

Assignment-11

1. Basic Nmap Commands

nmap<target>

Basic scan of a target (IP or hostname)

```
Nmap Output Ports / Hosts Topology Host Details Scans
nmap 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:44 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00012s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
7070/tcp  open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

nmap – v <target>

Verbose output of the scan

```
nmap -v 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:44 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 19:44
Scanning 172.191.36.214 [1000 ports]
Discovered open port 445/tcp on 172.191.36.214
Discovered open port 3306/tcp on 172.191.36.214
Discovered open port 139/tcp on 172.191.36.214
Discovered open port 135/tcp on 172.191.36.214
Discovered open port 7070/tcp on 172.191.36.214
Completed SYN Stealth Scan at 19:44, 0.05s elapsed (1000 total ports)
Nmap scan report for 172.191.36.214
Host is up (0.00056s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
7070/tcp  open  realserver

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2005 (84.220KB)
```

nmap -sS <target>

SYN (Stealth) scan

```
nmap -sS 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:54 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00012s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
7070/tcp  open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

nmap -sT <target>

TCP Connect scan (less stealthy)

```
nmap -sT 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:45 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.0017s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
7070/tcp  open  realserver

Nmap done: 1 IP address (1 host up) scanned in 5.64 seconds
```

nmap -sU <target>

UDP scan

```
nmap -sU 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:45 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00031s latency).
Not shown: 990 closed udp ports (port-unreach)
PORT      STATE     SERVICE
80/udp    open|filtered http
123/udp   open|filtered ntp
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
443/udp   open|filtered https
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
5050/udp  open|filtered mmcc
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 181.33 seconds
```

nmap -p <target>

Scan all 65535 ports

```
nmap -p 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:46 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00034s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE     SERVICE
135/tcp   open      msrpc
137/tcp   filtered netbios-ns
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
3306/tcp  open      mysql
5040/tcp  open      unknown
7070/tcp  open      realserver
7680/tcp  open      pando-pub
8885/tcp  open      unknown
8886/tcp  open      unknown
33060/tcp open      mysql
49664/tcp open      unknown
49665/tcp open      unknown
49668/tcp open      unknown
49669/tcp open      unknown
49672/tcp open      unknown
49688/tcp open      unknown
57272/tcp open      unknown
57621/tcp open      unknown

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

nmap -O <target>

Try to detect OS

```
nmap -O 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:47 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00042s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE     SERVICE
135/tcp   open      msrpc
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
3306/tcp  open      mysql
7070/tcp  open      realserver
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  

TCP/IP fingerprint:  

OS:SCAN (V=7.95%E=4%D=4/13%OT=135%CT=1%CU=34769%EV=N%DS=0%DC=L%G=Y%TM=67FB0C7  

OS:84%P=i686-pc-windows-windows) SEQ(SP=103%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=OS:S%TS=A) SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A) SEQ(SP=106%GCD=OS:I%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A) SEQ(SP=FU%GCD=1%ISR=10C%TI=I%CI=I%II=OS:I%SS=S%TS=A) OPS(OI=MFPD7NW8ST11%O2=MFPD7NW8ST11%O3=MFPD7NW8NNT11%O4=MFPDOS:7NW8ST11%O5=MFPD7NW8ST11%O6=MFPD7ST11) WIN(WI=FFFF%W2=FFFF%W3=FFFF%W4=FFFOS:P%W5=FFFF%W6=FFFF) ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFPD7NW8NNN%CC=N%Q=) T1(R=Y%OS:DF=Y%T=80%W=0%S=0%A=S+F=A%RD=0%Q=) T2(R=Y%DF=Y%T=80%W=0%S=2%A=S+F=A%RD=0%Q=) T3(R=Y%DF=Y%T=80%W=0%S=2%A=O%F=AR%O=%RD=0%Q=) T4(R=Y%DF=Y%T=80%W=0%S=OS:A%A=0%F=R%O=%RD=0%Q=) T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=) T6(R=OS:Y%DF=Y%T=80%W=0%S=Z%A=O%F=R%O=%RD=0%Q=) T7(R=Y%DF=Y%T=80%W=0%S=2%A=S+F=OS:AR%O=%RD=0%Q=) UL(R=Y%DF=N%T=80%IP=164%UN=0%RIPL=G%RID=G%RIPCK=2%RUCK=G%OS:RUD=G) IE(R=Y%DFI=N%T=80%CD=2)
```

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 10.70 seconds

nmap -A <target>

Aggressive scan (OS, version, script scanning, traceroute)

```

nmap -A 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:48 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00051s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql           MySQL (unauthorized)
7070/tcp   open  ssl/realserver?
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2023-07-27T16:15:58
|_ Not valid after: 2023-07-14T16:15:58
_|_ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=7.95%#D=4/13%OT=135%CT=1%CU=32230%PV=N%DS=0%DC=L%G=Y%TM=67FBC7
OS:CA#P=1606-%c-windows-windows) SEQ(SP=101%GCD=%ISR=10B#T=I%CI=I%II=I%SS=
OS:%TS=A) SEQ(SP=106%GCD=1%ISR=100%TI=%CI=I%II=I%SS=S%TS=A) SEQ(SP=FC%GCD=1
OS:%SR=F8#TI=%CI=I%II=I%TS=A) SEQ(SP=F8#GCD=1%ISR=10C#TI=%CI=I%II=I%SS=S%
OS:TS=A) SEQ(SP=PP#GCD=1%ISR=108#TI=%CI=I%II=I%SS=S%TS=A) OPS(O1=MFFD7NW8ST1
OS:1%O2=MFFD7NW8ST11%O3=MFFD7NW8NT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST11%O6=MP
OS:W1#F#W2=FFFF#W3=FFFF#W4=FFFF#W5=FFFF#W6=FFFF) ECN(R=Y#DF=Y
OS:t=80#W=FFFF#O=MFFD7NW8NNNS%CC=N%Q=T1 (R=Y#DF=Y#)=80#S=0%#A=8%#F=AS#RD=0%Q
OS:T2 (R=Y#DF=Y#)=80#S=2%#A=8%#F=AR#O=%RD=(%)Q) T3 (R=Y#DF=Y#)=80#W=0%#S=2%
OS:A=0%#F=AR#O=%RD=0%Q) T4 (R=Y#DF=Y#)=80#W=0%#S+A#A=0%#F=AR#O=%RD=0%Q) T5 (R=Y#D
OS:F=Y#T=80#W=0%#S=2%#A=8%#F=AR#O=%RD=0%Q) T6 (R=Y#DF=Y#)=80#W=0%#S+A#A=0%#F=R#O
OS:S=0%#RD=0%Q) T7 (R=Y#DF=Y#)=80#W=0%#S=2%#A=8%#F=AR#O=%RD=(%)Q) U1 (R=Y#DF=N#T=80
OS:IPL=164%UN=0%RIPL=G%RID=G%RIPCR=G%RUCK=G%RUD=G) IE(R=Y#DFI=N#T=80%CD=Z)

Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-04-13T14:18:39
|_ start_date: N/A
| smb2-security-mode:
|   3:1:::
|_ Message signing enabled but not required

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.82 seconds

```

nmap -sV <target>

Detect service versions

```

nmap -sV 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:49 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00091s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql           MySQL (unauthorized)
7070/tcp   open  ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.96 seconds

```

nmap -T4 <target>

Faster scan timing (T0 to T5, T4 is common for speed)

```

nmap -T4 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:50 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.000071s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
7070/tcp   open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds

```

nmap -Pn <target>

Skip host discovery (assume host is up)

```

nmap -Pn 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:50 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00016s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
7070/tcp   open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

```

nmap --script vuln <target>

Run common vulnerability scripts

```
nmap --script vuln 172.191.36.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 19:52 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.191.36.214
Host is up (0.00034s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
7070/tcp   open  realserver

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 29.05 seconds
```

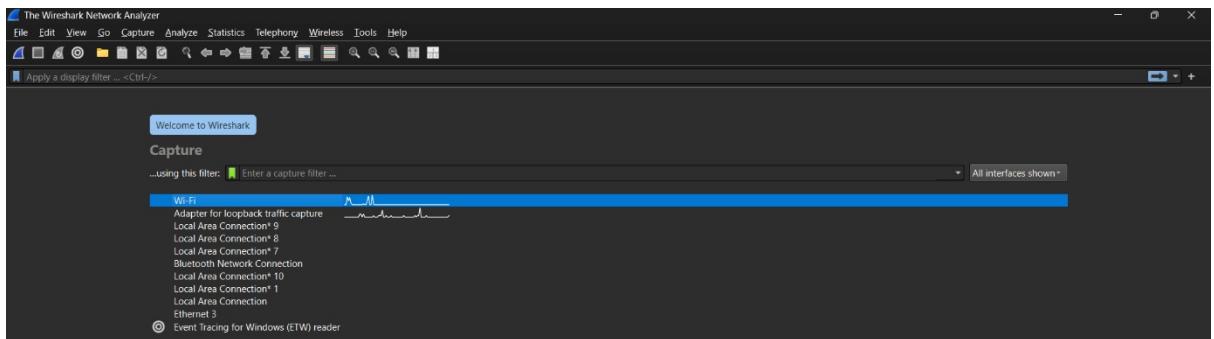
2. Capturing and Analyzing Network Traffic Using Wireshark

1. Download and Install Wireshark:

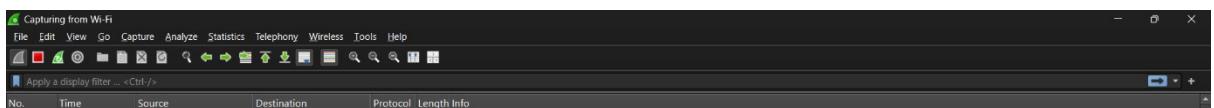
- o Visit <https://www.wireshark.org/>
- o Download and install the latest version for your operating system.

2. Start a Packet Capture Session:

- o Open Wireshark.
- o Select your active network interface (e.g., Wi-Fi or Ethernet).



- o Click the Start Capturing Packets button (shark fin icon).



3. Generate Some Network Traffic:

- o Open a web browser and visit a few websites.
- o You may also open apps that use the internet like email or messaging tools.

Wireshark Network Monitor

Apply a display filter... <Ctrl-/>

No. Time Source Destination Protocol Length Info

```

Frame 16556: 125 bytes captured (1000 bits) on interface \Device\NPF_{343... 00:00:00 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f
Ethernet II, Src: AzurWaveTec_beda:13 (50:5a:65:bada:13), Dst: VMware_77:aa:3f (00:0c:29:77:aa:3f)
Internet Protocol Version 4, Src: 172.191.36.214, Dst: 57.144.147.33
Transmission Control Protocol, Src Port: 61907, Dst Port: 443, Seq: 1154, Ack: 5939, Len: 71
Transport Layer Security

```

Frame 16556: 125 bytes captured (1000 bits) on interface \Device\NPF_{343... 00:00:00 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f 00:0c:29:77:a4:3f
Ethernet II, Src: AzurWaveTec_beda:13 (50:5a:65:bada:13), Dst: VMware_77:aa:3f (00:0c:29:77:aa:3f)
Internet Protocol Version 4, Src: 172.191.36.214, Dst: 57.144.147.33
Transmission Control Protocol, Src Port: 61907, Dst Port: 443, Seq: 1154, Ack: 5939, Len: 71
Transport Layer Security

No.	Time	Source	Destination	Protocol	Length	Info
16570	349.431932	MercuryCommu_fc:fc:.. Broadcast		ARP	60	Who has 192.168.73.20? Tell 192.168.73.11
16571	349.693523	MercuryTech_7b:ee:5.. Broadcast		ARP	60	Who has 192.168.73.20? Tell 192.168.73.81
16572	349.791569	MercuryTech_7b:ee:5.. Broadcast		ARP	60	Who has 192.168.73.20? Tell 192.168.73.19
16573	349.801569	MercuryTech_7b:ee:5.. Broadcast		ARP	60	Who has 192.168.73.20? Tell 192.168.73.19
16574	349.863471	MercuryTech_7b:ee:5.. Broadcast		ARP	60	Who has 192.168.73.20? Tell 192.168.73.84
16575	349.897380	MercuryCommu_fc:f6:.. Broadcast		ARP	60	Who has 192.168.73.20? Tell 192.168.73.14
16576	349.936954	MercuryCommu_fc:f6:.. Broadcast		ARP	60	Who has 192.168.73.20? Tell 192.168.73.13
16577	350.493953	128.195.10.252	172.191.36.214	TLSv1.3	78	Application Data
16578	350.493953	128.195.10.252	172.191.36.214	TCP	60	443 + 61879 [FIN, ACK] Seq=1821 Ack=3272 Win=63224 Len=0
16579	350.494653	172.191.36.214	128.195.10.252	TCP	54	61879 + 443 [ACK] Seq=3272 Ack=31822 Win=65280 Len=0
16580	350.720831	57.144.147.33	172.191.36.214	SSL	206	Continuation Data
16581	350.722676	172.191.36.214	57.144.147.33	SSL	125	Continuation Data
16582	350.730929	172.191.36.214	57.144.147.33	SSL	125	Continuation Data
16583	350.731807	57.144.147.33	172.191.36.214	TCP	60	443 + 61897 [ACK] Seq=6426 Ack=1363 Win=68864 Len=0
16584	350.731917	57.144.147.33	172.191.36.214	TCP	60	443 + 61897 [ACK] Seq=6426 Ack=1434 Win=68864 Len=0
16585	351.744907	172.64.151.4	172.191.36.214	TLSv1.2	255	Application Data
16586	351.746001	172.191.36.214	172.64.151.4	TLSv1.2	82	Application Data
16587	351.757609	172.64.151.4	172.191.36.214	TCP	60	443 + 61331 [ACK] Seq=6393 Ack=2461 Win=19 Len=0
16588	352.001239	172.191.36.62	224.0.0.251	MDNS	119	Standard query 0x001e PTR _googlecast._tcp.local, "QM" question PTR _67440243..sub._googlecast._tcp.local, "QM" question PTR _8E6CB..

4. Stop the Capture:

- o After about 2–5 minutes, stop the capture using the red square icon in Wireshark.

Wireshark Network Monitor

Apply a display filter... <Ctrl-/>

No. Time Source Destination Protocol Length Info

```

Frame 15467: 382 bytes captured (3056 bits) on interface \Device\NPF_{343... 00:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00
Ethernet II, Src: Intel_15:f2:7a (24:ee:9a:15:f2:7a), Dst: VMware_77:aa:3f (00:0c:29:77:aa:3f)
Internet Protocol Version 4, Src: 172.191.36.198, Dst: 34.104.35.123
Transmission Control Protocol, Src Port: 50519, Dst Port: 80, Seq: 1, Ack: 1, Len: 328
HyperText Transfer Protocol

```

No.	Time	Source	Destination	Protocol	Length	Info
21966	58.117600	34.104.35.123	172.191.36.198	HTTP	695	HTTP/1.1 200 OK
21970	58.117600	34.104.35.123	172.191.36.198	HTTP	387	GET /edged1/release2/chrome_component/gikiajhx6vvdbwrvbclvcybfm_499/lmelglejhemejginpboagddgfbepgmp_499_-
21999	58.140331	34.104.35.123	172.191.36.198	HTTP	349	HTTP/1.1 200 OK
22217	62.356986	172.191.36.198	34.104.35.123	HTTP	314	HEAD /edged1/diffgen-puffin/miikhgajplphfehabhhblakbdgeejf/1678659cff85786dff5950efb64fc935fd32632b3419_-
22224	62.367491	34.104.35.123	172.191.36.198	HTTP	604	HTTP/1.1 200 OK
22231	62.456643	172.191.36.198	34.104.35.123	HTTP	365	GET /edged1/diffgen-puffin/miikhgajplphfehabhhblakbdgeejf/1678659cff85786dff5950efb64fc935fd32632b3419_-
22238	62.483838	34.104.35.123	172.191.36.198	HTTP	812	HTTP/1.1 200 OK
23075	66.787747	172.191.36.198	23.60.172.26	HTTP	411	HEAD /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23087	66.806879	23.60.172.26	172.191.36.198	HTTP	660	HTTP/1.1 200 OK
23088	66.859675	172.191.36.198	23.60.172.26	HTTP	482	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23089	66.874085	23.60.172.26	172.191.36.198	HTTP	200	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23125	69.146520	172.191.36.198	23.60.172.26	HTTP	485	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23130	69.165384	23.60.172.26	172.191.36.198	HTTP	890	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23162	70.352892	172.191.36.198	23.60.172.26	HTTP	486	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23165	70.367983	23.60.172.26	172.191.36.198	HTTP	277	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23196	71.368818	172.191.36.198	23.60.172.26	HTTP	487	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23198	71.409692	23.60.172.26	172.191.36.198	HTTP	201	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23213	72.384930	172.191.36.198	23.60.172.26	HTTP	488	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-

5. Analyze the Traffic:

- o Use filters Simple filter HTTP, DNS, or TCP to view specific types of traffic.

HTTP :

Wireshark Network Monitor

Apply a display filter... <Ctrl-/>

No. Time Source Destination Protocol Length Info

```

Frame 15467: 382 bytes captured (3056 bits) on interface \Device\NPF_{343... 00:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00 00:0f:c3:c2:00:00
Ethernet II, Src: Intel_15:f2:7a (24:ee:9a:15:f2:7a), Dst: VMware_77:aa:3f (00:0c:29:77:aa:3f)
Internet Protocol Version 4, Src: 172.191.36.198, Dst: 34.104.35.123
Transmission Control Protocol, Src Port: 50519, Dst Port: 80, Seq: 1, Ack: 1, Len: 328
HyperText Transfer Protocol

```

No.	Time	Source	Destination	Protocol	Length	Info
21966	58.117600	34.104.35.123	172.191.36.198	HTTP	695	HTTP/1.1 200 OK
21970	58.117600	34.104.35.123	172.191.36.198	HTTP	387	GET /edged1/release2/chrome_component/gikiajhx6vvdbwrvbclvcybfm_499/lmelglejhemejginpboagddgfbepgmp_499_-
21999	58.140331	34.104.35.123	172.191.36.198	HTTP	349	HTTP/1.1 200 OK
22217	62.356986	172.191.36.198	34.104.35.123	HTTP	314	HEAD /edged1/diffgen-puffin/miikhgajplphfehabhhblakbdgeejf/1678659cff85786dff5950efb64fc935fd32632b3419_-
22224	62.367491	34.104.35.123	172.191.36.198	HTTP	604	HTTP/1.1 200 OK
22231	62.456643	172.191.36.198	34.104.35.123	HTTP	365	GET /edged1/diffgen-puffin/miikhgajplphfehabhhblakbdgeejf/1678659cff85786dff5950efb64fc935fd32632b3419_-
22238	62.483838	34.104.35.123	172.191.36.198	HTTP	812	HTTP/1.1 200 OK
23075	66.787747	172.191.36.198	23.60.172.26	HTTP	411	HEAD /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23087	66.806879	23.60.172.26	172.191.36.198	HTTP	660	HTTP/1.1 200 OK
23088	66.859675	172.191.36.198	23.60.172.26	HTTP	482	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23089	66.874085	23.60.172.26	172.191.36.198	HTTP	200	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23125	69.146520	172.191.36.198	23.60.172.26	HTTP	485	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23130	69.165384	23.60.172.26	172.191.36.198	HTTP	890	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23162	70.352892	172.191.36.198	23.60.172.26	HTTP	486	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23165	70.367983	23.60.172.26	172.191.36.198	HTTP	277	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23196	71.368818	172.191.36.198	23.60.172.26	HTTP	487	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-
23198	71.409692	23.60.172.26	172.191.36.198	HTTP	201	HTTP/1.1 200 Partial Content (application/x-chrome-extension)
23213	72.384930	172.191.36.198	23.60.172.26	HTTP	488	GET /filestreamingservice/files/5d32607d-ea9-44fc-ac55-77800b9862a5?1=1744954533&p2=404&p3=2&p4=J10TNEB_-

TCP :

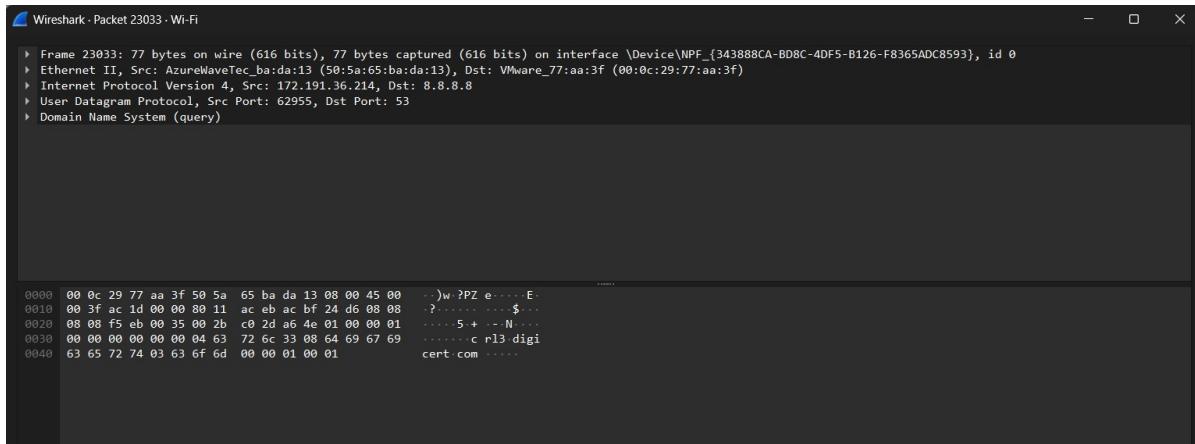
DNS :

o Select a few packets and inspect their details in the packet details pane.

```
Wireshark - Pocket 23041 - Wi-Fi

Frame 23041: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface \Device\NPF_{343888CA-BD8C-4DF5-B126-F8365ADC8593}, id 0
Ethernet II, Src: VMware_77:aa:3f (00:0c:29:77:aa:3f), Dst: AzureWaveTec_ba:da:13 (50:5a:65:ba:da:13)
Internet Protocol Version 4, Src: 162.247.243.29, Dst: 172.191.36.214
Transmission Control Protocol, Src Port: 443, Dst Port: 62827, Seq: 4249, Ack: 2029, Len: 9
[2 Reassembled TCP Segments (215 bytes): #23040(206), #23041(9)]
Transport Layer Security
```

0000 50 5a 65 ba da 13 00 0c 29 77 aa 3f 08 00 45 28 PZe-----)w ?-E(.....
0001 00 31 1e 29 40 00 38 06 bc cb a2 f7 f3 1d ac bf 1)@ 8-----
0020 24 d6 01 bb f5 6b bc 22 59 69 35 31 53 69 50 18 \$-----k " Yi51SiP
0030 01 1e 70 e1 00 00 7b d8 69 f3 ff 3d 69 c1 f2 p-----i =i ..



6. Export Your Capture: Save the capture as a .pcapng file for later review.

https://drive.google.com/drive/folders/1aHY89uyI8rcGuUdVozl8XzqsG5Se3KVf?usp=drive_link

Theory:-

Assignment-11

I) Basic Nmap Commands.

Command	Description
a) nmap <target>	Basic uscan of a target
b) nmap -v <target>	verbose output of the scan
c) nmap -sS <target>	SYN (stealth) scan
d) nmap -st <target>	TCP connect scan (less stealthy)
e) nmap -sU <target>	UDP scan
f) nmap -P2 <target>	Scan specific port(s)
g) nmap -Pf <target>	Scan all 65535 ports
h) nmap -O <target>	try to detect OS
i) nmap -A <target>	aggressive scan (OS, version, script scanning)
j) nmap -SV <target>	detect service versions
k) nmap -T4 <target>	faster scan timing (ToToTs, T4 is common for speed)
l) nmap -Pn <target>	skip host discovery (assume host is up)
m) nmap -L target.txt	scan multiple targets from a file.
n) nmap -ON <target>	output save output in normal format
o) nmap -script <script-name> <target>	run specific NSE script
p) nmap --script vuln <target>	Run common vulnerability scripts.

Q2 Capturing and analyzing network traffic using Wireshark.

Q1 What interface did you select for capturing packets?

Soln: For capturing packets, I selected Wi-Fi interface because my computer is connected to the internet via a wireless network. In Wireshark, all available network interfaces are listed when the application is launched, and selecting the correct one is essential to monitor the traffic effectively. The Wi-Fi interface typically shows ongoing data transmission in the form of spikes which indicates active network traffic. This interface allows the capture of all incoming and outgoing packets from the wireless connection in real-time.

Q2 List 3 protocols you observed during the capture session.

Soln: I observed the three commonly used network protocols: HTTP, TCP, and UDP.

1) HTTP (Hyper Text Transfer Protocol) is used for transferring web-page over the internet. I noticed several HTTP requests when I opened different websites.

- DATE
- 2) DNS (Domain name system)
this protocol translates domain names into IP addresses whenever I typed a URL. DNS packet generated to resolve the IP address.
- 3) TCP (Transmission control protocol)
A connection-oriented protocol that ensures reliable communication between devices. TCP packets were visible in every connection, especially during communications.
- Q3 Pick one HTTP packet. What was the host website being accessed?
⇒ I selected an HTTP GET request packet during the session. The host accessed in that particular packet was: www.example.com (Note: Replace this with actual domain name you saw during my session such as www.google.com, www.wikipedia.org etc.)
In the packet details, under the HTTP section the 'Host' field displays the exact domain being requested. The host field shows which server my browser or was trying to reach using the HTTP protocol.
- Q4 What is the IP address of your system and the destination IP for the selected packet?

1) Ethernet II: This is the datalink layer that includes the MAC addresses of the source and destination devices within the local network.

2) Internet Protocol version 4 (IPv4): This is the network layer, responsible for identifying source and destination IP addresses.

3) Transmission control protocol (TCP): This is the transport layer, ensuring reliable transmission and providing ports to identify applications.

4) Hypertext Transfer Protocol (HTTP): This is the application layer, where the actual web request (such as GET or POST) is visible. Each layer wraps the data from the layer above, which is called encapsulation when the packet is received from the layers in reverse order.

Q6: What did you learn from this activity about how data travels over the internet?

This activity offered a hands-on understanding of how data travels through the Internet using different protocol layers.

- Some Key takeaways:
- 1) Layer architecture - Data is encapsulated in layer (Ethernet, IP, HTTP, TCP) during transmission and de-encapsulated at the receiver's end.
 - 2) Protocol role - Each protocol serves a specific function - for example, DNS reserves domain names, IP handles addressing and TCP ensures reliable delivery.
 - 3) Traffic visibility - Wireshark allows us to inspect the raw data being transmitted, including requests to websites, responses from servers, and system interactions over the network.
 - 4) Security considerations: showing how easily HTTP data can be read underscores the importance of using HTTPS for secure communication.
 - 5) Packet-level understanding - viewing each packet's structure gives a deeper appreciation of the technical details involved in something as simple as opening a web page.
- Rid
Wu