

# ASSIGNMENT – 3

Q-1) Check which protocol service is available on the host cs.triple5.online

```
200420116059@kali:~$ sudo nmap -s0 cs.triple5.online
[sudo] password for 200420116059:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-30 06:03 UTC
Nmap scan report for cs.triple5.online (3.87.70.88)
Host is up (0.00081s latency).
rDNS record for 3.87.70.88: ec2-3-87-70-88.compute-1.amazonaws.com
```

| PROTOCOL | STATE         | SERVICE     |
|----------|---------------|-------------|
| 0        | open          | hopopt      |
| 1        | open          | icmp        |
| 2        | open filtered | igmp        |
| 3        | open          | ggp         |
| 4        | open          | ipv4        |
| 5        | open          | st          |
| 6        | open filtered | tcp         |
| 7        | open          | cbt         |
| 8        | open          | egp         |
| 9        | open          | igp         |
| 10       | open          | bbn-rcc-mon |
| 11       | open          | nvp-ii      |
| 12       | open          | pup         |
| 13       | open          | argus       |
| 14       | open          | emcon       |
| 15       | open          | xnet        |
| 16       | open          | chaos       |
| 17       | open filtered | udp         |
| 18       | open          | mux         |
| 19       | open          | dcn-meas    |
| 20       | open          | hmp         |
| 21       | open          | prm         |
| 22       | open          | xns-idp     |
| 23       | open          | trunk-1     |
| 24       | open          | trunk-2     |
| 25       | open          | leaf-1      |
| 26       | open          | leaf-2      |
| 27       | open          | rdp         |
| 28       | open          | irtp        |

|    |               |             |
|----|---------------|-------------|
| 29 | open          | iso-tp4     |
| 30 | open          | netblt      |
| 31 | open          | mfe-nsp     |
| 32 | open          | merit-inp   |
| 33 | open          | dccp        |
| 34 | open          | 3pc         |
| 35 | open          | idpr        |
| 36 | open          | xtp         |
| 37 | open          | ddp         |
| 38 | open          | idpr-cmtp   |
| 39 | open          | tp++        |
| 40 | open          | il          |
| 41 | open filtered | ipv6        |
| 42 | open          | sdrp        |
| 43 | open          | ipv6-route  |
| 44 | open          | ipv6-frag   |
| 45 | open          | idrp        |
| 46 | open          | rsvp        |
| 47 | open          | gre         |
| 48 | open          | dsp         |
| 49 | open          | bnat        |
| 50 | open          | esp         |
| 51 | open          | ah          |
| 52 | open          | i-nlsp      |
| 53 | open          | swipe       |
| 54 | open          | narp        |
| 55 | open          | mobile      |
| 56 | open          | tlsp        |
| 57 | open          | skip        |
| 58 | open filtered | ipv6-icmp   |
| 59 | open          | ipv6-nonxt  |
| 60 | open          | ipv6-opts   |
| 61 | open          | anyhost     |
| 62 | open          | cftp        |
| 63 | open          | anylocalnet |
| 64 | open          | sat-expak   |

|     |      |              |
|-----|------|--------------|
| 65  | open | kryptolan    |
| 66  | open | rxd          |
| 67  | open | ippc         |
| 68  | open | anydistribfs |
| 69  | open | sat-mon      |
| 70  | open | visa         |
| 71  | open | ipcv         |
| 72  | open | cpnx         |
| 73  | open | cphb         |
| 74  | open | wsn          |
| 75  | open | pvp          |
| 76  | open | br-sat-mon   |
| 77  | open | sun-nd       |
| 78  | open | wb-mon       |
| 79  | open | wb-expak     |
| 80  | open | iso-ip       |
| 81  | open | vmtp         |
| 82  | open | secure-vmtp  |
| 83  | open | vines        |
| 84  | open | iptm         |
| 85  | open | nsfnet-igp   |
| 86  | open | dgp          |
| 87  | open | tcf          |
| 88  | open | eigrp        |
| 89  | open | ospfigp      |
| 90  | open | sprite-rpc   |
| 91  | open | larp         |
| 92  | open | mtp          |
| 93  | open | ax.25        |
| 94  | open | ipip         |
| 95  | open | micp         |
| 96  | open | scc-sp       |
| 97  | open | etherip      |
| 98  | open | encap        |
| 99  | open | anyencrypt   |
| 100 | open | gmtp         |

|     |               |                 |
|-----|---------------|-----------------|
| 101 | open          | ifmp            |
| 102 | open          | pnni            |
| 103 | open filtered | pim             |
| 104 | open          | aris            |
| 105 | open          | scps            |
| 106 | open          | qnx             |
| 107 | open          | a/n             |
| 108 | open          | ipcomp          |
| 109 | open          | snp             |
| 110 | open          | compaq-peer     |
| 111 | open          | ipx-in-ip       |
| 112 | open          | vrrp            |
| 113 | open          | pgm             |
| 114 | open          | any0hop         |
| 115 | open          | l2tp            |
| 116 | open          | ddx             |
| 117 | open          | iatp            |
| 118 | open          | stp             |
| 119 | open          | srp             |
| 120 | open          | uti             |
| 121 | open          | smp             |
| 122 | open          | sm              |
| 123 | open          | ptp             |
| 124 | open          | isis-ipv4       |
| 125 | open          | fire            |
| 126 | open          | crtf            |
| 127 | open          | crudp           |
| 128 | open          | sscpmce         |
| 129 | open          | iplt            |
| 130 | open          | sps             |
| 131 | open          | pipe            |
| 132 | open          | sctp            |
| 133 | open          | fc              |
| 134 | open          | rsvp-e2e-ignore |
| 135 | open          | mobility-hdr    |
| 136 | open          | udplite         |

|     |      |            |
|-----|------|------------|
| 137 | open | mpls-in-ip |
| 138 | open | manet      |
| 139 | open | hip        |
| 140 | open | shim6      |
| 141 | open | wesp       |
| 142 | open | rohc       |
| 143 | open | ethernet   |
| 144 | open | unknown    |
| 145 | open | unknown    |
| 146 | open | unknown    |
| 147 | open | unknown    |
| 148 | open | unknown    |
| 149 | open | unknown    |
| 150 | open | unknown    |
| 151 | open | unknown    |
| 152 | open | unknown    |
| 153 | open | unknown    |
| 154 | open | unknown    |
| 155 | open | unknown    |
| 156 | open | unknown    |
| 157 | open | unknown    |
| 158 | open | unknown    |
| 159 | open | unknown    |
| 160 | open | unknown    |
| 161 | open | unknown    |
| 162 | open | unknown    |
| 163 | open | unknown    |
| 164 | open | unknown    |
| 165 | open | unknown    |
| 166 | open | unknown    |
| 167 | open | unknown    |
| 168 | open | unknown    |
| 169 | open | unknown    |
| 170 | open | unknown    |
| 171 | open | unknown    |
| 172 | open | unknown    |

|     |      |         |
|-----|------|---------|
| 173 | open | unknown |
| 174 | open | unknown |
| 175 | open | unknown |
| 176 | open | unknown |
| 177 | open | unknown |
| 178 | open | unknown |
| 179 | open | unknown |
| 180 | open | unknown |
| 181 | open | unknown |
| 182 | open | unknown |
| 183 | open | unknown |
| 184 | open | unknown |
| 185 | open | unknown |
| 186 | open | unknown |
| 187 | open | unknown |
| 188 | open | unknown |
| 189 | open | unknown |
| 190 | open | unknown |
| 191 | open | unknown |
| 192 | open | unknown |
| 193 | open | unknown |
| 194 | open | unknown |
| 195 | open | unknown |
| 196 | open | unknown |
| 197 | open | unknown |
| 198 | open | unknown |
| 199 | open | unknown |
| 200 | open | unknown |
| 201 | open | unknown |
| 202 | open | unknown |
| 203 | open | unknown |
| 204 | open | unknown |
| 205 | open | unknown |
| 206 | open | unknown |
| 207 | open | unknown |
| 208 | open | unknown |

|     |      |         |
|-----|------|---------|
| 209 | open | unknown |
| 210 | open | unknown |
| 211 | open | unknown |
| 212 | open | unknown |
| 213 | open | unknown |
| 214 | open | unknown |
| 215 | open | unknown |
| 216 | open | unknown |
| 217 | open | unknown |
| 218 | open | unknown |
| 219 | open | unknown |
| 220 | open | unknown |
| 221 | open | unknown |
| 222 | open | unknown |
| 223 | open | unknown |
| 224 | open | unknown |
| 225 | open | unknown |
| 226 | open | unknown |
| 227 | open | unknown |
| 228 | open | unknown |
| 229 | open | unknown |
| 230 | open | unknown |
| 231 | open | unknown |
| 232 | open | unknown |
| 233 | open | unknown |
| 234 | open | unknown |
| 235 | open | unknown |
| 236 | open | unknown |
| 237 | open | unknown |
| 238 | open | unknown |
| 239 | open | unknown |
| 240 | open | unknown |
| 241 | open | unknown |
| 242 | open | unknown |
| 243 | open | unknown |
| 244 | open | unknown |

|     |      |               |
|-----|------|---------------|
| 245 | open | unknown       |
| 246 | open | unknown       |
| 247 | open | unknown       |
| 248 | open | unknown       |
| 249 | open | unknown       |
| 250 | open | unknown       |
| 251 | open | unknown       |
| 252 | open | unknown       |
| 253 | open | experimental1 |
| 254 | open | experimental2 |
| 255 | open | unknown       |

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds

Q-2) Determine which services are available on the host www.scet.ac.in

```
200420116059@kali:~$ sudo nmap -sV scet.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-30 06:05 UTC
Nmap scan report for scet.ac.in (136.243.80.165)
Host is up (0.096s latency).
rDNS record for 136.243.80.165: lynx1.adaptable.services
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      Pure-FTPd
22/tcp    closed ssh
53/tcp    open  domain   PowerDNS
80/tcp    open  http     Apache httpd
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
443/tcp   open  ssl/http Apache httpd
587/tcp   open  smtp     Exim smtpd 4.95
687/tcp   open  ssh      OpenSSH 7.4 (protocol 2.0)
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  closed mysql

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.83 seconds
```

Q-3) Identify the Operating System of www.facebook.com

```
200420116059@kali:~$ sudo nmap -O www.facebook.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-30 06:10 UTC
Nmap scan report for www.facebook.com (31.13.66.35)
Host is up (0.00060s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f103:181:face:b00c:0:25de
rDNS record for 31.13.66.35: edge-star-mini-shv-01-iad3.facebook.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
843/tcp    closed unknown
5222/tcp  closed xmpp-client
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (86%), FreeBSD 11.2-STABLE (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.39 seconds
```

## Q-4) Capture Live Packets using Wire shark.

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| No.   | Time      | Source                           | Destination   | Protocol | Length | Info   |
|-------|-----------|----------------------------------|---------------|----------|--------|--|
| 34867 | 63.480557 | 172.16.17.75                     | 224.0.0.251   | MDNS     | 90     | Standard query response 0x0000 A, cache flush 172.16.17.75 |
| 34868 | 63.484079 | 172.16.17.131                    | 172.16.17.255 | NBNS     | 92     | Name query NB DESKTOP-9H9A93Q<00>                          |
| 34869 | 63.484167 | 172.16.17.72                     | 224.0.0.251   | MDNS     | 90     | Standard query response 0x0000 A, cache flush 172.16.17.72 |
| 34870 | 63.484877 | 172.16.17.67                     | 224.0.0.251   | MDNS     | 90     | Standard query response 0x0000 A, cache flush 172.16.17.67 |
| 34871 | 63.490107 | 172.16.17.62                     | 224.0.0.251   | MDNS     | 90     | Standard query response 0x0000 A, cache flush 172.16.17.62 |
| 34872 | 63.491433 | 172.16.17.114                    | 172.16.17.255 | NBNS     | 92     | Name query NB IT<00>                                       |
| 34873 | 63.497386 | 172.16.17.64                     | 224.0.0.251   | MDNS     | 90     | Standard query response 0x0000 A, cache flush 172.16.17.64 |
| 34874 | 63.497431 | 172.16.17.46                     | 224.0.0.251   | MDNS     | 90     | Standard query response 0x0000 A, cache flush 172.16.17.46 |
| 34875 | 63.498956 | 172.16.17.88                     | 224.0.0.251   | MDNS     | 90     | Standard query response 0x0000 A, cache flush 172.16.17.88 |
| 34876 | 63.501150 | fe80::e1f3:290e:4f9... ff02::1:3 |               | LLMNR    | 82     | Standard query 0xd315 A it                                 |

> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF\_{A17E0212-D301-4A95-B24E-76F7F30520DA}, id 0  
> Ethernet II, Src: Elitegro\_d2:93:01 (74:27:ea:d2:93:01), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)  
> Internet Protocol Version 4, Src: 172.16.17.75, Dst: 224.0.0.251  
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
> Multicast Domain Name System (response)

```
0000  01 00 5e 00 00 fb 74 27  ea d2 93 01 08 00 45 00  ..^...t' .....E-
0010  00 4c 22 23 00 00 ff 11  fb 26 ac 10 11 4b e0 00  -L"#....-&...K..
0020  00 fb 14 e9 14 e9 00 38  a6 e7 00 00 84 00 00 00  .....8 .....
0030  00 01 00 00 00 00 0e 49  54 37 35 2d 61 6b 61 73  .....I T75-akas
0040  68 2d 63 6f 6d 05 6c 6f  63 61 6c 00 00 01 80 01  h-com.lo cal .
0050  00 00 00 0a 00 04 ac 10  11 4b  .....-K
```

## Q-5) Analyze the contents of various protocols.

Wireshark · Packet 61453 · Ethernet

> Frame 61453: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF\_{A17E0212-D301-4A95-B24E-76F7F30520DA},  
> Ethernet II, Src: Dell\_ad:1d:1a (8c:ec:4b:ad:1d:1a), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)  
> Internet Protocol Version 4, Src: 172.16.17.46, Dst: 224.0.0.251  
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
> Multicast Domain Name System (response)

0000 01 00 5e 00 00 fb 8c ec 4b ad 1d 1a 08 00 45 00 ..^.....K.....E-  
0010 00 4c 6f b0 00 00 ff 11 ad b6 ac 10 11 2e e0 00 ..Lo.....,..  
0020 00 fb 14 e9 14 e9 00 38 a6 20 00 00 84 00 00 00 .....8.....  
0030 00 01 00 00 00 00 0e 49 54 38 36 2d 61 6b 61 73 .....I T86-akas  
0040 68 2d 63 6f 6d 05 6c 6f 63 61 6c 00 00 01 80 01 h-com.lo cal.....  
0050 00 00 00 0a 00 04 ac 10 11 2e ..... ,

No.: 61453 · Time: 121.746678 · Source: 172.16.17.46 · Destination: 224.0.0.251 · Protocol: MDNS · Length: 90 · Info: Standard query response 0x0000 A, cache flush 172.16.17.46

Close Help

Wireshark · Packet 16889 · Ethernet

> Frame 16889: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF\_{A17E0212-D301-4A95-B24E-76F7F30520DA},  
> Ethernet II, Src: D-LinkIn\_ee:24:0e (d8:fe:e3:ee:24:0e), Dst: HewlettP\_21:51:84 (c8:d9:d2:21:51:84)  
> Internet Protocol Version 4, Src: 172.16.3.1, Dst: 172.16.17.110  
> Transmission Control Protocol, Src Port: 3128, Dst Port: 54048, Seq: 38187, Ack: 566, Len: 1460  
> Hypertext Transfer Protocol

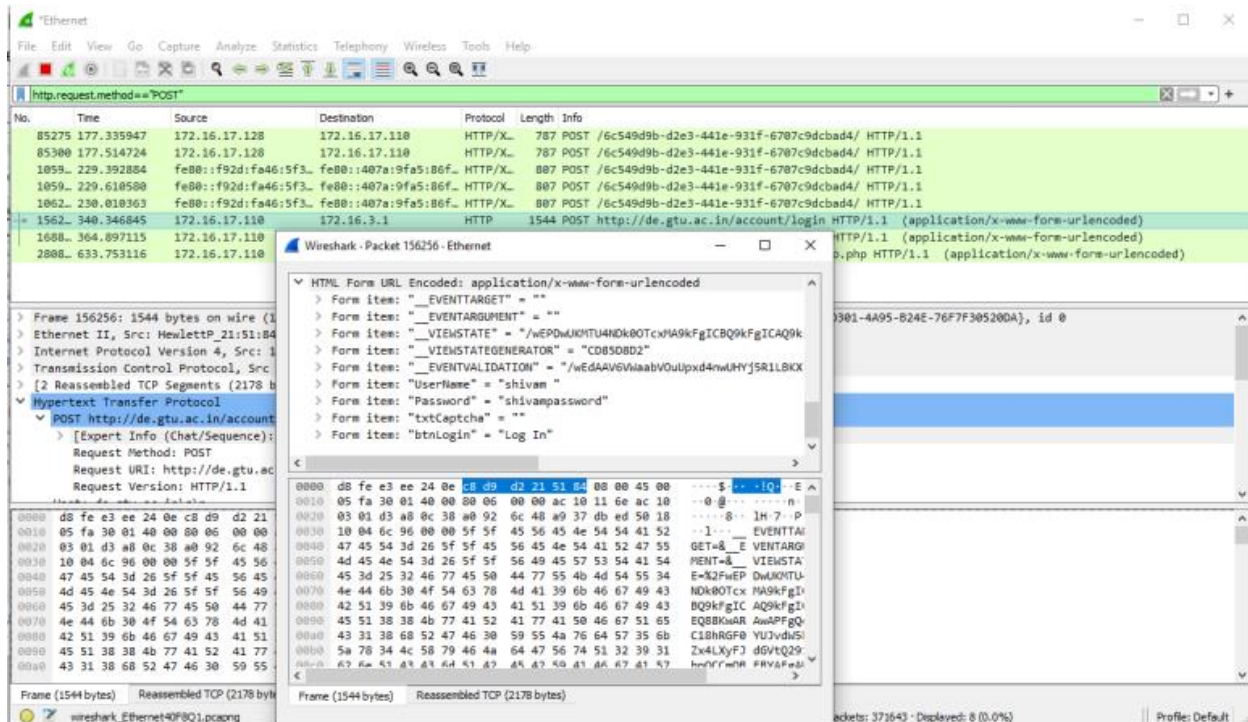
0000 c8 d9 d2 21 51 84 d8 fe e3 ee 24 0e 08 00 45 00 ...!Q...\$...E-  
0010 05 dc 4d be 40 00 7f 06 3b ce ac 10 03 01 ac 10 ..M@...;.....  
0020 11 6e 0c 38 d3 20 49 84 eb 45 5b f0 50 38 50 10 ..n·8· I· ·E[-P8P·  
0030 00 fc 82 fe 00 00 3d d5 91 6d 10 6b 8c 92 bf fa .....m·k.....  
0040 dd 5c 4d 08 6a 75 39 a6 ce 28 5a c0 e5 d1 1e da \M·ju9· (Z.....  
0050 75 16 54 3a 97 aa 6e c7 58 24 e4 63 b3 9e 5d c9 u·T·:·n· X\$·c··]  
0060 17 2c db 99 51 d9 9f 74 3b 4a 03 27 6e c3 3d 0e ..,·Q·t ;J·'n·=  
0070 3a 20 59 9c c7 ce b3 a9 a6 ec 47 50 ac 90 ee e0 : Y·.....GP.....  
0080 4d ce 65 aa d0 67 01 08 0f 7e 8a ce 7a 46 1a a1 M·e·g· · ·zF··  
0090 3e cf 02 1b 4a 36 55 8f ba 30 ce a6 9c bb 18 a0 >...J6U· ·0.....  
00a0 a9 06 94 15 ca 49 8e 13 18 09 cc fd d0 56 a2 6d .....I· ···V·m  
00b0 69 07 d2 d5 4f 35 ec a4 8b f3 8b e8 20 a4 c0 64 i...05· ··· ·d  
00c0 a6 e1 d8 ef 40 a7 a4 3d 86 8d fc 4c a6 ca 01 e8 ....@· ···L· ···  
00d0 ba fe e8 e9 62 b7 c5 e6 29 f0 b8 af 40 31 ad 3f ....b· ···)· ·@1·?  
00e0 2e d5 0a 9f bb fd 60 2b 86 e0 f8 49 7d de 0b 1c .....+ ···I]· ···  
00f0 5a c2 0d 2c 5f a6 39 d0 90 3a 04 ce af 55 24 97 Z· ·,·\_9· ···U\$·

No.: 16889 · Time: 36.118998 · Source: 172.16.3.1 · Destination: 172.16.17.110 · Protocol: TCP · Length: 1514 · Info: 3128 → 54048 [ACK] Seq=38187 Ack=566 Win=252 Len=1460

Close Help



Q-6) Try to obtain the username and password of an insecure website using Wire shark.



Q-7) Demonstrate the usage of hping.

```
200420116059@kali:~$ sudo hping3 -c 4 -n -i 2 www.gtu.ac.in
[sudo] password for 200420116059:
HPING www.gtu.ac.in (eth0 65.1.31.76): NO FLAGS are set, 40 headers + 0 data bytes

--- www.gtu.ac.in hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```