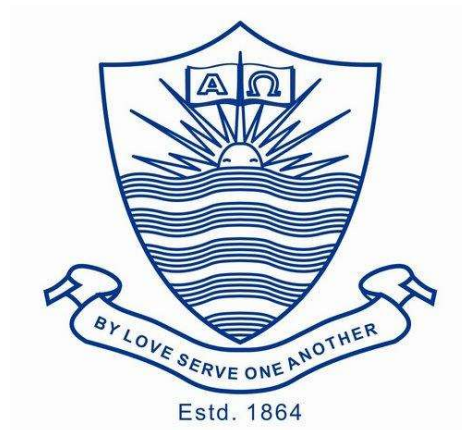


# **FORMAN CHRISTIAN COLLEGE (A CHARTERED UNIVERSITY)**



**COMP 421 (Information Security)**

**SECTION - B**

**2023 FALL**

**ASSIGNMENT # 3**

**NMAP Basic Port Scans**

**Gulraiz Noor Bari (231-525536)**

## SCAN # 1 – TCP CONNECT SCAN

```
root@ip-10-10-227-139: ~  
File Edit View Search Terminal Help  
root@ip-10-10-227-139:~# nmap -sT 10.10.227.139  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-13 13:54 GMT  
Nmap scan report for ip-10-10-227-139.eu-west-1.compute.internal (10.10.227.139)  
Host is up (0.00021s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
111/tcp   open  rpcbind  
389/tcp   open  ldap  
3389/tcp  open  ms-wbt-server  
5901/tcp  open  vnc-1  
6001/tcp  open  X11:1  
7777/tcp  open  cbt  
7778/tcp  open  interwise  
  
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds  
root@ip-10-10-227-139:~#
```

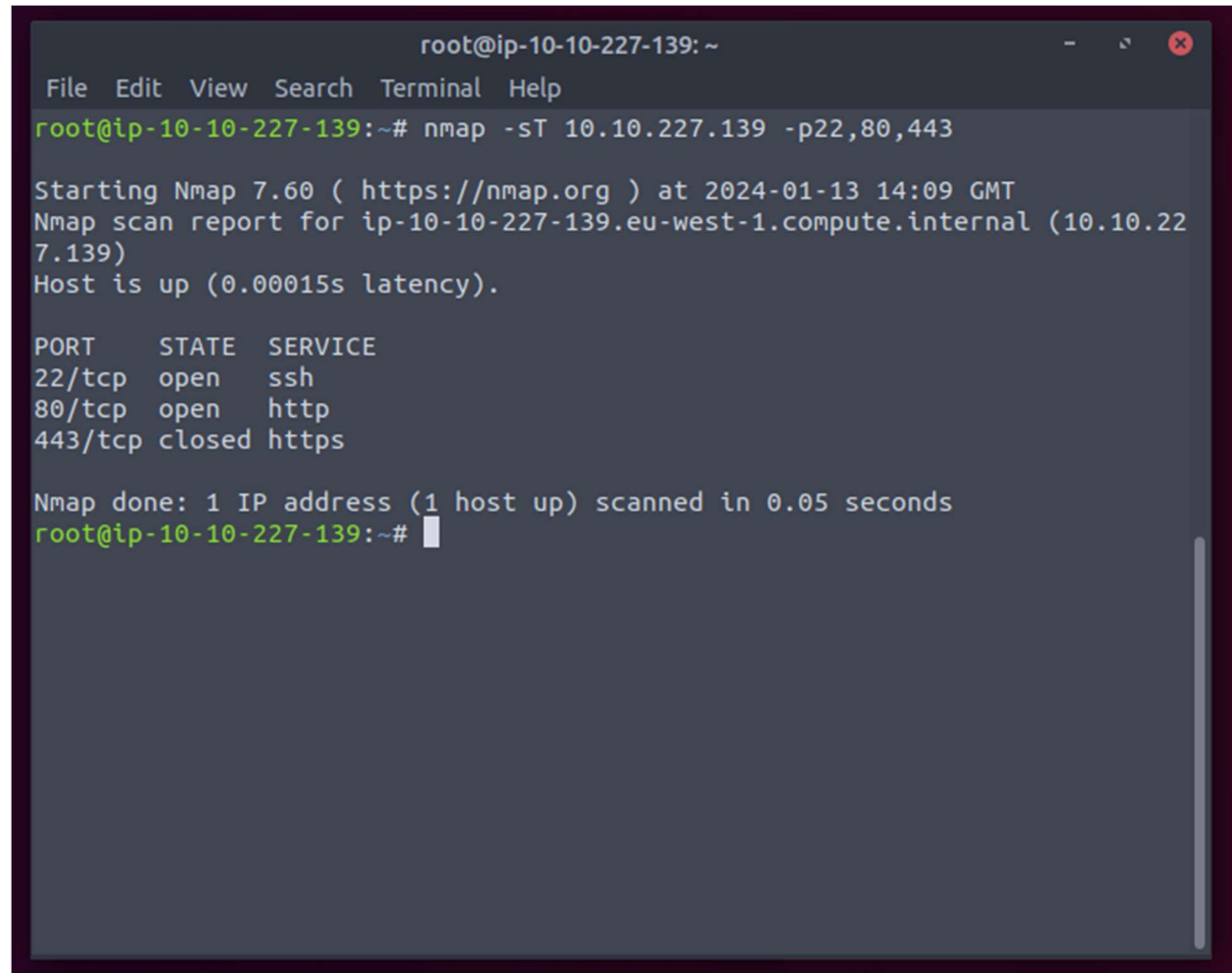
## SCAN # 2 – TCP SYN SCAN

```
root@ip-10-10-227-139: ~  
File Edit View Search Terminal Help  
root@ip-10-10-227-139:~# sudo nmap -sS 10.10.227.139  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-13 13:59 GMT  
Nmap scan report for ip-10-10-227-139.eu-west-1.compute.internal (10.10.227.139)  
Host is up (0.0000080s latency).  
Not shown: 991 closed ports  
PORT      STATE      SERVICE  
22/tcp    open      ssh  
80/tcp    open      http  
111/tcp   open      rpcbind  
389/tcp   open      ldap  
3389/tcp  open      ms-wbt-server  
5901/tcp  open      vnc-1  
6001/tcp  open      X11:1  
7777/tcp  filtered  cbt  
7778/tcp  filtered  interwise  
  
Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds  
root@ip-10-10-227-139:~#
```

### SCAN # 3 – UDP SCAN

```
root@ip-10-10-227-139: ~  
File Edit View Search Terminal Help  
root@ip-10-10-227-139:~# sudo nmap -sU -F -v 10.10.227.139  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-13 14:04 GMT  
Initiating Parallel DNS resolution of 1 host. at 14:04  
Completed Parallel DNS resolution of 1 host. at 14:04, 0.00s elapsed  
Initiating UDP Scan at 14:04  
Scanning ip-10-10-227-139.eu-west-1.compute.internal (10.10.227.139) [100  
ports]  
Discovered open port 111/udp on 10.10.227.139  
Increasing send delay for 10.10.227.139 from 0 to 50 due to 31 out of 103  
dropped probes since last increase.  
Increasing send delay for 10.10.227.139 from 50 to 100 due to 11 out of 34  
dropped probes since last increase.  
Increasing send delay for 10.10.227.139 from 100 to 200 due to 11 out of 2  
2 dropped probes since last increase.  
Completed UDP Scan at 14:04, 7.58s elapsed (100 total ports)  
Nmap scan report for ip-10-10-227-139.eu-west-1.compute.internal (10.10.22  
7.139)  
Host is up (0.000073s latency).  
Not shown: 96 closed ports  
PORT      STATE      SERVICE  
68/udp    open|filtered dhcpc  
111/udp    open              rpcbind  
631/udp    open|filtered ipp  
5353/udp   open|filtered zeroconf  
  
Read data files from: /usr/bin/../../share/nmap
```

## SCAN # 4 – TCP SCAN ON SPECIFIC PORTS



```
root@ip-10-10-227-139: ~  
File Edit View Search Terminal Help  
root@ip-10-10-227-139:~# nmap -sT 10.10.227.139 -p22,80,443  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-13 14:09 GMT  
Nmap scan report for ip-10-10-227-139.eu-west-1.compute.internal (10.10.227.139)  
Host is up (0.00015s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
443/tcp   closed https  
  
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds  
root@ip-10-10-227-139:~#
```