 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:49974 -> 192.168.198.148:80
09/14-11:00:59.391058 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:49974 -> 192.168.198.148:80
09/14-11:00:59.391058 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38054 -> 192.168.198.148:80
09/14-11:01:00.499374 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38054 -> 192.168.198.148:80
09/14-11:01:00.499374 [**] [1:1000014:3] "[ALERT] Brute Force Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38054 -> 192.168.198.148:80
09/14-11:01:00.499374 [**] [1:1000004:3] "[ALERT] HTTP Access Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:38054 -> 192.168.198.148:80
09/14-11:01:00.499921 [**] [1:1000400:1] "[ALERT] Possible Webshell Upload Detected (.php)" [**] [Priority: 0] {TCP} 192.168.198.130:38054 -> 192.168.198.148:80
```

The desktop environment includes a taskbar with various icons and system status indicators.

## 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):**

The screenshot shows a terminal window titled "root@kali:/home/kali/Desktop" with the command "snort" running. The output displays numerous alerts from Snort, primarily regarding ICMP Echo Requests and possible DoS/DDoS attacks. The alerts are timestamped and show source and destination IP addresses. The terminal window is part of a VMware Workstation interface, with other windows visible in the background.

```
09/11-08:59:09.219900 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.219900 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.220458 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.220458 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.220898 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.220898 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.221506 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.221506 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.221885 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.221885 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.222218 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.222218 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.222533 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.222533 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.222878 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.222878 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.223226 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.223226 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.223573 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.223573 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.223930 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.223930 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.224271 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.224271 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.224688 [**] [1:1000020:2] "[ALERT] Possible DoS/DDoS Attack Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
09/11-08:59:09.224688 [**] [1:1000003:3] "[ALERT] ICMP Echo Request Detected" [**] [Priority: 0] {ICMP} 192.168.198.130 → 192.168.198.148
```

## 26) UDP packet detection — SID 1000015

**Attacker (192.168.198.130):**

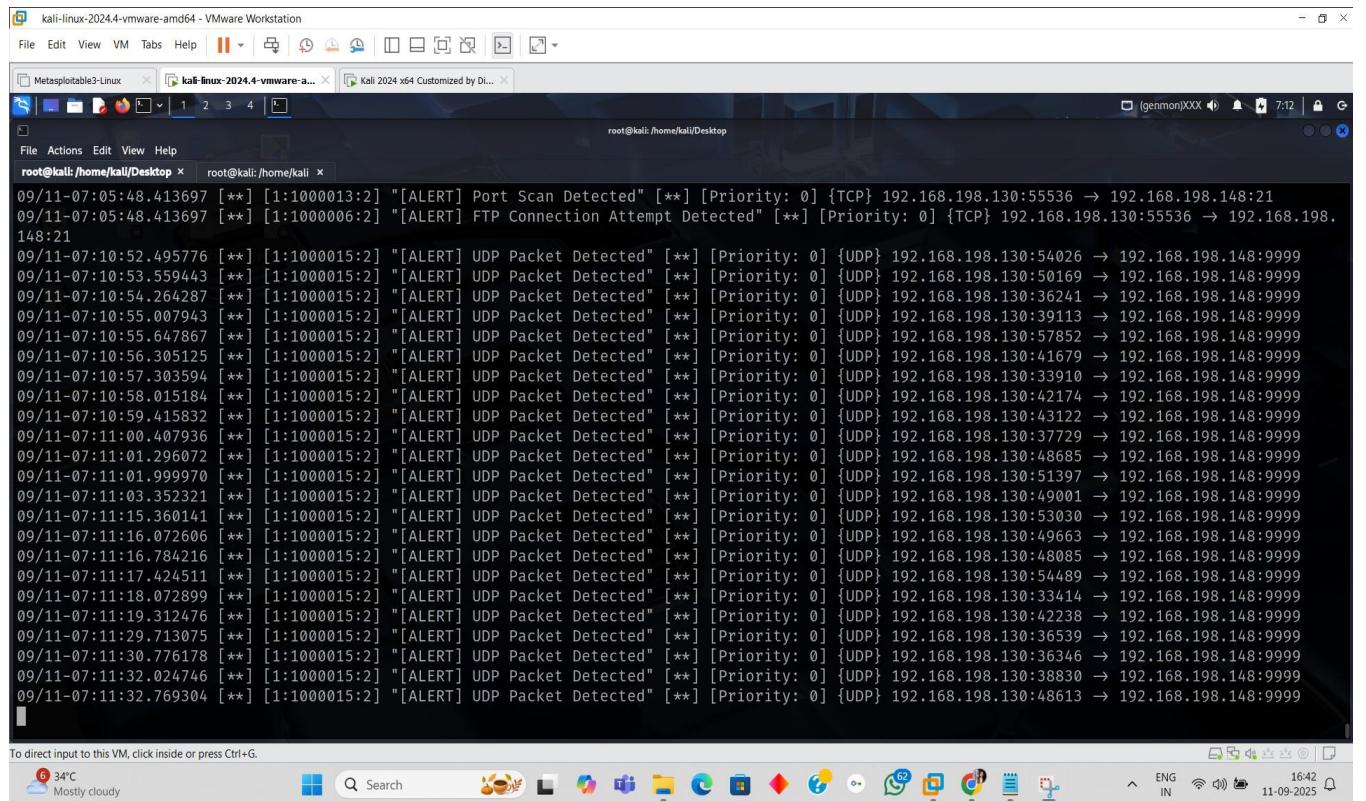
- sudo hping3 --udp -p 12345 -c 20 -i u1000 192.168.198.148

**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):**



```

root@kali: /home/kali/Desktop
root@kali: /home/kali/Desktop
09/11-07:05:48.413697 [**] [1:1000013:2] "[ALERT] Port Scan Detected" [**] [Priority: 0] {TCP} 192.168.198.130:55536 → 192.168.198.148:21
09/11-07:05:48.413697 [**] [1:1000006:2] "[ALERT] FTP Connection Attempt Detected" [**] [Priority: 0] {TCP} 192.168.198.130:55536 → 192.168.198.148:21
09/11-07:10:52.495776 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:54026 → 192.168.198.148:9999
09/11-07:10:53.559443 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:50169 → 192.168.198.148:9999
09/11-07:10:54.264287 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:36241 → 192.168.198.148:9999
09/11-07:10:55.007943 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:39113 → 192.168.198.148:9999
09/11-07:10:55.647867 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:57852 → 192.168.198.148:9999
09/11-07:10:56.305125 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:41679 → 192.168.198.148:9999
09/11-07:10:57.303594 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:33910 → 192.168.198.148:9999
09/11-07:10:58.015184 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:42174 → 192.168.198.148:9999
09/11-07:10:59.415832 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:43122 → 192.168.198.148:9999
09/11-07:11:00.407936 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:37729 → 192.168.198.148:9999
09/11-07:11:01.296072 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:48685 → 192.168.198.148:9999
09/11-07:11:01.999970 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:51397 → 192.168.198.148:9999
09/11-07:11:03.352321 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:49001 → 192.168.198.148:9999
09/11-07:11:15.360141 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:53030 → 192.168.198.148:9999
09/11-07:11:16.072606 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:49663 → 192.168.198.148:9999
09/11-07:11:16.784216 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:48085 → 192.168.198.148:9999
09/11-07:11:17.424511 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:54489 → 192.168.198.148:9999
09/11-07:11:18.072899 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:33414 → 192.168.198.148:9999
09/11-07:11:19.312476 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:42238 → 192.168.198.148:9999
09/11-07:11:29.713075 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:36539 → 192.168.198.148:9999
09/11-07:11:30.776178 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:36346 → 192.168.198.148:9999
09/11-07:11:32.024746 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:38830 → 192.168.198.148:9999
09/11-07:11:32.769304 [**] [1:1000015:2] "[ALERT] UDP Packet Detected" [**] [Priority: 0] {UDP} 192.168.198.130:48613 → 192.168.198.148:9999

```

## 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.