College Name	**University of Hertfordshire** **SEGi College Subang Jaya**		
Programme Name	**BACHELOR OF CYBERSECURITY AND NETWORKS**		
Module Name	CYBERSECURITY	Module Code	6COM1040
		Semester	**SEP 2025**
Module Leader	DR ANESHKUMAR THANGAVELOO	Assessment Type	PROJECT VULNERABILITY ASSESSMENT
Lecturer Name	MS NUR DIANA MADINAH		

Student's declaration

I hereby certify that this assignment is my own work and where materials have been used from other resources, they have been properly acknowledged. I also understand I will face the possibility of failing the module if the content of this assignment is plagiarized.

No.	**Name**	**Student ID**	**Signature / Initial**
1	TAN JIAJIAN	SCSJ1901781	TAN

Release Date		Submission Due Date		Marks obtained:
Date Received		Student's work assessed by / date		

Module Leader′s Feedback.

Contents

List of Figure

4. Testing

In this assessment, I used Nmap, tcpdump and Snort IDS to identify vulnerabilities in the test network. The target machine Ubuntu server with IP address 192.168.10.1 was hosting two services:

- Nginx on port 80
- DVWA on port 8080
- Snort IDS running in docker on Ubuntu
- Kali Linux used as attacker machine.

From these tools, I identified several vulnerabilities explained below.

Vulnerability 1 - Port 80 (HTTP) is Open Without Encryption

Evidence

From nmap

80/tcp open http

Reasoning

HTTP on port 80 sends data in plain text, including:

- Cookies
- Login information
- Session tokens
- Web requests

An attacker can capture this traffic using tcpdump or Wireshark

Risk Level

Medium to High

Because attackers in the same network can sniff traffic and steal sensitive data.

Recommended Fix

- Enable HTTPS with SSL/TLS certificates
- Redirect all HTTP traffic to HTTPS
- Disable plain HTTP if not needed

Vulnerability 2 - DVWA (Port 8080) Running in “Low Security Mode”

Evidence

From tcpdump on port 8080:

HTTP/1.1 200 OK

DVWA login page

From the browser: DVWA accessible without restriction.

Reasoning

DVWA in low security mode contains intentional vulnerabilities:

- SQL Injection
- XSS
- Insecure file upload
- Command execution
- CSRF

If a malicious user accesses DVWA, they can exploit these vulnerabilities to attack the server or compromise network.

Risk Level

High

DVWA is purposely vulnerable.

Recommended Fix

- Never expose DVWA to a real production network
- Use firewall rules to only allow trusted hosts
- Run DVWA in an isolated environment / VM only

Vulnerability 3 - Port 80 (Nginx) Traffic Not Captured by tcpdump

Evidence

- tcpdump -i enp0s8 port 80 shows no packets when Kali accesses http://192.168.10.1.
- But tcpdump -i enp0s8 port 8080 shows GET / 200 OK when accessing DVWA.
- This means port 80 traffic is not passing through enp0s8.

Reasoning

Nginx on port 80 is likely bound to the NAT interface, not the internal network interface enp0s8.

Because of this, tcpdump and Snort cannot see or monitor port 80 traffic, creating a monitoring gap.

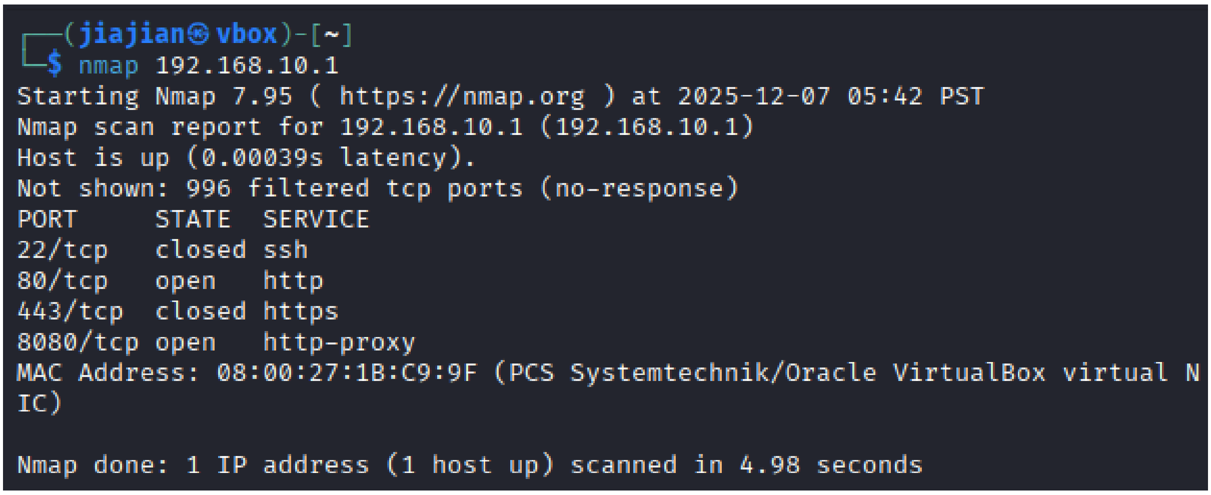
Risk Level

Critical - Attacks on port 80 bypass Snort and tcpdump, allowing undetected exploitation of the web server.

Recommended Fix

- Bind Nginx to the internal network IP (192.168.10.1).
- Re-run the container with correct port mapping.

- Verify that port 80 traffic goes through enp0s8 so Snort and tcpdump can inspect it.

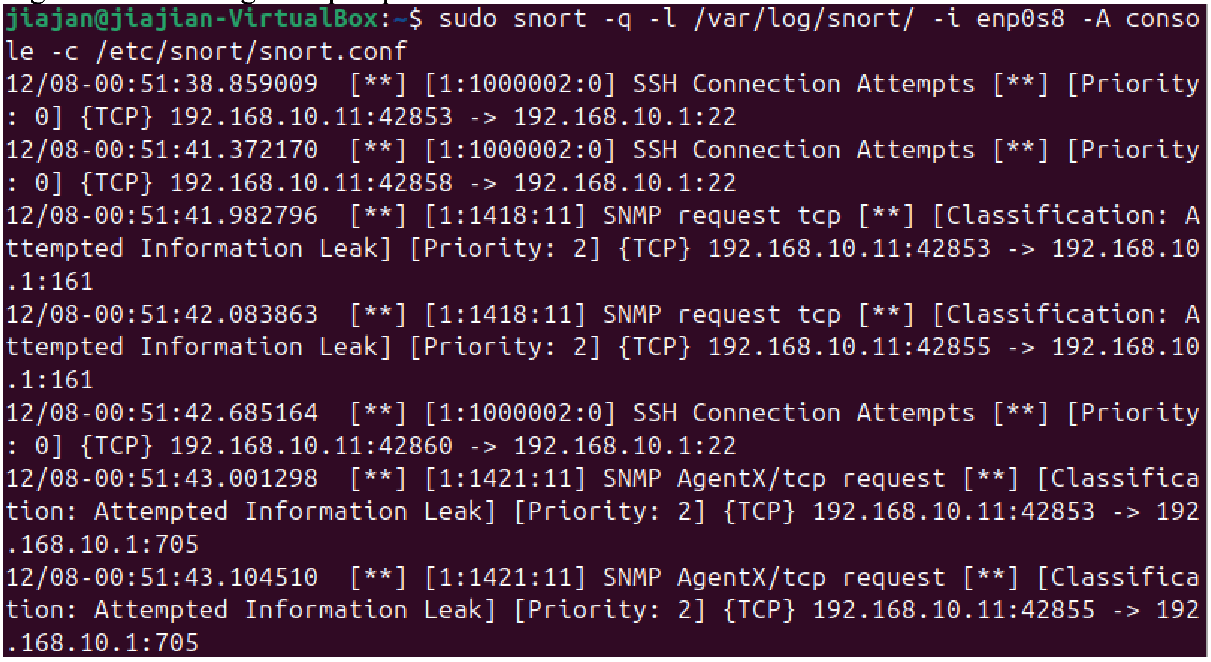


```
┌──(jiajian㉿vbox)-[~]
└─$ nmap 192.168.10.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 05:42 PST
Nmap scan report for 192.168.10.1 (192.168.10.1)
Host is up (0.00039s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
443/tcp  closed https
8080/tcp open   http-proxy
MAC Address: 08:00:27:1B:C9:9F (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds
```

Figure 1

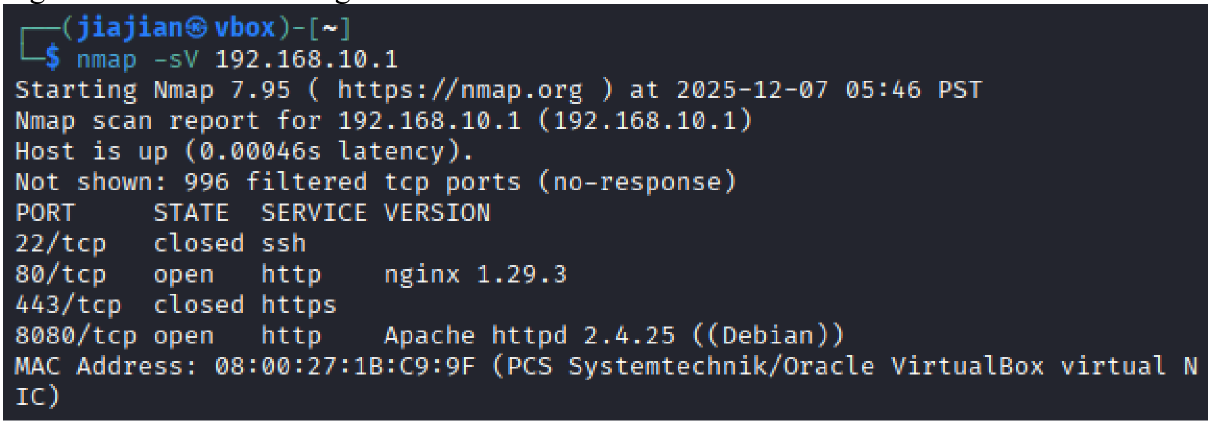
Figure 34 is finding the open ports on Ubuntu.



```
jiajan@jiajian-VirtualBox:~$ sudo snort -q -l /var/log/snort/ -i enp0s8 -A conso
le -c /etc/snort/snort.conf
12/08-00:51:38.859009  [**] [1:1000002:0] SSH Connection Attempts [**] [Priority
: 0] {TCP} 192.168.10.11:42853 -> 192.168.10.1:22
12/08-00:51:41.372170  [**] [1:1000002:0] SSH Connection Attempts [**] [Priority
: 0] {TCP} 192.168.10.11:42858 -> 192.168.10.1:22
12/08-00:51:41.982796  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:42853 -> 192.168.10
.1:161
12/08-00:51:42.083863  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:42855 -> 192.168.10
.1:161
12/08-00:51:42.685164  [**] [1:1000002:0] SSH Connection Attempts [**] [Priority
: 0] {TCP} 192.168.10.11:42860 -> 192.168.10.1:22
12/08-00:51:43.001298  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:42853 -> 192
.168.10.1:705
12/08-00:51:43.104510  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:42855 -> 192
.168.10.1:705
```

Figure 2

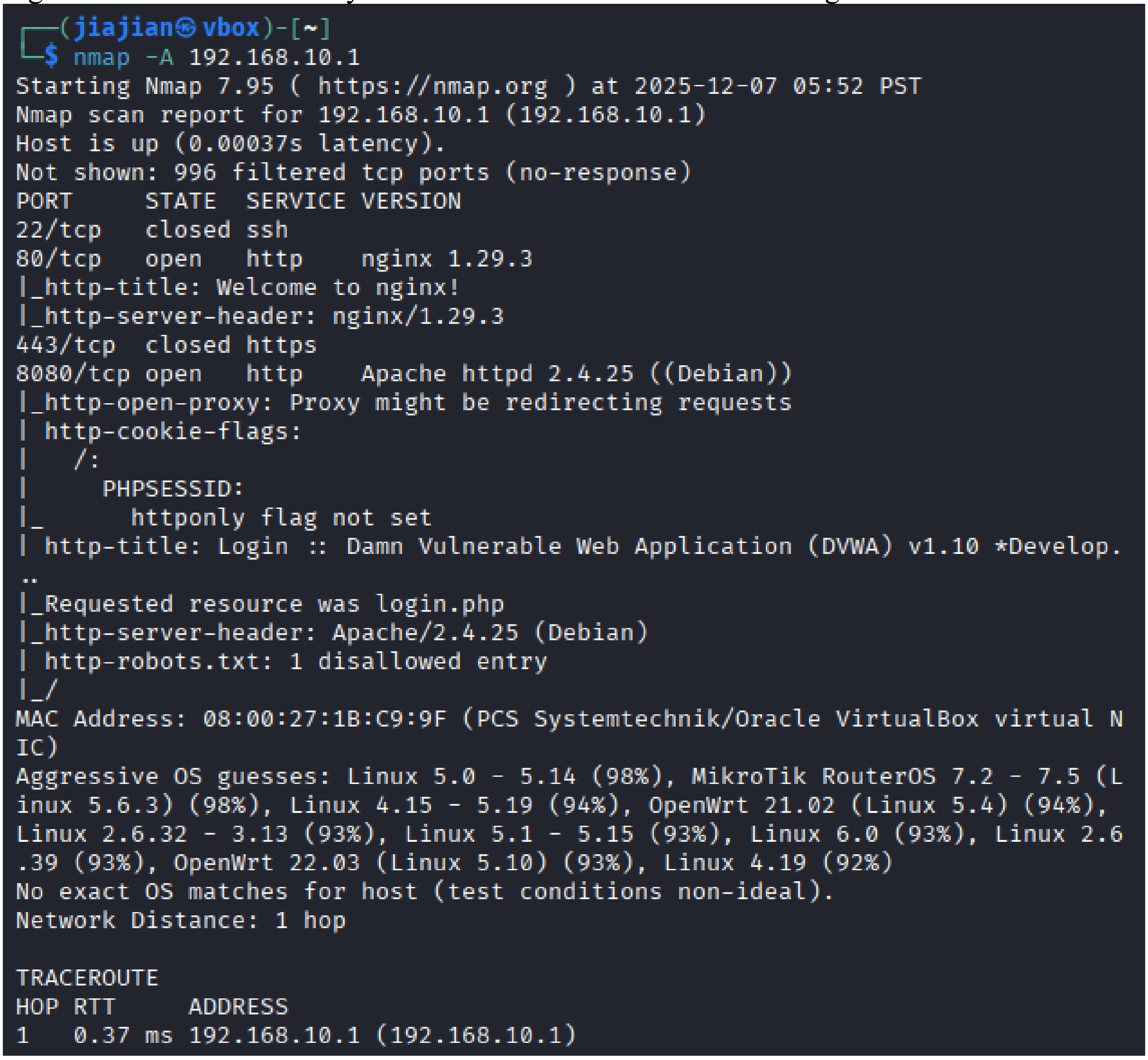
Figure 35 shows all the log.



```
┌──(jiajian㉿vbox)-[~]
└─$ nmap -sV 192.168.10.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 05:46 PST
Nmap scan report for 192.168.10.1 (192.168.10.1)
Host is up (0.00046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
22/tcp   closed ssh
80/tcp   open   http    nginx 1.29.3
443/tcp  closed https
8080/tcp open   http    Apache httpd 2.4.25 ((Debian))
MAC Address: 08:00:27:1B:C9:9F (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
```

Figure 3

Figure 36 commands identify what services and versions are running.

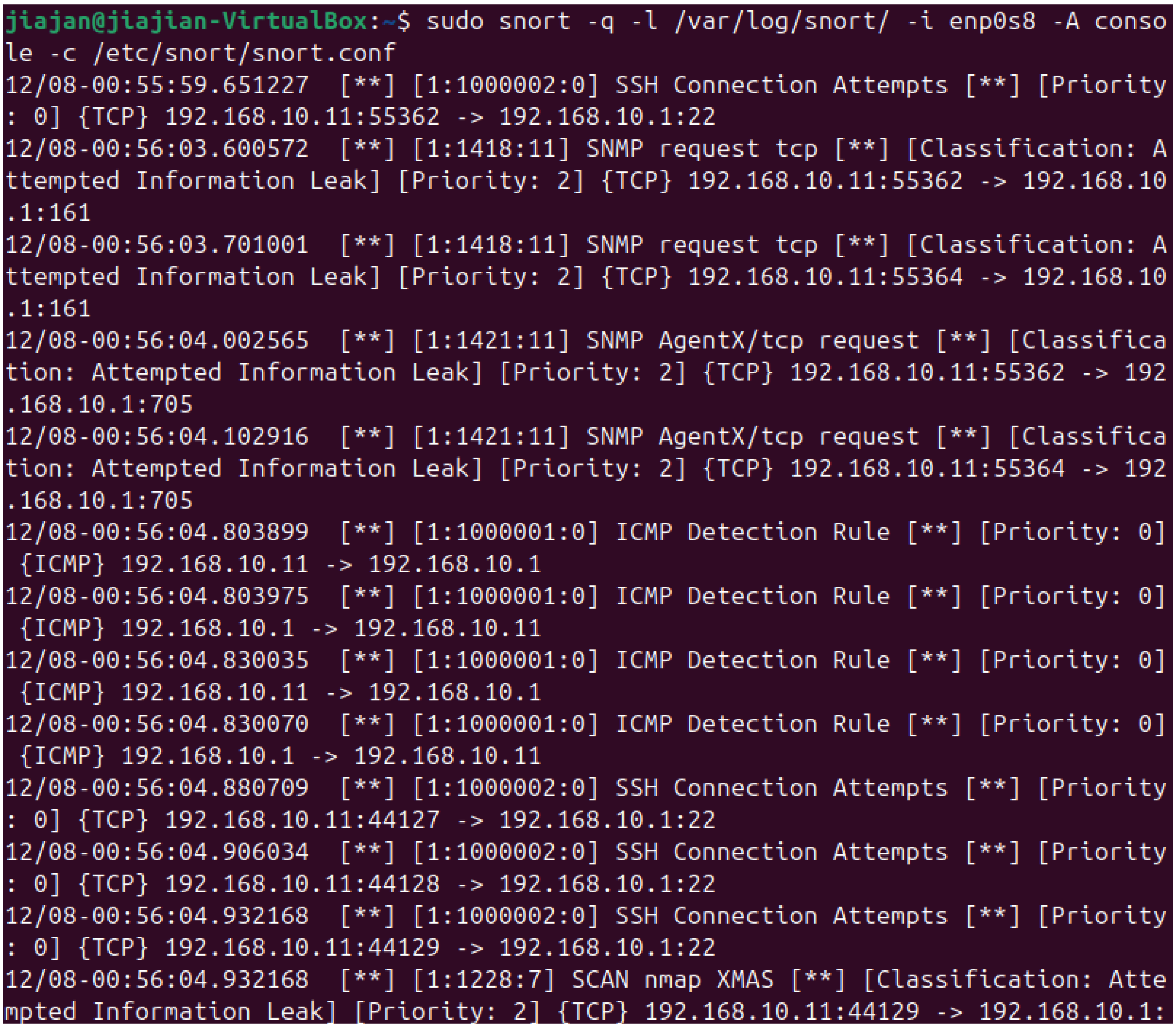


```
┌──(jiajian㉿vbox)-[~]
└─$ nmap -A 192.168.10.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 05:52 PST
Nmap scan report for 192.168.10.1 (192.168.10.1)
Host is up (0.00037s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
22/tcp   closed ssh
80/tcp   open   http    nginx 1.29.3
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.29.3
443/tcp  closed https
8080/tcp open   http    Apache httpd 2.4.25 ((Debian))
|_http-open-proxy: Proxy might be redirecting requests
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Develop.
..
|_Requested resource was login.php
|_http-server-header: Apache/2.4.25 (Debian)
| http-robots.txt: 1 disallowed entry
|_/
MAC Address: 08:00:27:1B:C9:9F (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Aggressive OS guesses: Linux 5.0 - 5.14 (98%), MikroTik RouterOS 7.2 - 7.5 (L
inux 5.6.3) (98%), Linux 4.15 - 5.19 (94%), OpenWrt 21.02 (Linux 5.4) (94%),
Linux 2.6.32 - 3.13 (93%), Linux 5.1 - 5.15 (93%), Linux 6.0 (93%), Linux 2.6
.39 (93%), OpenWrt 22.03 (Linux 5.10) (93%), Linux 4.19 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 192.168.10.1 (192.168.10.1)
```

Figure 4

Figure 37 commands used to aggressive scan and this scan performs OS detection, version detection and traceroute.

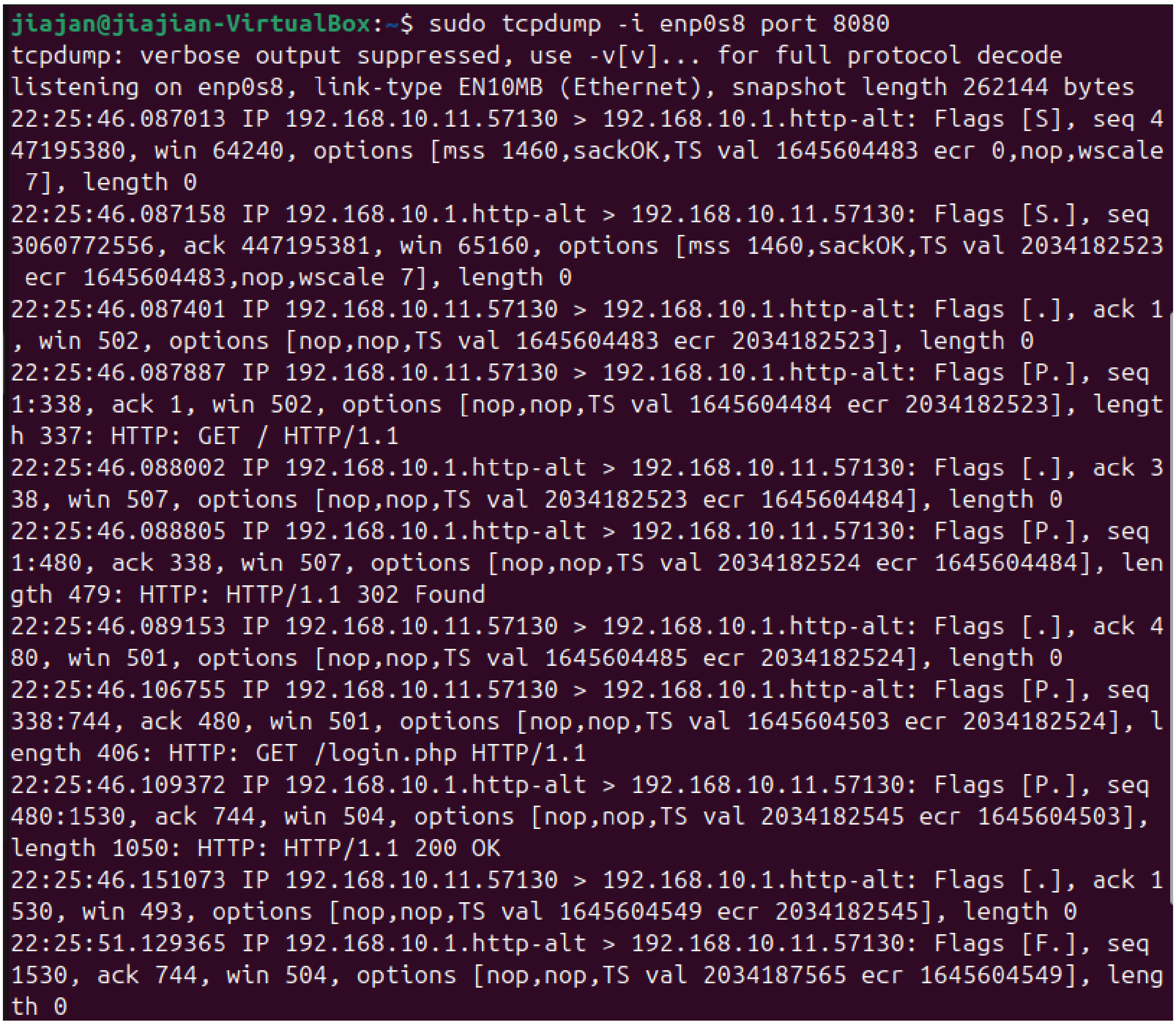


```
jiajan@jiajian-VirtualBox:~$ sudo snort -q -l /var/log/snort/ -i enp0s8 -A conso
le -c /etc/snort/snort.conf
12/08-00:55:59.651227  [**] [1:1000002:0] SSH Connection Attempts [**] [Priority
: 0] {TCP} 192.168.10.11:55362 -> 192.168.10.1:22
12/08-00:56:03.600572  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:55362 -> 192.168.10
.1:161
12/08-00:56:03.701001  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:55364 -> 192.168.10
.1:161
12/08-00:56:04.002565  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:55362 -> 192
.168.10.1:705
12/08-00:56:04.102916  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 192.168.10.11:55364 -> 192
.168.10.1:705
12/08-00:56:04.803899  [**] [1:1000001:0] ICMP Detection Rule [**] [Priority: 0]
 {ICMP} 192.168.10.11 -> 192.168.10.1
12/08-00:56:04.803975  [**] [1:1000001:0] ICMP Detection Rule [**] [Priority: 0]
 {ICMP} 192.168.10.1 -> 192.168.10.11
12/08-00:56:04.830035  [**] [1:1000001:0] ICMP Detection Rule [**] [Priority: 0]
 {ICMP} 192.168.10.11 -> 192.168.10.1
12/08-00:56:04.830070  [**] [1:1000001:0] ICMP Detection Rule [**] [Priority: 0]
 {ICMP} 192.168.10.1 -> 192.168.10.11
12/08-00:56:04.880709  [**] [1:1000002:0] SSH Connection Attempts [**] [Priority
: 0] {TCP} 192.168.10.11:44127 -> 192.168.10.1:22
12/08-00:56:04.906034  [**] [1:1000002:0] SSH Connection Attempts [**] [Priority
: 0] {TCP} 192.168.10.11:44128 -> 192.168.10.1:22
12/08-00:56:04.932168  [**] [1:1000002:0] SSH Connection Attempts [**] [Priority
: 0] {TCP} 192.168.10.11:44129 -> 192.168.10.1:22
12/08-00:56:04.932168  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.10.11:44129 -> 192.168.10.1:
```

Figure 5

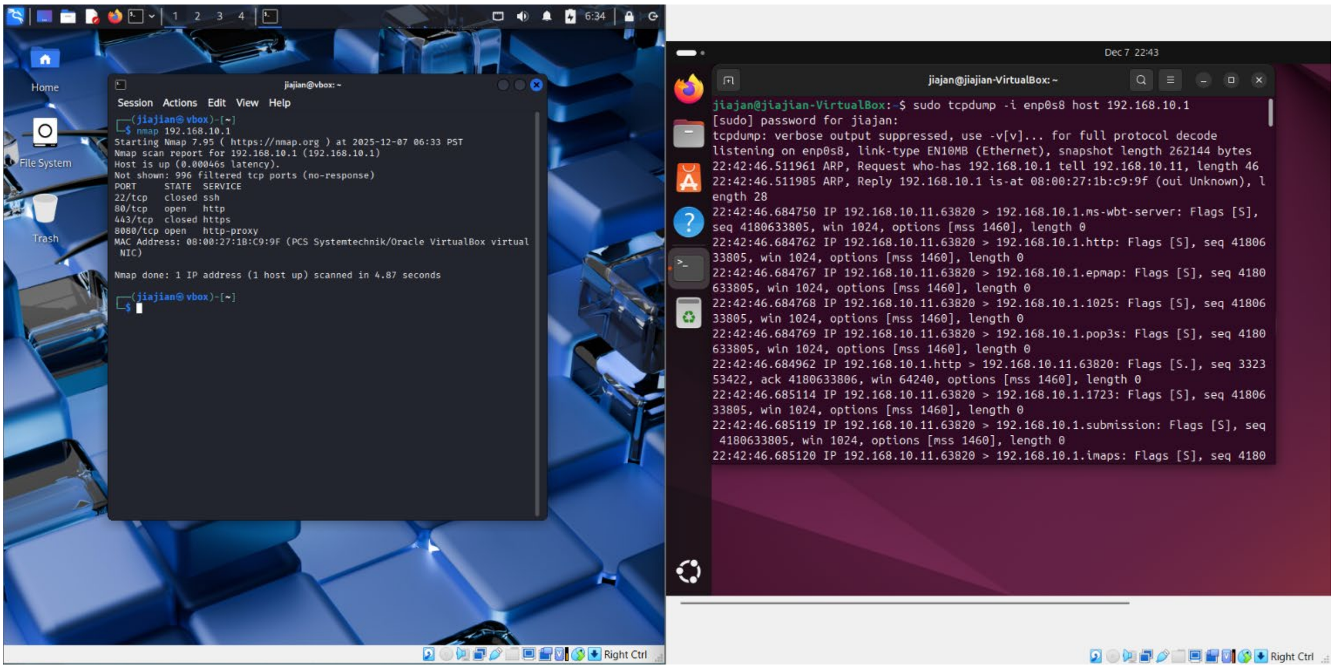
Figure 38 also shows all the logs.

Next, to capture HTTP Traffic using tcpdump, run tcpdump on Ubuntu and on Kali-Tester open the browser and type http://192.168.10.1:8080. The output will show GET/HTTP/1.1 and HTTP/1.1 200 OK.



```
jiajan@jiajian-VirtualBox:~$ sudo tcpdump -i enp0s8 port 8080
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:25:46.087013 IP 192.168.10.11.57130 > 192.168.10.1.http-alt: Flags [S], seq 4
47195380, win 64240, options [mss 1460,sackOK,TS val 1645604483 ecr 0,nop,wscale
 7], length 0
22:25:46.087158 IP 192.168.10.1.http-alt > 192.168.10.11.57130: Flags [S.], seq
3060772556, ack 447195381, win 65160, options [mss 1460,sackOK,TS val 2034182523
 ecr 1645604483,nop,wscale 7], length 0
22:25:46.087401 IP 192.168.10.11.57130 > 192.168.10.1.http-alt: Flags [.], ack 1
, win 502, options [nop,nop,TS val 1645604483 ecr 2034182523], length 0
22:25:46.087887 IP 192.168.10.11.57130 > 192.168.10.1.http-alt: Flags [P.], seq
1:338, ack 1, win 502, options [nop,nop,TS val 1645604484 ecr 2034182523], lengt
h 337: HTTP: GET / HTTP/1.1
22:25:46.088002 IP 192.168.10.1.http-alt > 192.168.10.11.57130: Flags [.], ack 3
38, win 507, options [nop,nop,TS val 2034182523 ecr 1645604484], length 0
22:25:46.088805 IP 192.168.10.1.http-alt > 192.168.10.11.57130: Flags [P.], seq
1:480, ack 338, win 507, options [nop,nop,TS val 2034182524 ecr 1645604484], len
gth 479: HTTP: HTTP/1.1 302 Found
22:25:46.089153 IP 192.168.10.11.57130 > 192.168.10.1.http-alt: Flags [.], ack 4
80, win 501, options [nop,nop,TS val 1645604485 ecr 2034182524], length 0
22:25:46.106755 IP 192.168.10.11.57130 > 192.168.10.1.http-alt: Flags [P.], seq
338:744, ack 480, win 501, options [nop,nop,TS val 1645604503 ecr 2034182524], l
ength 406: HTTP: GET /login.php HTTP/1.1
22:25:46.109372 IP 192.168.10.1.http-alt > 192.168.10.11.57130: Flags [P.], seq
480:1530, ack 744, win 504, options [nop,nop,TS val 2034182545 ecr 1645604503],
length 1050: HTTP: HTTP/1.1 200 OK
22:25:46.151073 IP 192.168.10.11.57130 > 192.168.10.1.http-alt: Flags [.], ack 1
530, win 493, options [nop,nop,TS val 1645604549 ecr 2034182545], length 0
22:25:51.129365 IP 192.168.10.1.http-alt > 192.168.10.11.57130: Flags [F.], seq
1530, ack 744, win 504, options [nop,nop,TS val 2034187565 ecr 1645604549], leng
th 0
```

Figure 6



```
┌──(jiajian㉿vbox)-[~]
└─$ nmap 192.168.10.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 06:33 PST
Nmap scan report for 192.168.10.1 (192.168.10.1)
Host is up (0.00046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
443/tcp  closed https
8080/tcp open   http-proxy
MAC Address: 08:00:27:1B:C9:9F (PCS Systemtechnik/Oracle VirtualBox virtual
 NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds

┌──(jiajian㉿vbox)-[~]
└─$ 
```

```
jiajan@jiajian-VirtualBox:~$ sudo tcpdump -i enp0s8 host 192.168.10.1
[sudo] password for jiajan:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:42:46.511961 ARP, Request who-has 192.168.10.1 tell 192.168.10.11, length 46
22:42:46.511985 ARP, Reply 192.168.10.1 is-at 08:00:27:1b:c9:9f (oui Unknown), l
ength 28
22:42:46.684750 IP 192.168.10.11.63820 > 192.168.10.1.ms-wbt-server: Flags [S],
seq 4180633805, win 1024, options [mss 1460], length 0
22:42:46.684762 IP 192.168.10.11.63820 > 192.168.10.1.http: Flags [S], seq 41806
33805, win 1024, options [mss 1460], length 0
22:42:46.684767 IP 192.168.10.11.63820 > 192.168.10.1.epmap: Flags [S], seq 4180
633805, win 1024, options [mss 1460], length 0
22:42:46.684768 IP 192.168.10.11.63820 > 192.168.10.1.1025: Flags [S], seq 41806
33805, win 1024, options [mss 1460], length 0
22:42:46.684769 IP 192.168.10.11.63820 > 192.168.10.1.pop3s: Flags [S], seq 4180
633805, win 1024, options [mss 1460], length 0
22:42:46.684962 IP 192.168.10.1.http > 192.168.10.11.63820: Flags [S.], seq 3323
53422, ack 4180633806, win 64240, options [mss 1460], length 0
22:42:46.685114 IP 192.168.10.11.63820 > 192.168.10.1.1723: Flags [S], seq 41806
33805, win 1024, options [mss 1460], length 0
22:42:46.685119 IP 192.168.10.11.63820 > 192.168.10.1.submission: Flags [S], seq
 4180633805, win 1024, options [mss 1460], length 0
22:42:46.685120 IP 192.168.10.11.63820 > 192.168.10.1.imaps: Flags [S], seq 4180
```

Figure 7

Figure 40 is capture nmap scan traffic, from Ubuntu run the command and on Kali-Tester run namp 192.168.10.1. The tcpdump will show the log.