NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

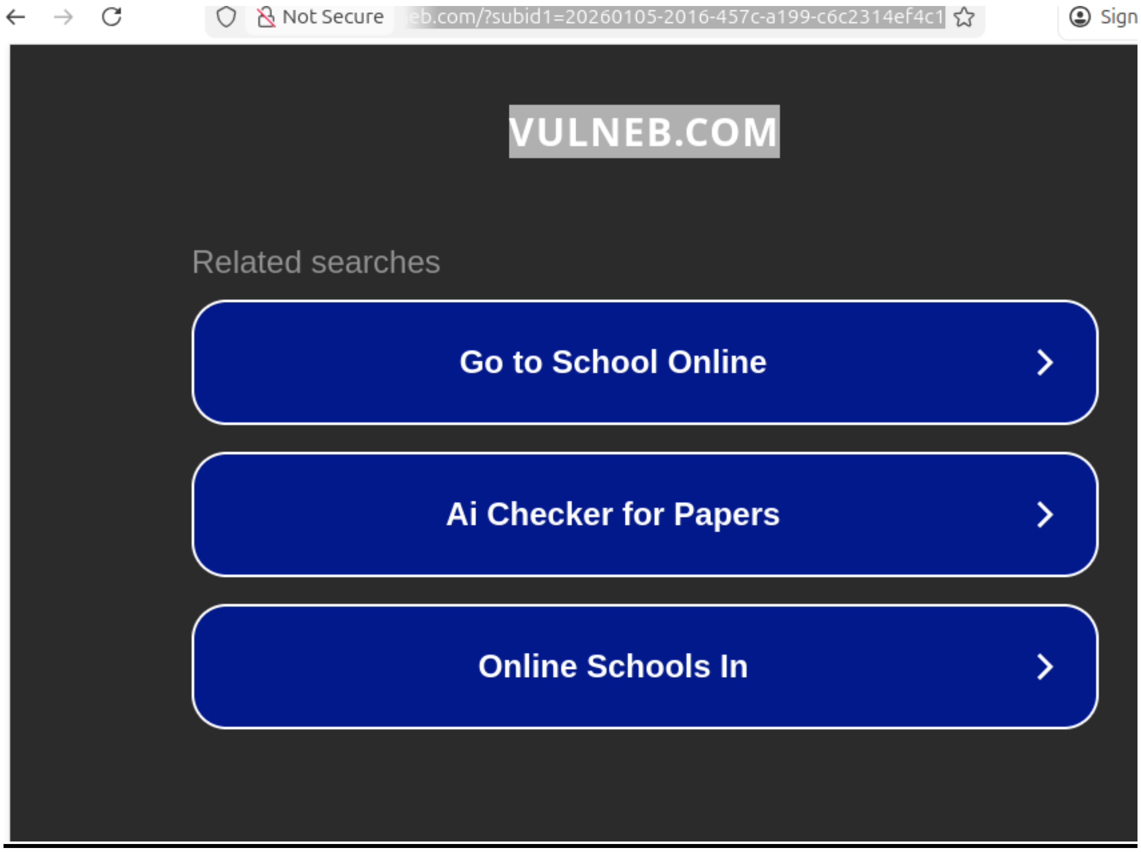
DEPARTMENT OF COMPUTER SCIENCE

INFORMATION SECURITY LAB

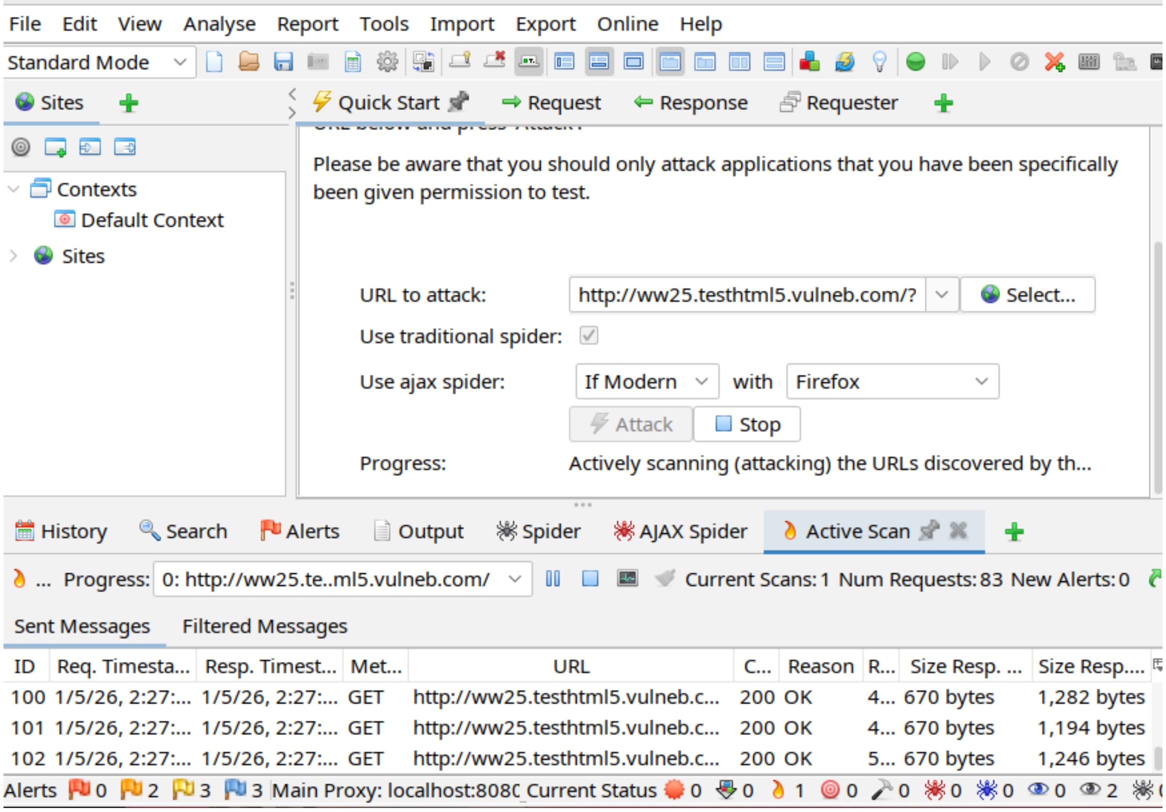
NAME	Ayesha Imran
Class	CS-A
Lab	Final
Course	Information Security
Date	5th -January-26
Submitted To	Lec. Attiya Ashraf

LAB TASKS

Question 01:



Enter Zaproxy:



Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://ww25.testhtml5.vulneb.com/?

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

Progress: Actively scanning (attacking) the URLs discovered by th...

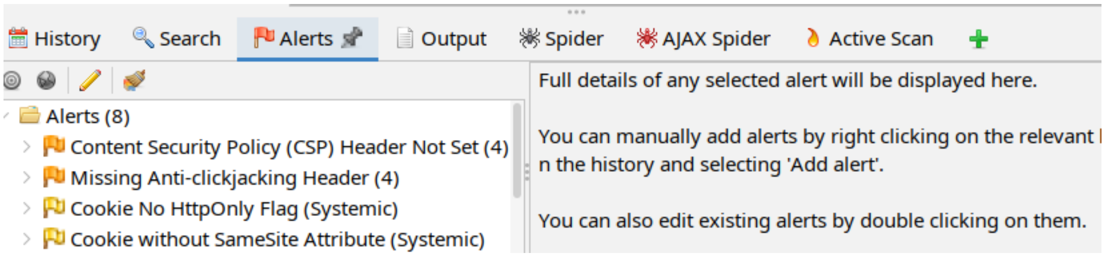
... Progress: 0: http://ww25.te..ml5.vulneb.com/ Current Scans: 1 Num Requests: 83 New Alerts: 0

ID	Req. Timesta...	Resp. Timest...	Met...	URL	C...	Reason	R...	Size Resp. ...	Size Resp....
100	1/5/26, 2:27:...	1/5/26, 2:27:...	GET	http://ww25.testhtml5.vulneb.c...	200	OK	4...	670 bytes	1,282 bytes
101	1/5/26, 2:27:...	1/5/26, 2:27:...	GET	http://ww25.testhtml5.vulneb.c...	200	OK	4...	670 bytes	1,194 bytes
102	1/5/26, 2:27:...	1/5/26, 2:27:...	GET	http://ww25.testhtml5.vulneb.c...	200	OK	5...	670 bytes	1,246 bytes

Alerts 0 2 3 3 Main Proxy: localhost:8080 Current Status 0 0 1 0 0 0 0 0 2

Alerts:

The vulnerability is that the website doesnot uses secure protocol and it was missing content Security Policy Header



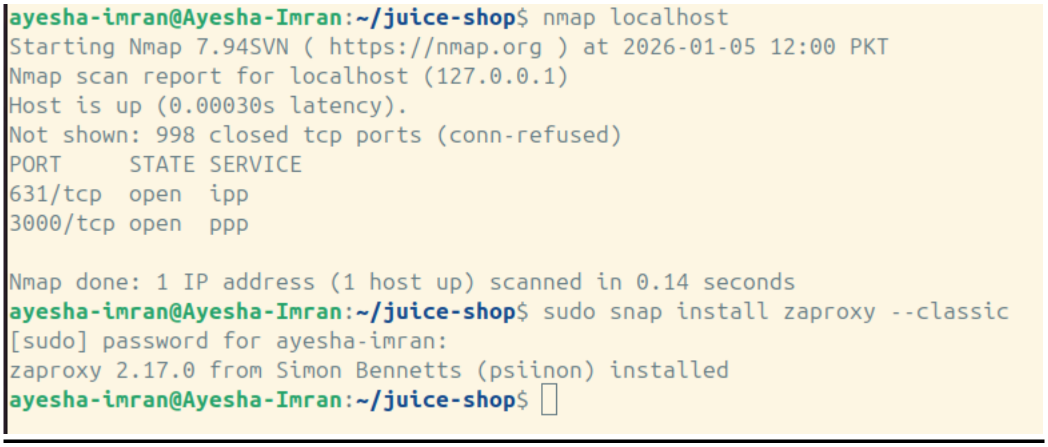
Alerts (8)
- Content Security Policy (CSP) Header Not Set (4)
- Missing Anti-clickjacking Header (4)
- Cookie No HttpOnly Flag (Systemic)
- Cookie without SameSite Attribute (Systemic)

Full details of any selected alert will be displayed here.

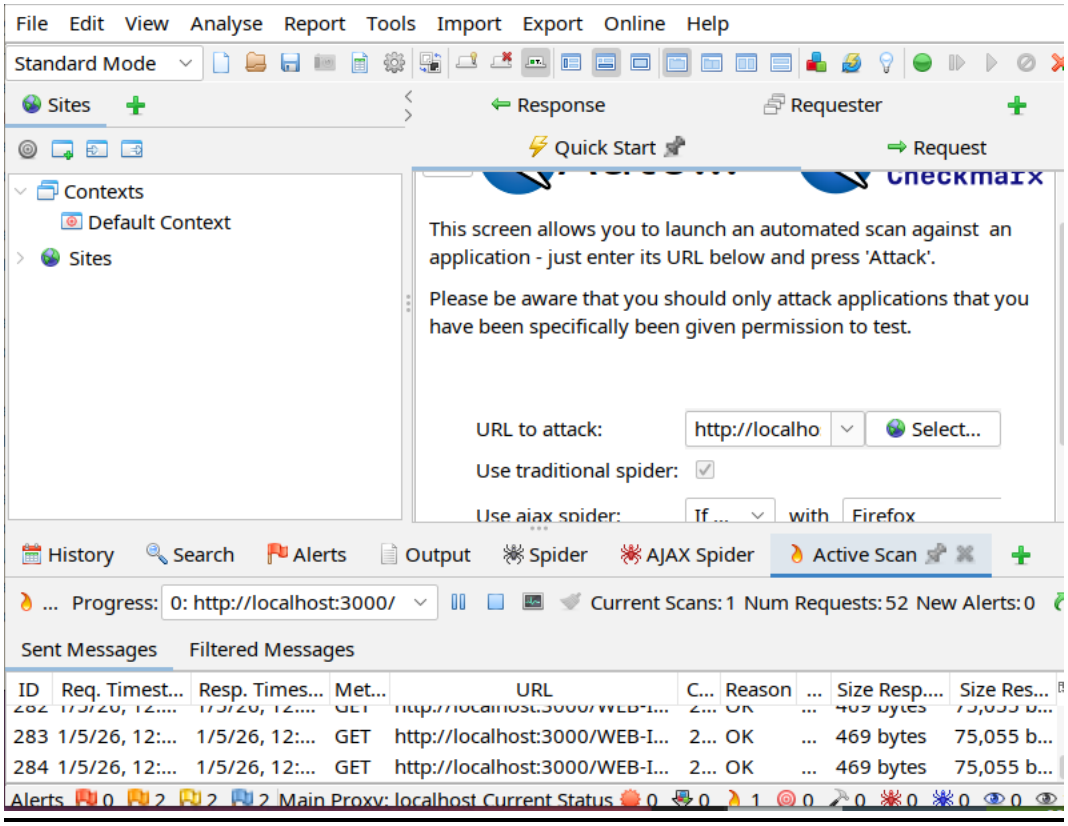
You can manually add alerts by right clicking on the relevant l n the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Juice Shop:



```
ayesha-imran@Ayesha-Imran:~/juice-shop$ nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-05 12:00 PKT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00030s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
631/tcp  open  ipp
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
ayesha-imran@Ayesha-Imran:~/juice-shop$ sudo snap install zaproxy --classic
[sudo] password for ayesha-imran:
zaproxy 2.17.0 from Simon Bennetts (psiinon) installed
ayesha-imran@Ayesha-Imran:~/juice-shop$ 
```



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://localho Select...

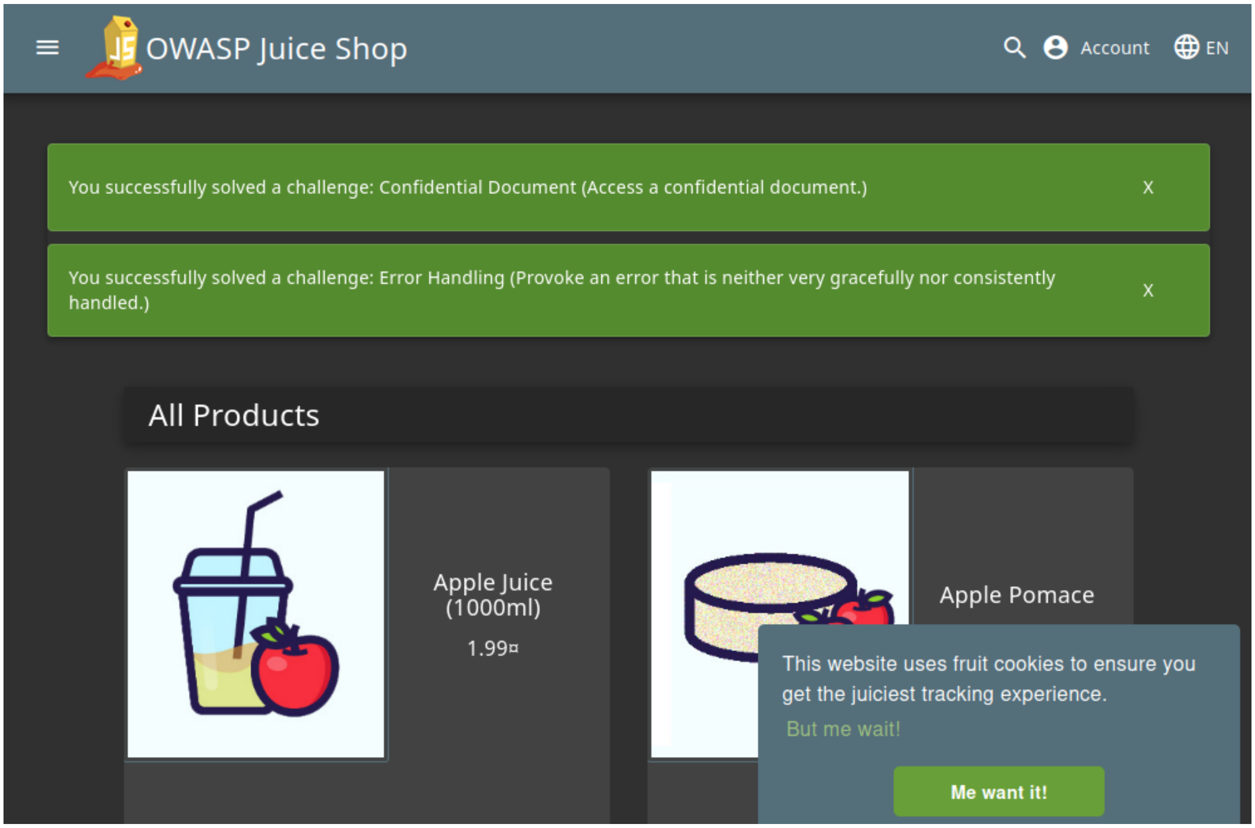
Use traditional spider: ☑

Use ajax spider: If ... with Firefox

... Progress: 0: http://localhost:3000/ Current Scans: 1 Num Requests: 52 New Alerts: 0

ID	Req. Timest...	Resp. Times...	Met...	URL	C...	Reason	...	Size Resp....	Size Res...
282	1/5/26, 12:...	1/5/26, 12:...	GET	http://localhost:3000/WEB-I...	2...	OK	...	469 bytes	75,055 b...
283	1/5/26, 12:...	1/5/26, 12:...	GET	http://localhost:3000/WEB-I...	2...	OK	...	469 bytes	75,055 b...
284	1/5/26, 12:...	1/5/26, 12:...	GET	http://localhost:3000/WEB-I...	2...	OK	...	469 bytes	75,055 b...

Alerts 0 2 2 2 Main Proxy: localhost Current Status 0 0 1 0 0 0 0 0



You successfully solved a challenge: Confidential Document (Access a confidential document.)

You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

All Products

Apple Juice (1000ml) 1.99¤

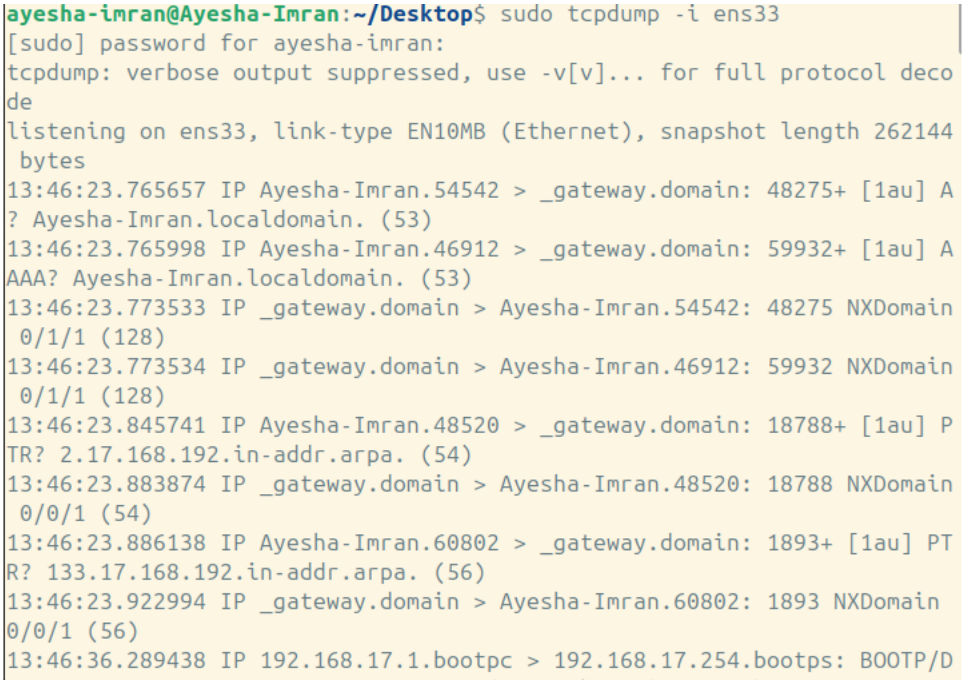
Apple Pomace

This website uses fruit cookies to ensure you get the juiciest tracking experience.

Question 02:

Command: tcpdump -I ens33

This command is to capture the traffic from Ethernet interface . It captures the live traffic of all the protocols.

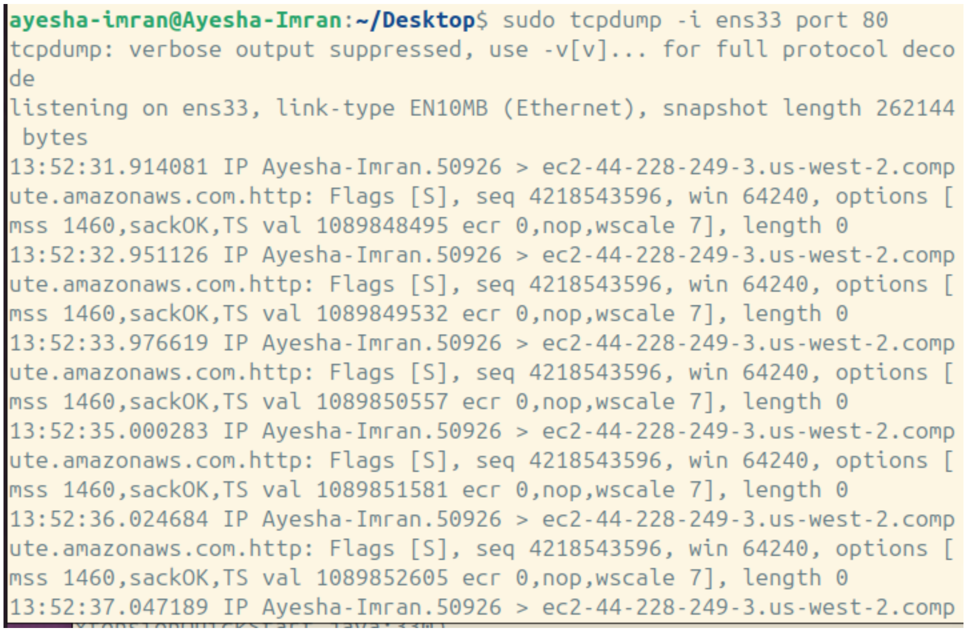


```
ayesha-imran@Ayesha-Imran:~/Desktop$ sudo tcpdump -i ens33
[sudo] password for ayesha-imran:
tcpdump: verbose output suppressed, use -v[v]... for full protocol deco
de
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144
 bytes
13:46:23.765657 IP Ayesha-Imran.54542 > _gateway.domain: 48275+ [1au] A
? Ayesha-Imran.localdomain. (53)
13:46:23.765998 IP Ayesha-Imran.46912 > _gateway.domain: 59932+ [1au] A
AAA? Ayesha-Imran.localdomain. (53)
13:46:23.773533 IP _gateway.domain > Ayesha-Imran.54542: 48275 NXDomain
 0/1/1 (128)
13:46:23.773534 IP _gateway.domain > Ayesha-Imran.46912: 59932 NXDomain
 0/1/1 (128)
13:46:23.845741 IP Ayesha-Imran.48520 > _gateway.domain: 18788+ [1au] P
TR? 2.17.168.192.in-addr.arpa. (54)
13:46:23.883874 IP _gateway.domain > Ayesha-Imran.48520: 18788 NXDomain
 0/0/1 (54)
13:46:23.886138 IP Ayesha-Imran.60802 > _gateway.domain: 1893+ [1au] PT
R? 133.17.168.192.in-addr.arpa. (56)
13:46:23.922994 IP _gateway.domain > Ayesha-Imran.60802: 1893 NXDomain
0/0/1 (56)
13:46:36.289438 IP 192.168.17.1.bootpc > 192.168.17.254.bootps: BOOTP/D
```

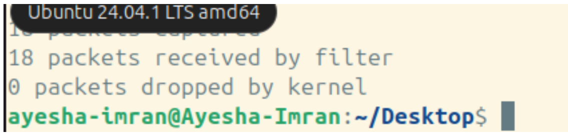
2.

Command : sudo tcpdump –I ens33 port 80 // http

By filtering the traffic we can observe the packets of our own protocol like udp, tcp, http which makes easier to analyze the task.



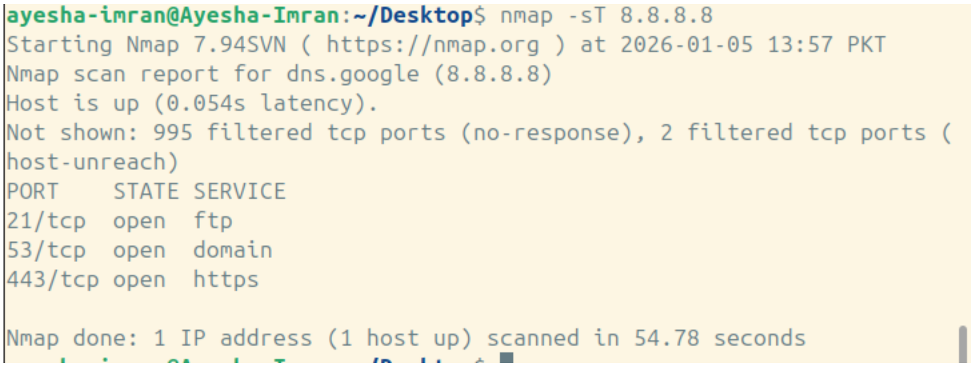
```
ayesha-imran@Ayesha-Imran:~/Desktop$ sudo tcpdump -i ens33 port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol deco
de
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144
 bytes
13:52:31.914081 IP Ayesha-Imran.50926 > ec2-44-228-249-3.us-west-2.comp
ute.amazonaws.com.http: Flags [S], seq 4218543596, win 64240, options [
mss 1460,sackOK,TS val 1089848495 ecr 0,nop,wscale 7], length 0
13:52:32.951126 IP Ayesha-Imran.50926 > ec2-44-228-249-3.us-west-2.comp
ute.amazonaws.com.http: Flags [S], seq 4218543596, win 64240, options [
mss 1460,sackOK,TS val 1089849532 ecr 0,nop,wscale 7], length 0
13:52:33.976619 IP Ayesha-Imran.50926 > ec2-44-228-249-3.us-west-2.comp
ute.amazonaws.com.http: Flags [S], seq 4218543596, win 64240, options [
mss 1460,sackOK,TS val 1089850557 ecr 0,nop,wscale 7], length 0
13:52:35.000283 IP Ayesha-Imran.50926 > ec2-44-228-249-3.us-west-2.comp
ute.amazonaws.com.http: Flags [S], seq 4218543596, win 64240, options [
mss 1460,sackOK,TS val 1089851581 ecr 0,nop,wscale 7], length 0
13:52:36.024684 IP Ayesha-Imran.50926 > ec2-44-228-249-3.us-west-2.comp
ute.amazonaws.com.http: Flags [S], seq 4218543596, win 64240, options [
mss 1460,sackOK,TS val 1089852605 ecr 0,nop,wscale 7], length 0
13:52:37.047189 IP Ayesha-Imran.50926 > ec2-44-228-249-3.us-west-2.comp
```



```
Ubuntu 24.04.1 LTS amd64
18 packets captured
18 packets received by filter
0 packets dropped by kernel
ayesha-imran@Ayesha-Imran:~/Desktop$
```

Question 03:

Scan: Connect Scan

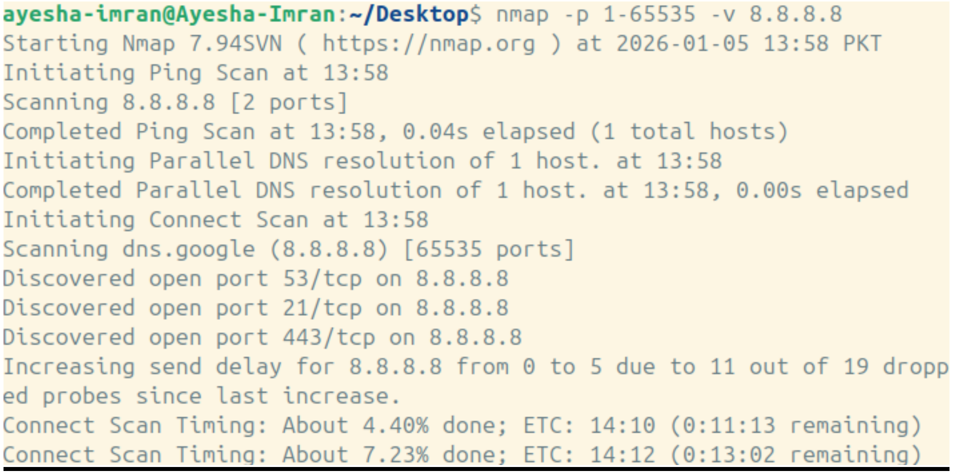


```
ayesha-imran@Ayesha-Imran:~/Desktop$ nmap -sT 8.8.8.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-05 13:57 PKT
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.054s latency).
Not shown: 995 filtered tcp ports (no-response), 2 filtered tcp ports (
host-unreach)
PORT    STATE SERVICE
21/tcp  open  ftp
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 54.78 seconds
```

Https,Printer ports were open:

Ports: 53, 21, 443 were open

Security Risk: Open port give an intruder a endpoint to use that port maliciously For example Hackers can you open port to do Dos or DDOS attack where He send multiple Packets.

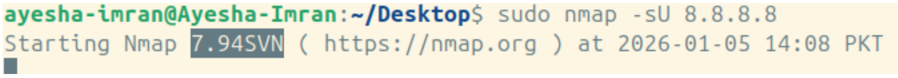


```
ayesha-imran@Ayesha-Imran:~/Desktop$ nmap -p 1-65535 -v 8.8.8.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-05 13:58 PKT
Initiating Ping Scan at 13:58
Scanning 8.8.8.8 [2 ports]
Completed Ping Scan at 13:58, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:58
Completed Parallel DNS resolution of 1 host. at 13:58, 0.00s elapsed
Initiating Connect Scan at 13:58
Scanning dns.google (8.8.8.8) [65535 ports]
Discovered open port 53/tcp on 8.8.8.8
Discovered open port 21/tcp on 8.8.8.8
Discovered open port 443/tcp on 8.8.8.8
Increasing send delay for 8.8.8.8 from 0 to 5 due to 11 out of 19 dropp
ed probes since last increase.
Connect Scan Timing: About 4.40% done; ETC: 14:10 (0:11:13 remaining)
Connect Scan Timing: About 7.23% done; ETC: 14:12 (0:13:02 remaining)
```

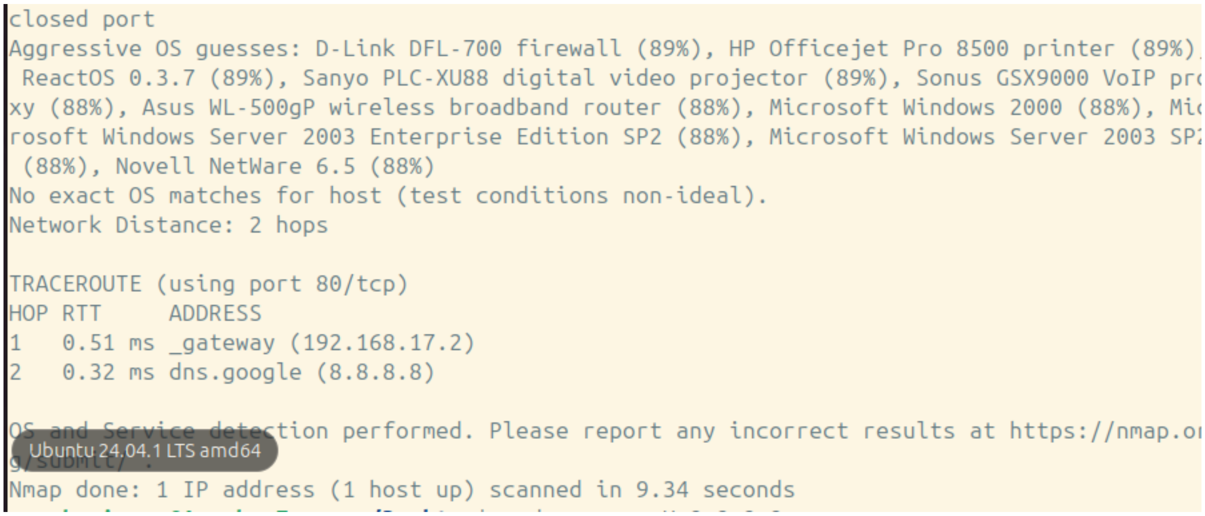
UDP scan:

sudo nmap -sU 8.8.8.8

This scsn is used for scanning user datagram protocol packets.



```
ayesha-imran@Ayesha-Imran:~/Desktop$ sudo nmap -sU 8.8.8.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-05 14:08 PKT
```

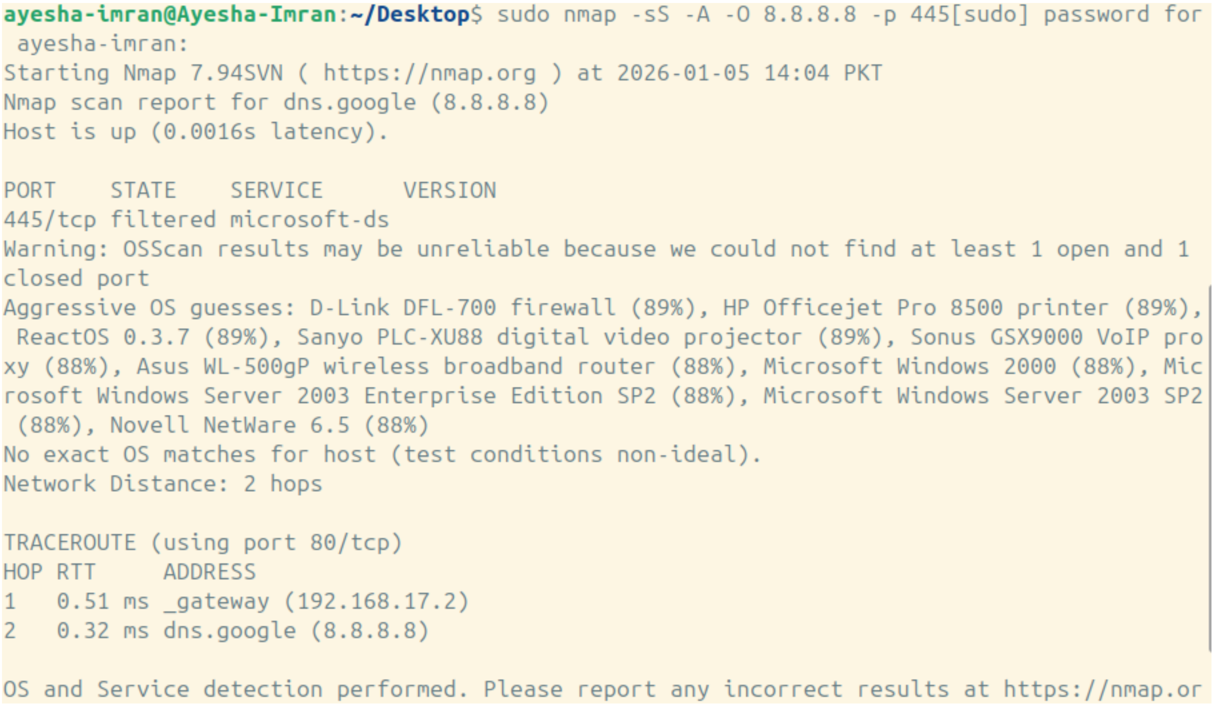


```
closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%),
 ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital video projector (89%), Sonus GSX9000 VoIP pro
xy (88%), Asus WL-500gP wireless broadband router (88%), Microsoft Windows 2000 (88%), Mic
rosoft Windows Server 2003 Enterprise Edition SP2 (88%), Microsoft Windows Server 2003 SP2
 (88%), Novell NetWare 6.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.51 ms _gateway (192.168.17.2)
2   0.32 ms dns.google (8.8.8.8)

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.34 seconds
```

Stealth Scan:

Command: sudo nmap –Ss –A –O 8.8.8.8 –p445

Explaination: This scan is a force scan that also detects round time trip,It is more powefull scan than the other, Most of the Analyst prefer this scan.



```
ayesha-imran@Ayesha-Imran:~/Desktop$ sudo nmap -sS -A -O 8.8.8.8 -p 445[sudo] password for
 ayesha-imran:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-05 14:04 PKT
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0016s latency).

PORT    STATE    SERVICE      VERSION
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%),
 ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital video projector (89%), Sonus GSX9000 VoIP pro
xy (88%), Asus WL-500gP wireless broadband router (88%), Microsoft Windows 2000 (88%), Mic
rosoft Windows Server 2003 Enterprise Edition SP2 (88%), Microsoft Windows Server 2003 SP2
 (88%), Novell NetWare 6.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.51 ms _gateway (192.168.17.2)
2   0.32 ms dns.google (8.8.8.8)

OS and Service detection performed. Please report any incorrect results at https://nmap.or
```