ASSIGNMENT – 3

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

```
200420116059@kali:~$ sudo nmap -sO 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           bna
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           rvd
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           crtp
127     open           crudp
128     open           sscopmce
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
```

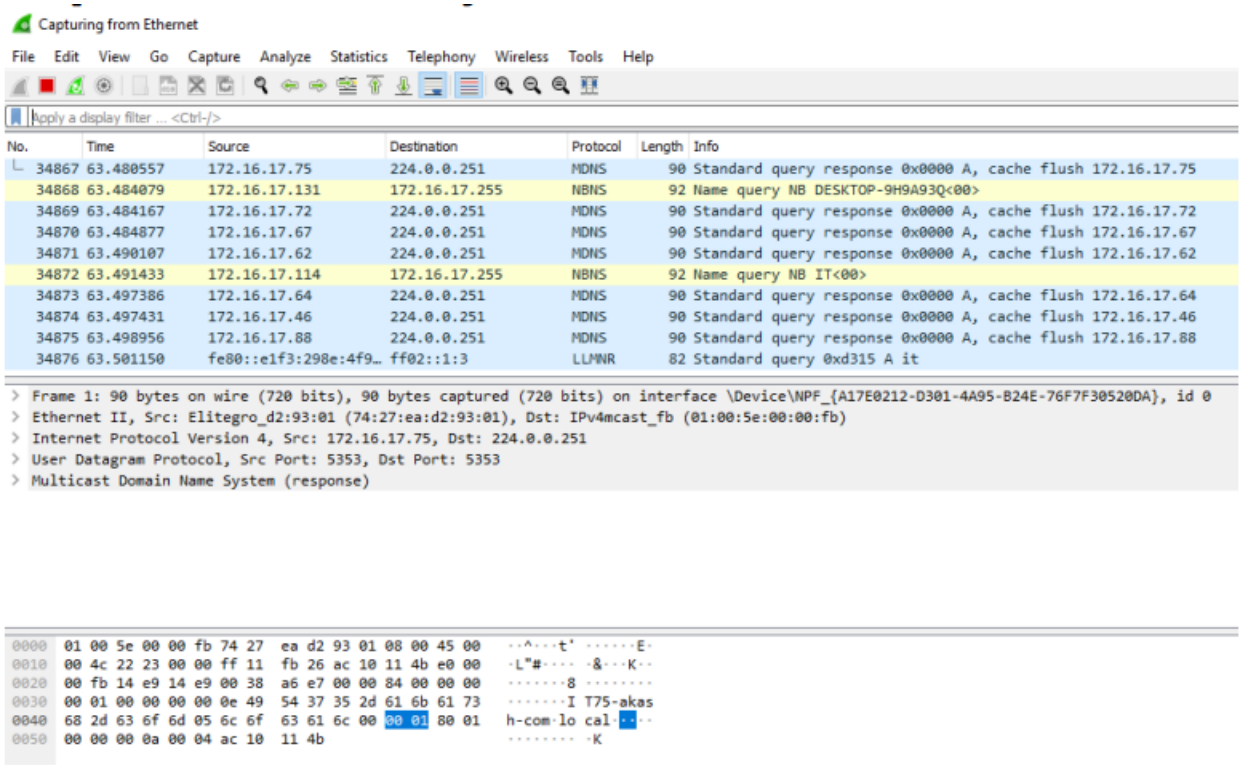
Q-2) Determine which services are available on the host www.scet.ac.in

```
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
```

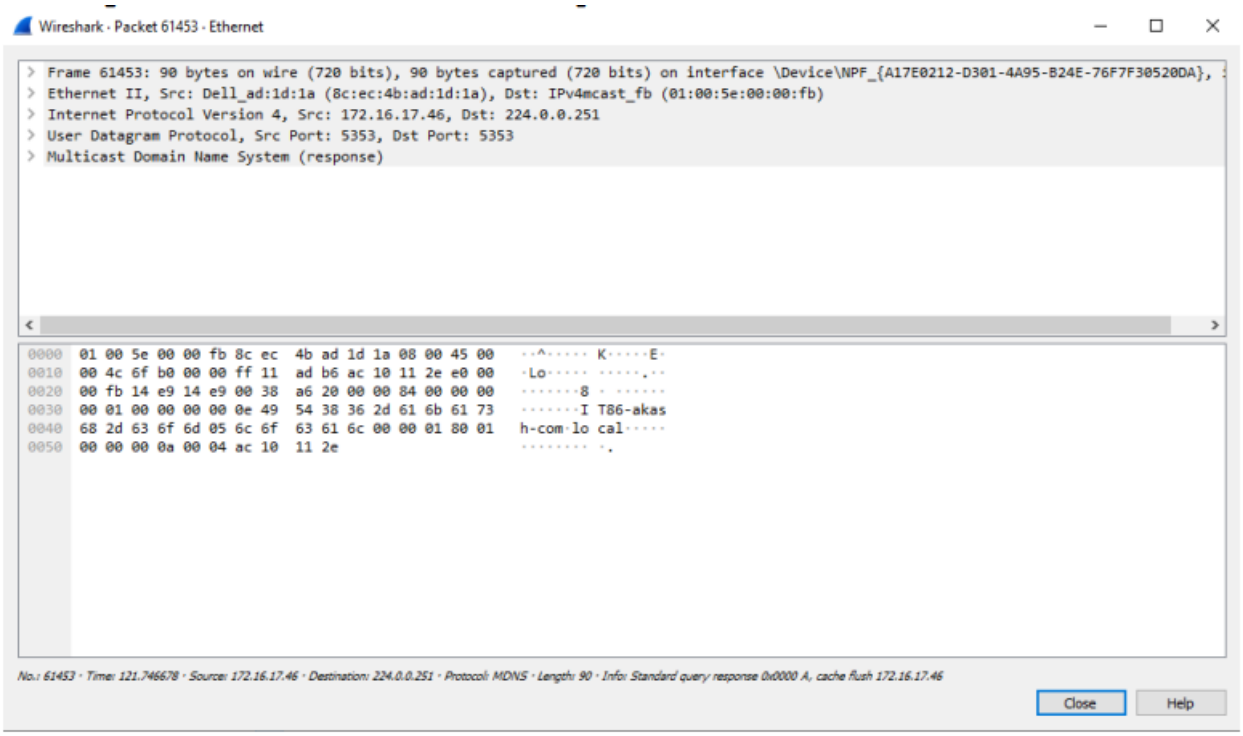
Q-3) Identify the Operating System of www.facebook.com

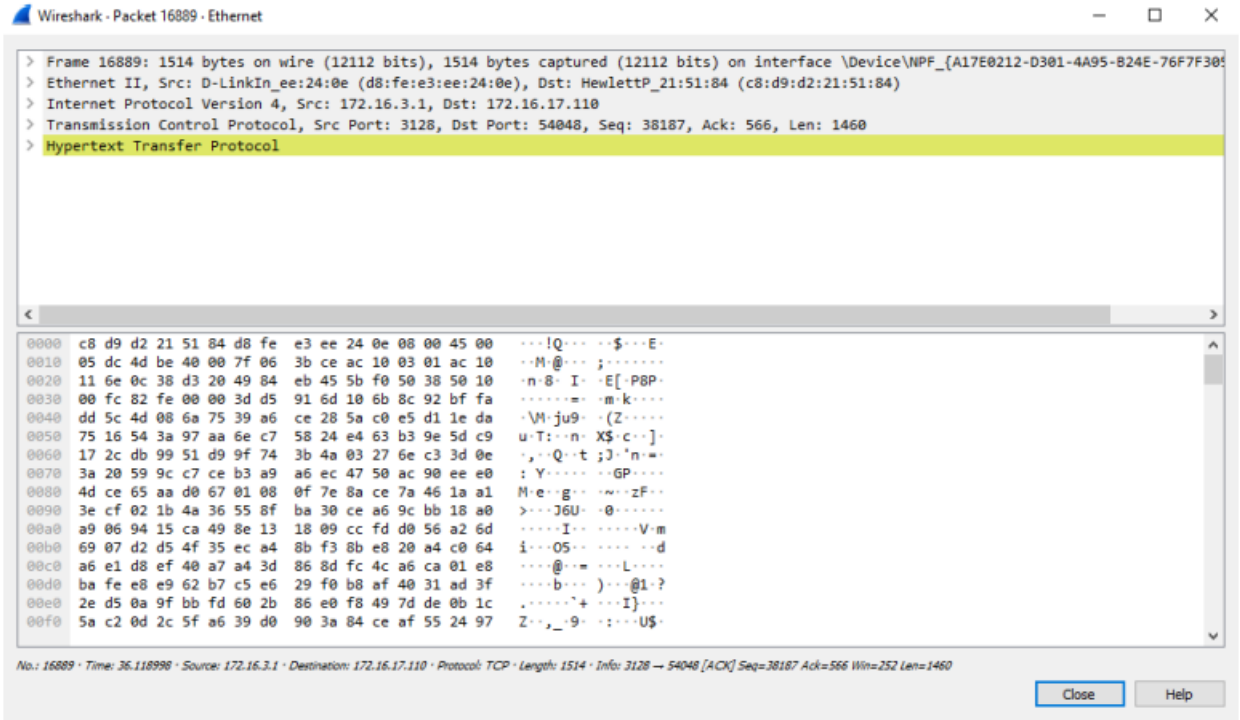
```
200420116059@kali:~$ sudo nmap -O www.facebook.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-30 06:10 UTC
Nmap scan report for www.facebook.com (31.13.66.35)
Host is up (0.00060s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f103:181:face:b00c:0:25de
rDNS record 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.

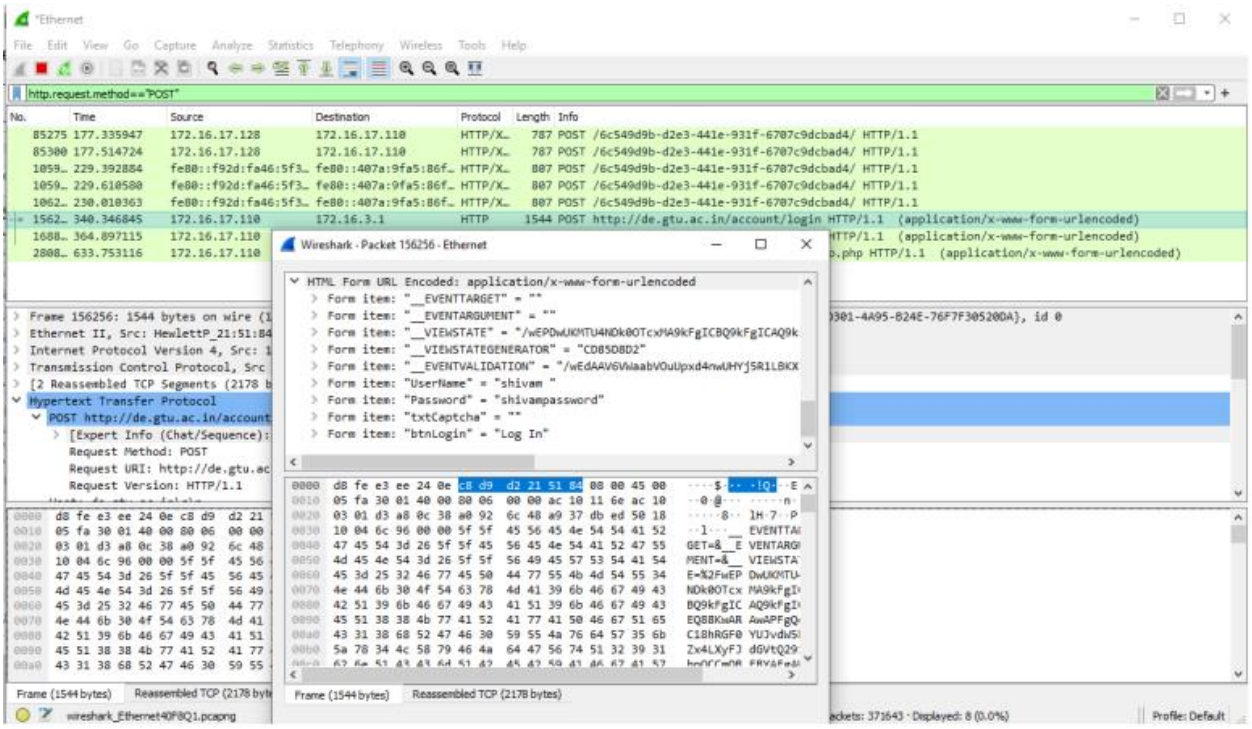


Q-5) Analyze the contents of various protocols.





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
```