Experiment 3

Name: Danyl Fernandes (72)
Class: TE COMPS
XIE ID: 2020012004
Date: 14-08-2021

Aim: Perform network discovery using discovery tools (eg. nmap, netdiscover)

What is nmap?

- Nmap is a network mapper software that maps the entire network.
- It can give information about a computer inside the network.
- It can be used for various purposes like detecting live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection
- Apart from these it can be used for vulnerability detection and security testing purposes.

Zenmap

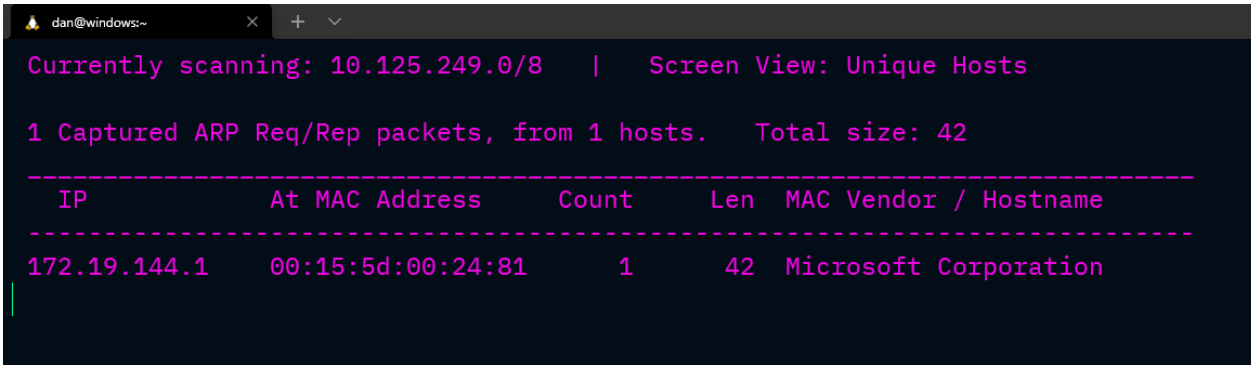
- Since nmap is a linux command line utility, it can require some command line knowledge and hence, nmap also provides a GUI version of nmap that has all the same features as the CLI application.
- Zenmap is the official nmap security scanner GUI and it is multi-platform, open-source and free and makes using nmap really easy for non-technical users.
- It is a nice introduction to nmap for beginners.

Commands:

netdiscover:

- This command helps to find the computers connected in your house
- All the devices connected in the current network can be listed using this command
- It provides us with a list of IP addresses and mac addresses in the network
- It was initially developed to gain information about wireless networks without DHCP servers.
- It can also be used to monitor your network's ARP traffic.
- **Syntax:** netdiscover [options]

Output:



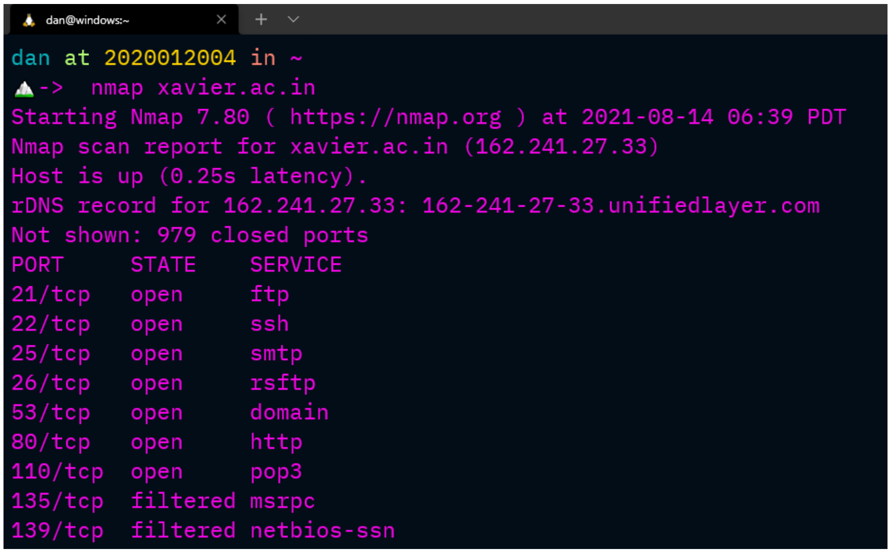
```
Currently scanning: 10.125.249.0/8   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 42
_____________________________________________________________________________
  IP             At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.19.144.1    00:15:5d:00:24:81      1      42  Microsoft Corporation
```

When to use nmap?

- Nmap can be used when all the services on a server, mobile, PC, Switch, Router need to be discovered
- When the services and the versions of those services need to be detected for troubleshooting or intelligence gathering.
- It can be used widely during Security Audits to detect vulnerabilities, get services, check for ports that are open unnecessarily and get more information about the server overall.
- It can be used during security testing when the OS information is needed to be detected.
- It can also be used as the GUI versions to quickly perform the same tasks but without having to know the command line or terminal.

nmap xavier.ac.in

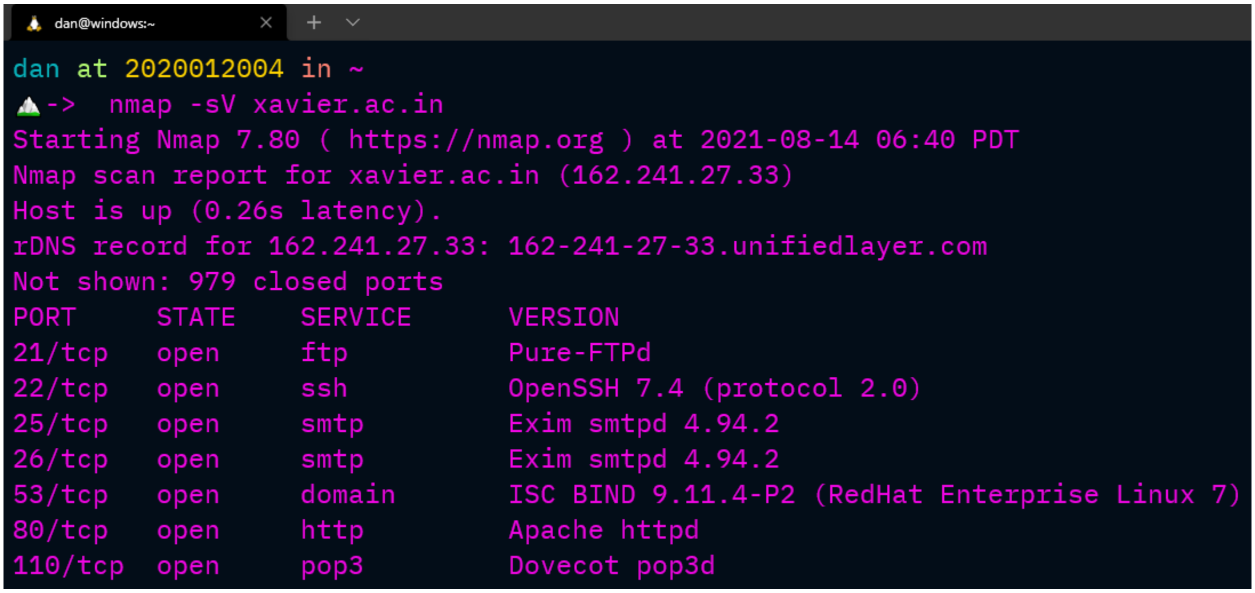
- This command is used to scan a single host
- The second argument in the command is the host that needs to be scanned (in this case xavier.ac.in)
- **Output:**



```
dan at 2020012004 in ~
-> nmap xavier.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:39 PDT
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.25s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com
Not shown: 979 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
```

nmap -sV xavier.ac.in

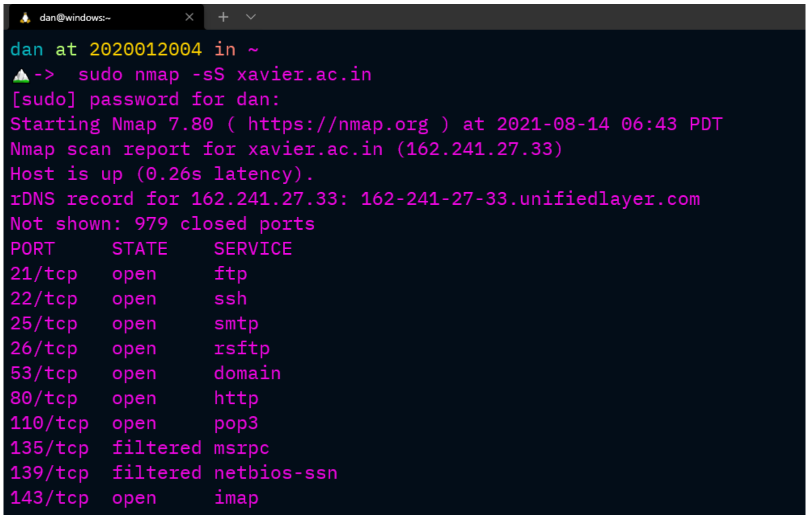
- This command uses the -V flag
- The V stands for version
- It returns all the services that are running on the host along with the actual or an estimate of the version number of the services.
- This is helpful in intelligence gathering and getting a look at more information.
- **Output:**



```
dan at 2020012004 in ~
▲->  nmap -sV xavier.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:40 PDT
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.26s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com
Not shown: 979 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          Pure-FTPd
22/tcp   open     ssh          OpenSSH 7.4 (protocol 2.0)
25/tcp   open     smtp         Exim smtpd 4.94.2
26/tcp   open     smtp         Exim smtpd 4.94.2
53/tcp   open     domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp   open     http         Apache httpd
110/tcp  open     pop3         Dovecot pop3d
```

nmap -sS xavier.ac.in

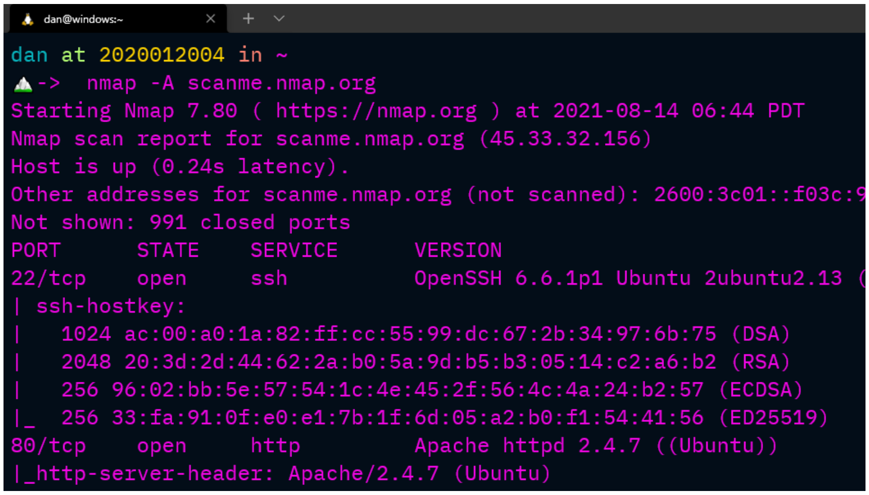
- This command uses the -S option
- This option S stands for Stealth mode.
- It works by sending the SYN packet, which is followed by receiving the SYN ACK packet from the host.
- But the stealth works by not sending the final ACK packet in the TCP 3-way handshake and instead sending the RST (reset) packet.
- **Output:**



```
dan at 2020012004 in ~
▲->  sudo nmap -sS xavier.ac.in
[sudo] password for dan:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:43 PDT
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.26s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com
Not shown: 979 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
```

nmap -A scanme.nmap.org

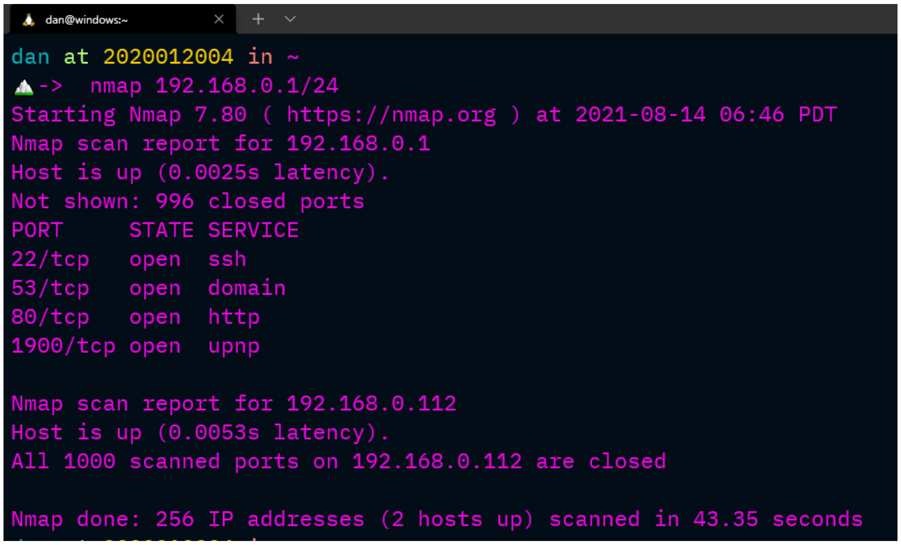
- This command used the A option
- This option A stands for All.
- As the name suggests the all options returns all useful information that is required in intelligence gathering
- A scan of all the ports, estimation of the OS running on the host, possible services, service version numbers, and even vulnerabilities (if any).
- **Output:**



```
dan at 2020012004 in ~
-> nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:44 PDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:9
Not shown: 991 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
```

nmap 192.168.0.1/24

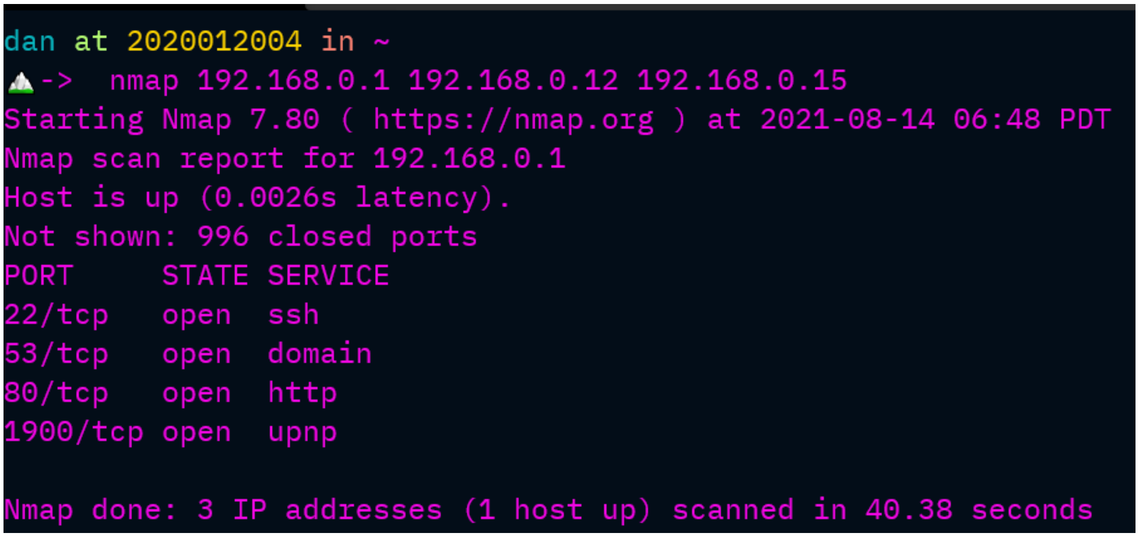
- This command is used to do a multiple host scan.
- This particular command is scanning all the hosts on a host server that has a /24 subnet
- Which means the possible IP addresses from 192.168.0.1-254 will all be scanned
- This is useful when you want to scan the entire network but are not sure about what services are on what host device
- **Output:**



```
dan at 2020012004 in ~
-> nmap 192.168.0.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:46 PDT
Nmap scan report for 192.168.0.1
Host is up (0.0025s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp

Nmap scan report for 192.168.0.112
Host is up (0.0053s latency).
All 1000 scanned ports on 192.168.0.112 are closed

Nmap done: 256 IP addresses (2 hosts up) scanned in 43.35 seconds
```

nmap 192.168.0.1 192.168.0.12 192.168.0.15

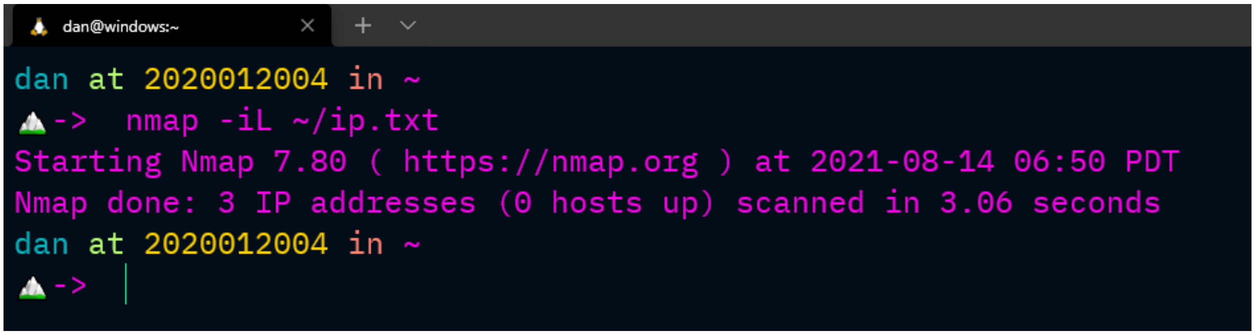
- This command is also a variant of doing a multiple host scan.
- The functioning of this command is exactly the same as the previous command but only difference is that we have explicitly specified exactly 3 IPs
- So the previous command scanned 254 devices and this one will scan 3 (the exact three as specified)
- **Output:**



```
dan at 2020012004 in ~
▲->  nmap 192.168.0.1 192.168.0.12 192.168.0.15
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:48 PDT
Nmap scan report for 192.168.0.1
Host is up (0.0026s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp

Nmap done: 3 IP addresses (1 host up) scanned in 40.38 seconds
```

nmap -iL ~/ip.txt

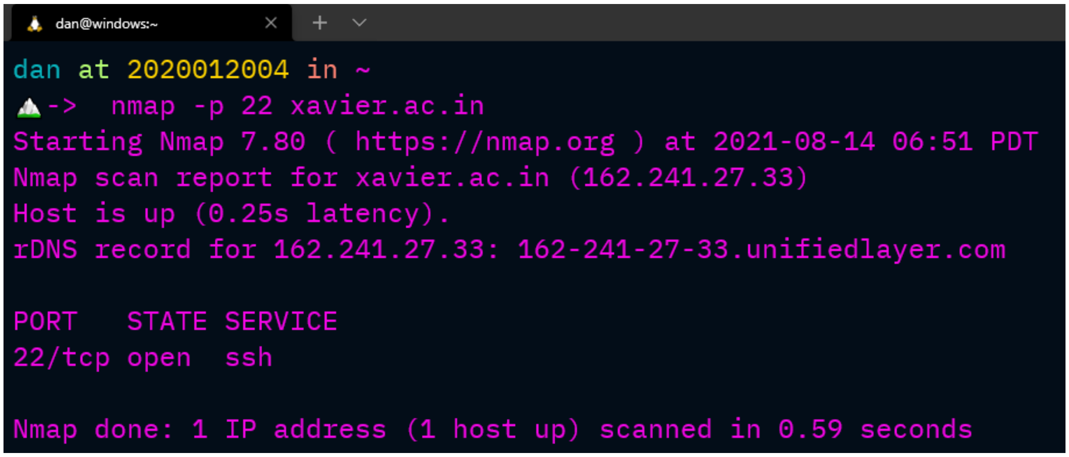
- This command is another variant of the multiple host scan.
- Here we are specifying the IP addresses but through a text file (which in my case is inside my home directory but you can specify any path)
- It will scan all the IP addresses specified in the .txt file
- This is useful when you want to scan multiple addresses many times, so that you don't have to type all the addresses everytime into the command.
- You can type them once and use the file multiple times.
- **Output:**



```
dan at 2020012004 in ~
▲->  nmap -iL ~/ip.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:50 PDT
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.06 seconds
dan at 2020012004 in ~
▲->
```

nmap -p 22 xavier.ac.in

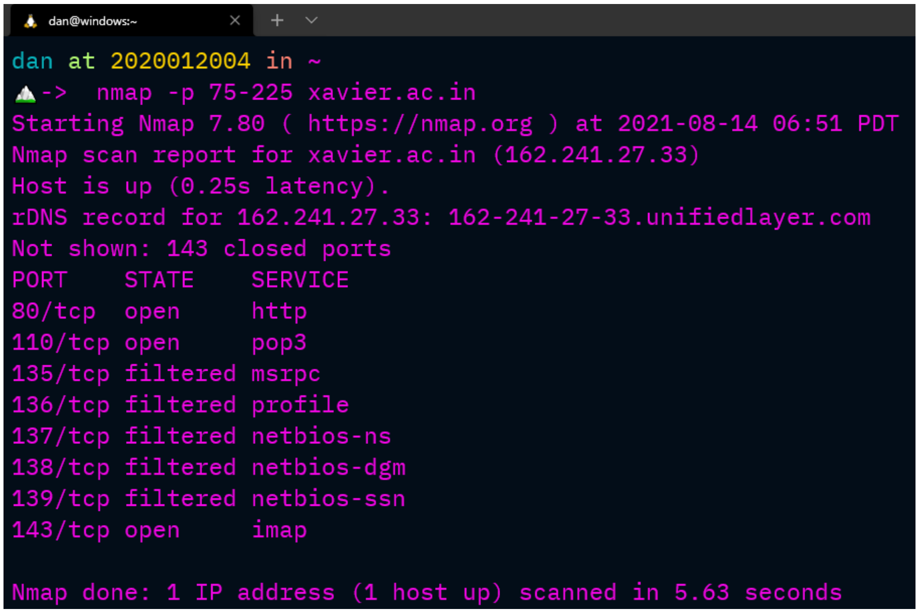
- This command uses the -p option.
- The p option stands for port.
- Here you can specify a port number after -p and nmap will scan that exact port and give you information about the service running on that port.
- It will also let you know if the port is open (Open), closed (Closed), or behind a firewall or proxy (Filtered)
- In this particular command we are scanning port 22 which is the SSH port.
- **Output:**



```
dan at 2020012004 in ~
-> nmap -p 22 xavier.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:51 PDT
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.25s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

nmap -p 75-225 xavier.ac.in

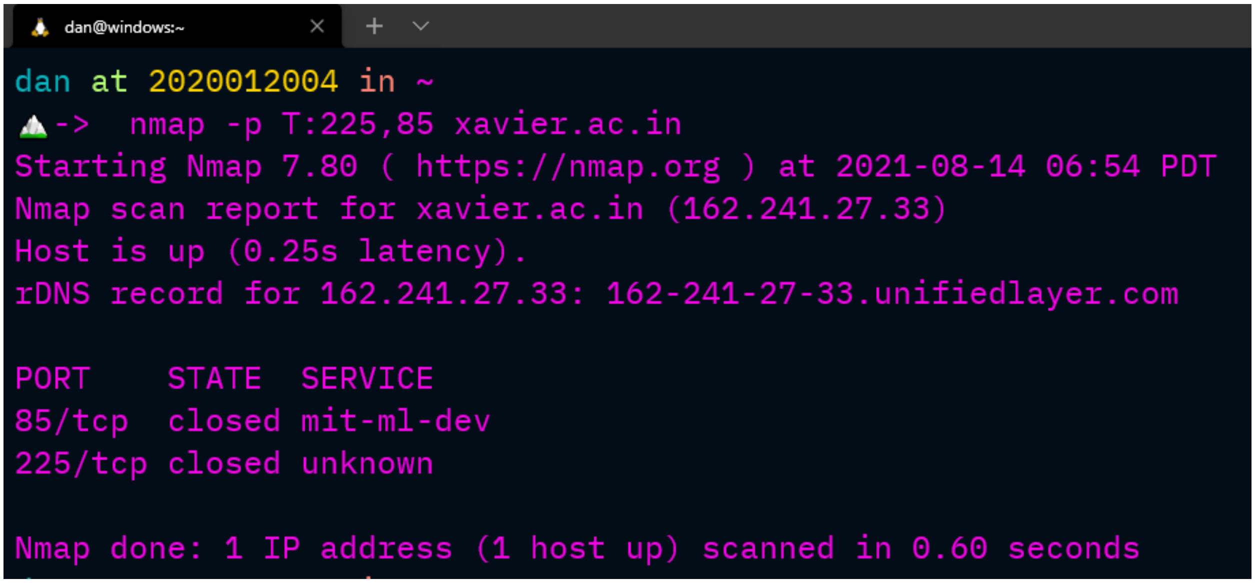
- This command uses the -p option again.
- Here the command takes a range of ports to scan.
- By default, nmap will scan for the top 1000 ports and check them.
- But if you want to scan for a specific range of ports, you can use this command for that purpose.
- **Output:**



```
dan at 2020012004 in ~
-> nmap -p 75-225 xavier.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:51 PDT
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.25s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com
Not shown: 143 closed ports
PORT    STATE    SERVICE
80/tcp  open     http
110/tcp open     pop3
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
143/tcp open     imap

Nmap done: 1 IP address (1 host up) scanned in 5.63 seconds
```

nmap -p T:225,85 xavier.ac.in

- This command is the same as the previous command.
- The only difference we can see is the T option.
- The T option here specifies that we want to scan a specific set of ports but only TCP ports not UDP.
- **Output:**

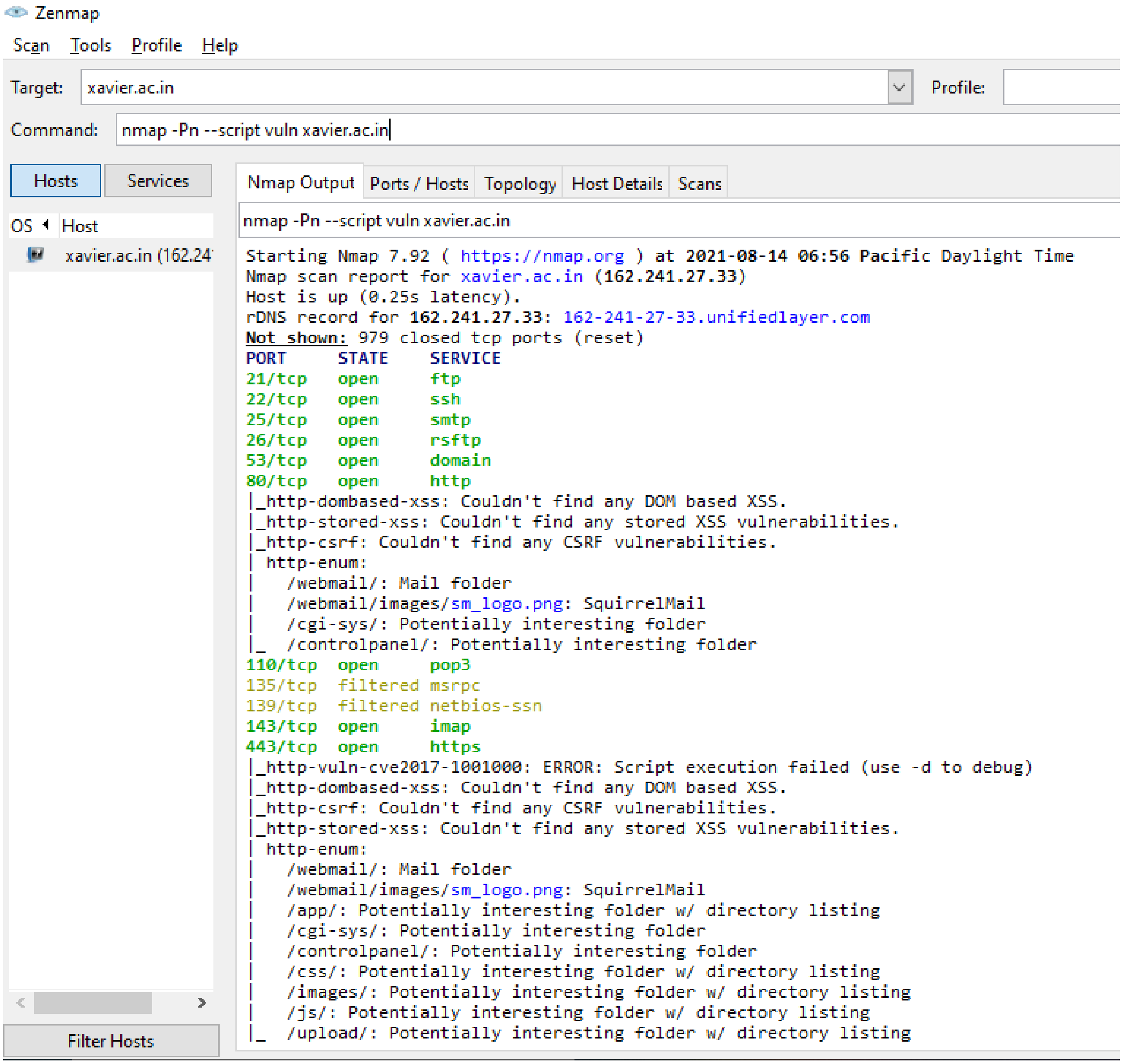


```
dan at 2020012004 in ~
▲->  nmap -p T:225,85 xavier.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-14 06:54 PDT
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.25s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com

PORT    STATE  SERVICE
85/tcp  closed mit-ml-dev
225/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

Zenmap GUI Commands

nmap -Pn --script vuln xavier.ac.in

- This command uses two main options -Pn and –script.
- The -Pn option specifies that we want to scan all 65535 ports on the host xavier.ac.in
- The –script option helps us to give nmap a script to run to check for vulnerabilities on the host.
- The vuln is a built-in script that checks for the most common vulnerabilities on the common ports
- **Output:**

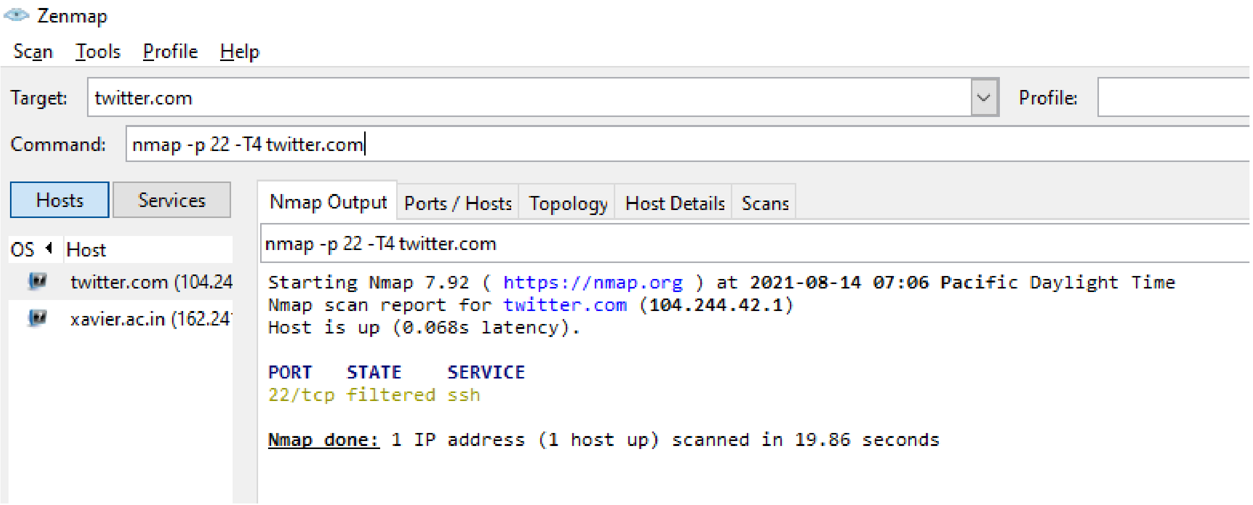


```
nmap -Pn --script vuln xavier.ac.in
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-14 06:56 Pacific Daylight Time
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.25s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com
Not shown: 979 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /webmail/: Mail folder
|   /webmail/images/sm_logo.png: SquirrelMail
|   /cgi-sys/: Potentially interesting folder
|_  /controlpanel/: Potentially interesting folder
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /webmail/: Mail folder
|   /webmail/images/sm_logo.png: SquirrelMail
|   /app/: Potentially interesting folder w/ directory listing
|   /cgi-sys/: Potentially interesting folder
|   /controlpanel/: Potentially interesting folder
|   /css/: Potentially interesting folder w/ directory listing
|   /images/: Potentially interesting folder w/ directory listing
|   /js/: Potentially interesting folder w/ directory listing
|_  /upload/: Potentially interesting folder w/ directory listing
```

nmap -p 22 -T4 twitter.com

- This command uses the option -p as we have seen before.
- It also uses the T option.
- This option specifies the speed by which you want to scan.
- T1 is a slow scan and T4 is a fast scan.
- **Output:**



Target: twitter.com

Profile:

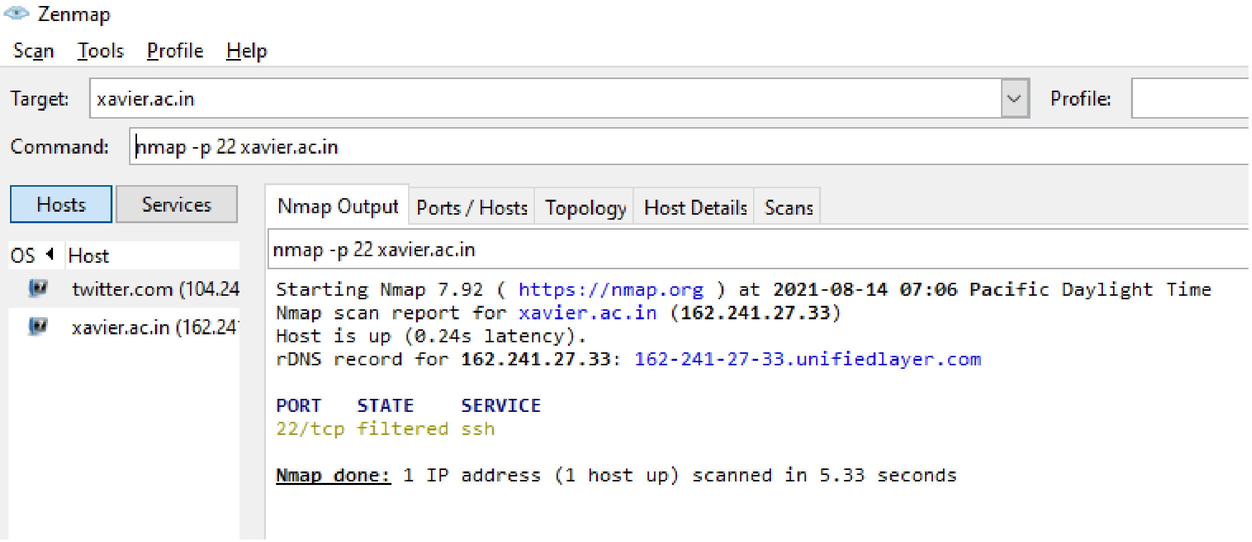
Command: nmap -p 22 -T4 twitter.com

twitter.com (104.24
xavier.ac.in (162.24

```
nmap -p 22 -T4 twitter.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-14 07:06 Pacific Daylight Time
Nmap scan report for twitter.com (104.244.42.1)
Host is up (0.068s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 19.86 seconds
```

nmap -p 22 xavier.ac.in

- This command scans xavier.ac.in and checks the status of port 22 on the server
- **Output:**



Target: xavier.ac.in

Profile:

Command: nmap -p 22 xavier.ac.in

twitter.com (104.24
xavier.ac.in (162.24

```
nmap -p 22 xavier.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-14 07:06 Pacific Daylight Time
Nmap scan report for xavier.ac.in (162.241.27.33)
Host is up (0.24s latency).
rDNS record for 162.241.27.33: 162-241-27-33.unifiedlayer.com

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 5.33 seconds
```

Conclusion: Hence we successfully learnt how to perform network discovery using discovery tools such as nmap and netdiscover.