ASSIGNMENT – 2

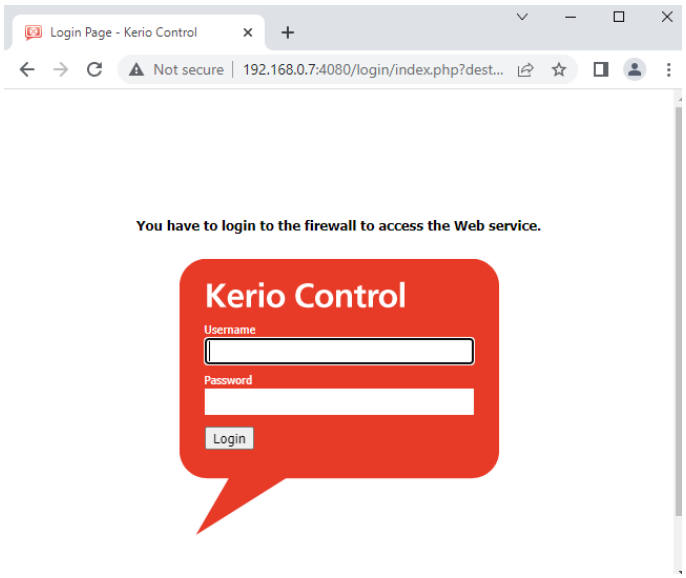
Q-1) Demonstrate the working socat tool.

```
200420116059@kali:~$ socat -d -d - TCP4:www.google.com:80
2022/08/23 06:06:00 socat[525170] N reading from and writing to stdio
2022/08/23 06:06:00 socat[525170] N opening connection to AF=2 172.253.115.103:80
2022/08/23 06:06:00 socat[525170] N successfully connected from local address AF=2 172.31.94.236:56010
2022/08/23 06:06:00 socat[525170] N starting data transfer loop with FDs [0,1] and [5,5]
2022/08/23 06:10:00 socat[525170] N socket 2 (fd 5) is at EOF
2022/08/23 06:10:00 socat[525170] N exiting with status 0
```

Q-2) Perform port forwarding using Fpipe.

```
C:\Users\mvc>FPipe.exe -l 8080 -r 80 www.scet.ac.in
FPipe v2.1 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

Pipe connected:
   In:        127.0.0.1:30283 --> 127.0.0.1:8080
  Out:    172.16.17.106:30285 --> 136.243.80.165:80
Pipe connected:
   In:        127.0.0.1:30286 --> 127.0.0.1:8080
  Out:    172.16.17.106:30287 --> 136.243.80.165:80
Pipe connected:
   In:        127.0.0.1:30284 --> 127.0.0.1:8080
  Out:    172.16.17.106:30293 --> 136.243.80.165:80
```



Q-3) Identify which hosts are live on the network.

```
200420116059@kali:~$ nmap -sn www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-23 06:42 UTC
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.18s latency).
rDNS record for 3.109.160.49: triple5.online
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Q-4) Scan all TCP Port of the any two hosts.

```
200420116059@kali:~$ nmap -sT www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-23 06:42 UTC
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.19s latency).
rDNS record for 3.109.160.49: triple5.online
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
```

Q-5) Scan all TCP Port of the any two hosts without completing TCP three-way handshakes.

```
200420116059@kali:~$ sudo nmap -sS www.triple5.online
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-23 07:03 UTC
Nmap scan report for www.triple5.online (3.109.160.49)
Host is up (0.19s latency).
rDNS record for 3.109.160.49: triple5.online
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 26.58 seconds
```

Q-6) Scan all TCP Port of the any two hosts with stealth scan.