MALLE RAKESH

11903020

B42

KE022

INT301- OPENSOURCE TECHNOLOGIES

As a network administrator, briefly what techniques, tools, and methodologies would follow to perform testing on the following (use any open source software) :-

a) Network devices security

b) Physical security

Network devices security: There are lot of tools to perform the network devices security some of them are Nmap, OpenVAS and Burp Suite etc.

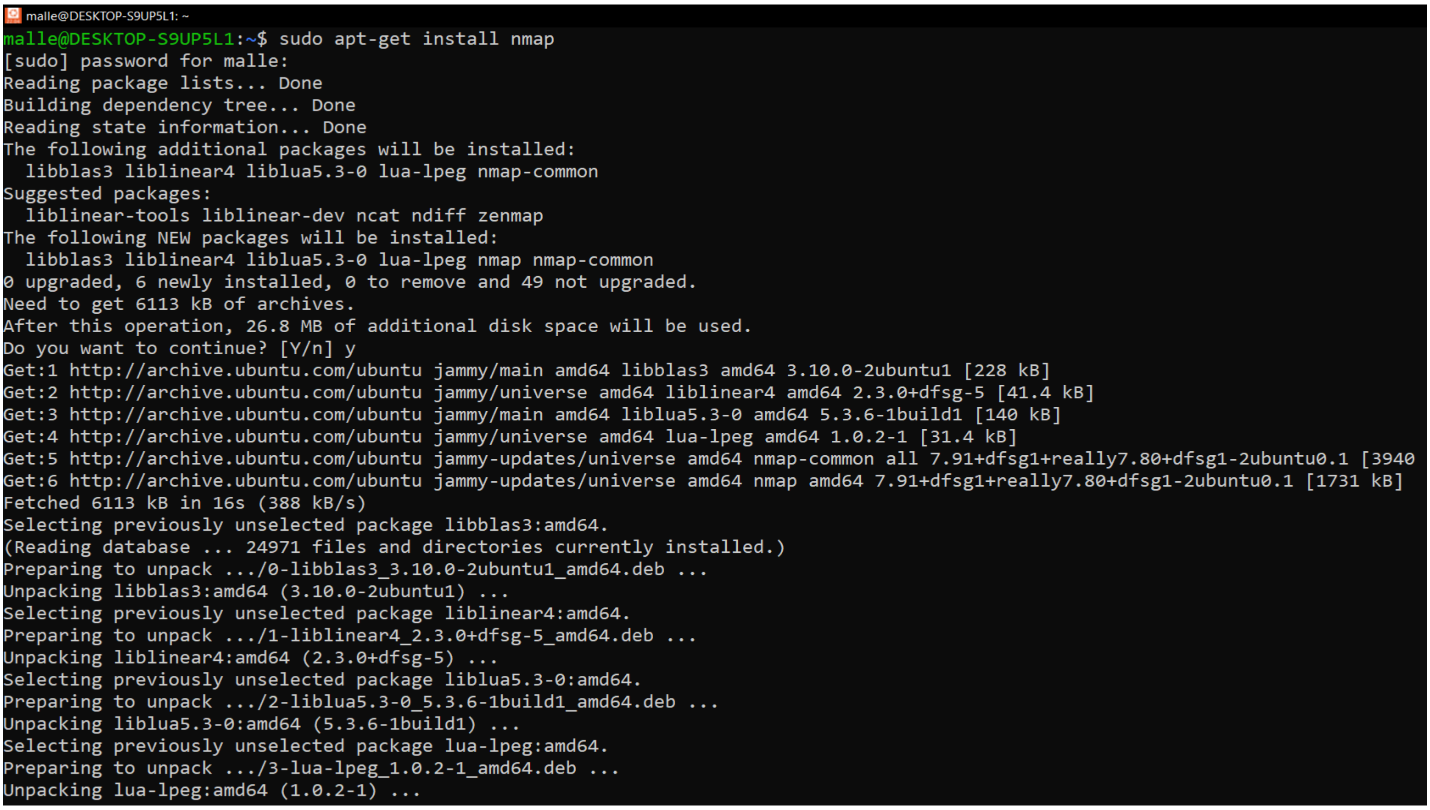
I am going to Use Nmap tool to test the network devices and physical security.

Nmap (Network Mapper) is a free and open-source network scanning tool used for exploring networks and conducting security audits. It is widely used by security professionals, system administrators, and network administrators to identify open ports, running services, and operating systems on a network.

Nmap is widely used for network security auditing, vulnerability assessment, and penetration testing. It can also be used to map out a network and identify potential vulnerabilities, misconfigured devices, and other security risks. However, it's important to note that Nmap should only be used on networks that you own or have permission to scan. Using it on unauthorized networks can be illegal and result in severe consequences.

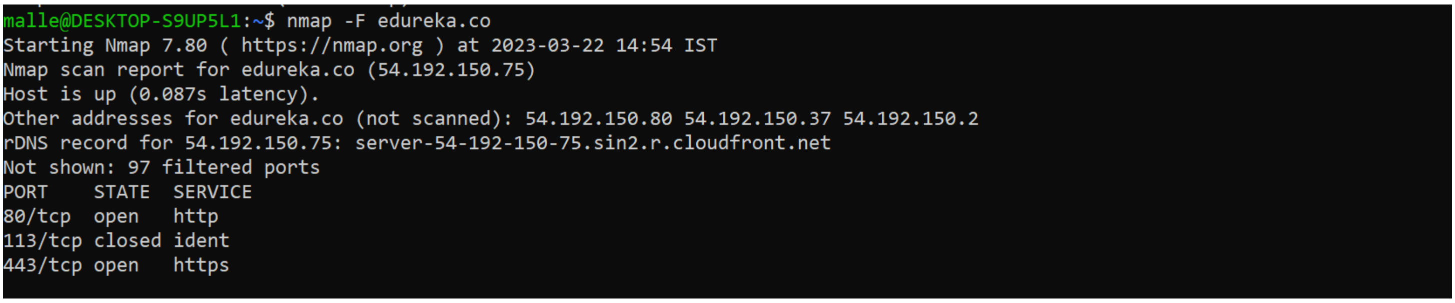
Nmap can be run on a variety of operating systems, including Windows, Linux, and macOS. It can be used to perform a wide range of network analysis and security tasks, such as network inventory, network mapping, vulnerability assessment, and penetration testing. Nmap is a powerful tool but should be used responsibly and ethically, as unauthorized scanning of networks or hosts without permission can be illegal and result in serious consequences.

Nmap



```
malle@DESKTOP-S9UP5L1: ~
malle@DESKTOP-S9UP5L1:~$ sudo apt-get install nmap
[sudo] password for malle:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 49 not upgraded.
Need to get 6113 kB of archives.
After this operation, 26.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/main amd64 libblas3 amd64 3.10.0-2ubuntu1 [228 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 liblinear4 amd64 2.3.0+dfsg-5 [41.4 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/main amd64 liblua5.3-0 amd64 5.3.6-1build1 [140 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap-common all 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [3940
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap amd64 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [1731 kB]
Fetched 6113 kB in 16s (388 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 24971 files and directories currently installed.)
Preparing to unpack .../0-libblas3_3.10.0-2ubuntu1_amd64.deb ...
Unpacking libblas3:amd64 (3.10.0-2ubuntu1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../1-liblinear4_2.3.0+dfsg-5_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-5) ...
Selecting previously unselected package liblua5.3-0:amd64.
Preparing to unpack .../2-liblua5.3-0_5.3.6-1build1_amd64.deb ...
Unpacking liblua5.3-0:amd64 (5.3.6-1build1) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../3-lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
```

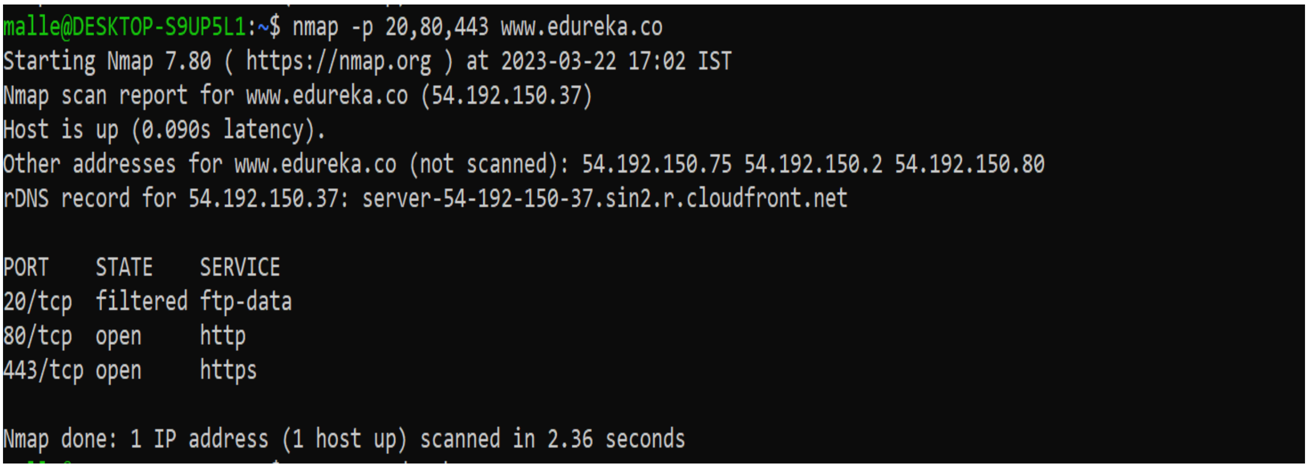
To install nmap software in ubuntu type **sudo apt-get install nmap** in terminal.



```
malle@DESKTOP-S9UP5L1:~$ nmap -F edureka.co
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-22 14:54 IST
Nmap scan report for edureka.co (54.192.150.75)
Host is up (0.087s latency).
Other addresses for edureka.co (not scanned): 54.192.150.80 54.192.150.37 54.192.150.2
rDNS record for 54.192.150.75: server-54-192-150-75.sin2.r.cloudfront.net
Not shown: 97 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https
```

In the above Image we are scanning website

Nmap -F (websitename) F indicates scanning the website in the fast mode. It scans the website and gives the information about the ports and DNS, Ip address of the website in quickly.



```
malle@DESKTOP-S9UP5L1:~$ nmap -p 20,80,443 www.edureka.co
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-22 17:02 IST
Nmap scan report for www.edureka.co (54.192.150.37)
Host is up (0.090s latency).
Other addresses for www.edureka.co (not scanned): 54.192.150.75 54.192.150.2 54.192.150.80
rDNS record for 54.192.150.37: server-54-192-150-37.sin2.r.cloudfront.net

PORT    STATE    SERVICE
20/tcp  filtered ftp-data
80/tcp  open     http
443/tcp open     https

Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds
```

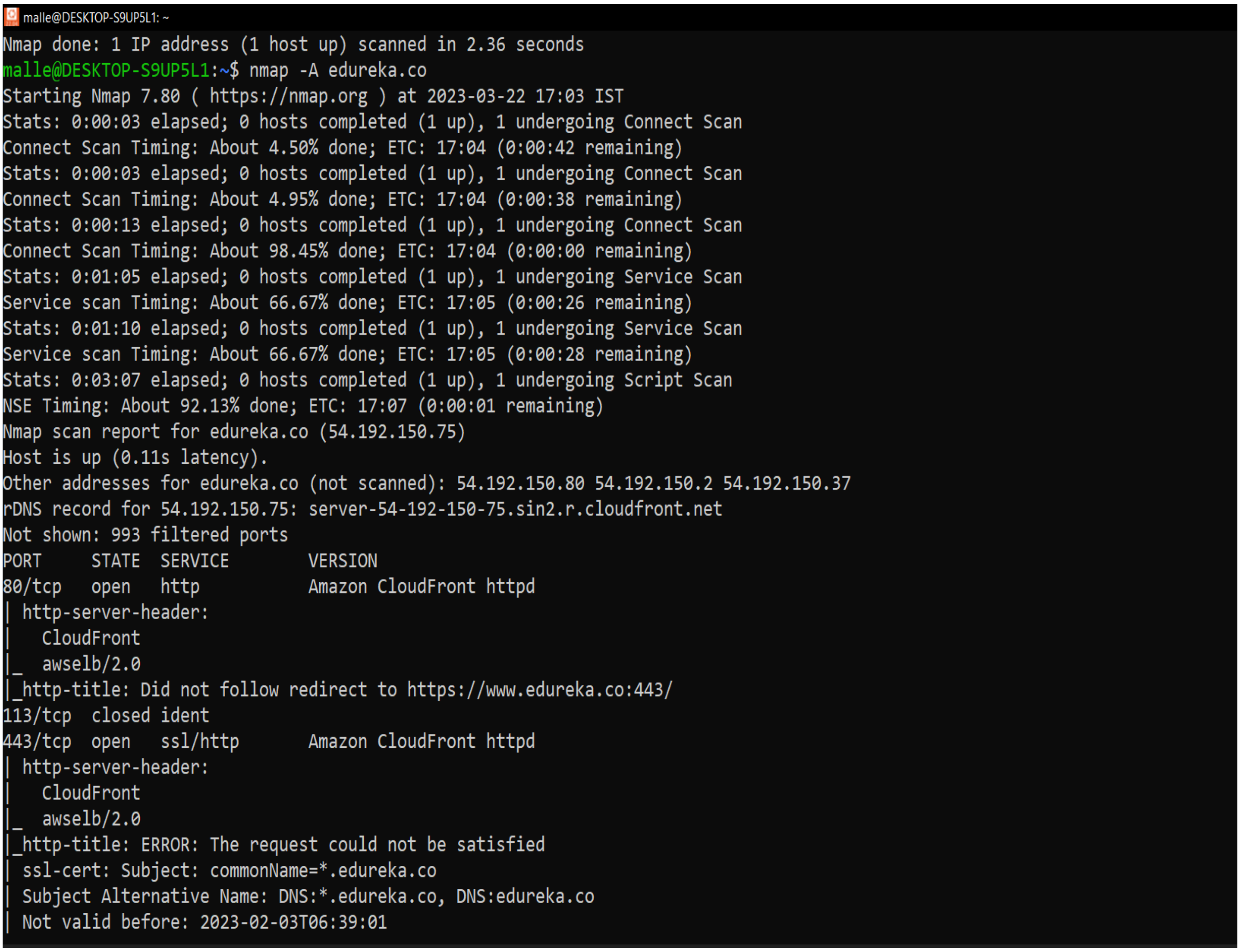
We can find the ports of the network by typing **nmap -p [port number] [website name]** “p indicates port”

An open port means that a process or service is actively listening on that port and is ready to accept incoming connections.

An closed port means it means that there is no process or service actively listening on that port.

It's worth noting that there are other states that a port can be in, such as filtered or stealth, which means that the port is being blocked by a firewall or other security mechanism.

Understanding the state of ports on a device is an essential part of network scanning and security testing, as it can help identify potential vulnerabilities or misconfigurations.

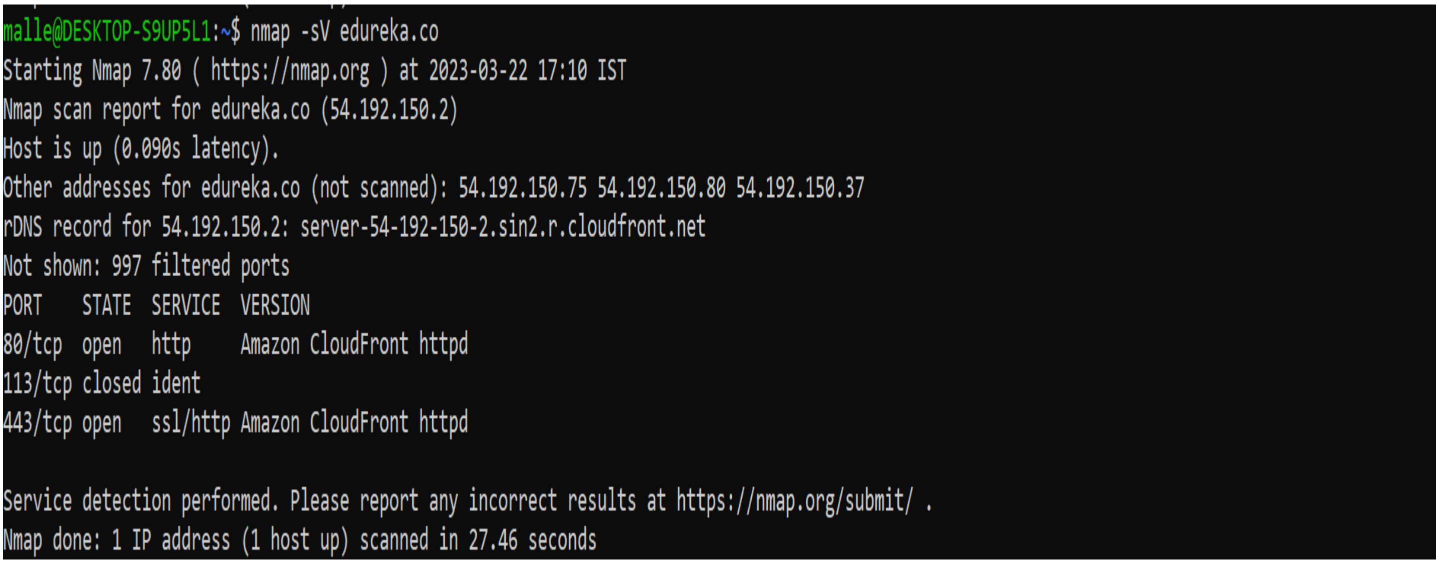


```
malle@DESKTOP-S9UP5L1: ~
Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds
malle@DESKTOP-S9UP5L1:~$ nmap -A edureka.co
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-22 17:03 IST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 4.50% done; ETC: 17:04 (0:00:42 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 4.95% done; ETC: 17:04 (0:00:38 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.45% done; ETC: 17:04 (0:00:00 remaining)
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 17:05 (0:00:26 remaining)
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 17:05 (0:00:28 remaining)
Stats: 0:03:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.13% done; ETC: 17:07 (0:00:01 remaining)
Nmap scan report for edureka.co (54.192.150.75)
Host is up (0.11s latency).
Other addresses for edureka.co (not scanned): 54.192.150.80 54.192.150.2 54.192.150.37
rDNS record for 54.192.150.75: server-54-192-150-75.sin2.r.cloudfront.net
Not shown: 993 filtered ports
PORT     STATE  SERVICE       VERSION
80/tcp   open   http          Amazon CloudFront httpd
| http-server-header:
|   CloudFront
|_  awselb/2.0
|_http-title: Did not follow redirect to https://www.edureka.co:443/
113/tcp  closed ident
443/tcp  open   ssl/http      Amazon CloudFront httpd
| http-server-header:
|   CloudFront
|_  awselb/2.0
|_http-title: ERROR: The request could not be satisfied
| ssl-cert: Subject: commonName=*.edureka.co
| Subject Alternative Name: DNS:*.edureka.co, DNS:edureka.co
| Not valid before: 2023-02-03T06:39:01
```

In this we are running aggressive test of the network by using the command **nmap -A [website name]** A indicates aggressive.

In this it provides complete information of the network of the website like ports, DNS, IP address, traceroute that how the packets move from the client to targeted server and the tcp protocol and the operating system of the network. It useful that the network has any

Vulnerability in the network. It helps the user to keep their network safe and secure from the attackers.

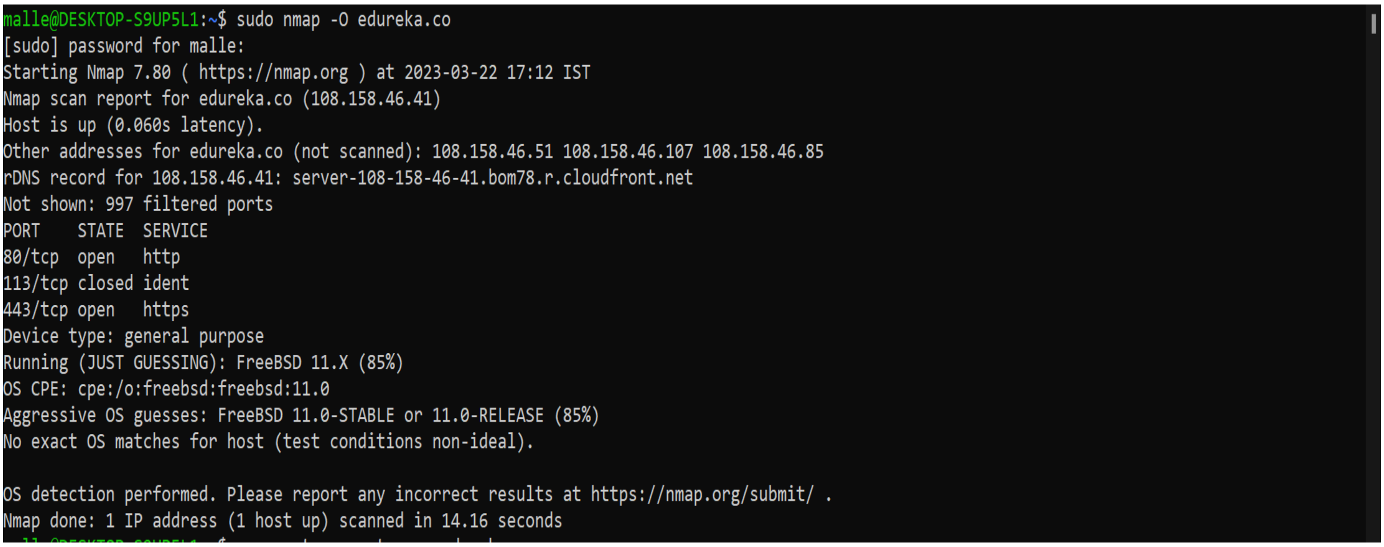


```
malle@DESKTOP-S9UP5L1:~$ nmap -sV edureka.co
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-22 17:10 IST
Nmap scan report for edureka.co (54.192.150.2)
Host is up (0.090s latency).
Other addresses for edureka.co (not scanned): 54.192.150.75 54.192.150.80 54.192.150.37
rDNS record for 54.192.150.2: server-54-192-150-2.sin2.r.cloudfront.net
Not shown: 997 filtered ports
PORT    STATE  SERVICE  VERSION
80/tcp  open   http     Amazon CloudFront httpd
113/tcp closed ident
443/tcp open   ssl/http Amazon CloudFront httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.46 seconds
```

In this we are finding the service version by nmap -sV [websitename]

sV indicates the service version which shows the version of the service and we can keep the updates of the new version of the service if not then the attackers can attack the network easily.

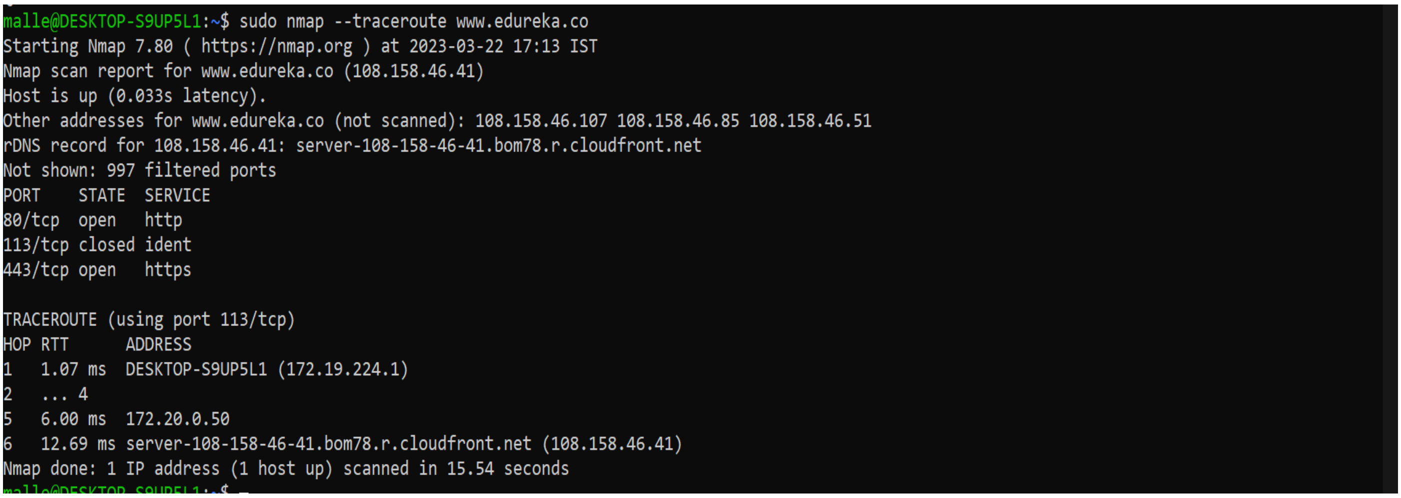


```
malle@DESKTOP-S9UP5L1:~$ sudo nmap -O edureka.co
[sudo] password for malle:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-22 17:12 IST
Nmap scan report for edureka.co (108.158.46.41)
Host is up (0.060s latency).
Other addresses for edureka.co (not scanned): 108.158.46.51 108.158.46.107 108.158.46.85
rDNS record for 108.158.46.41: server-108-158-46-41.bom78.r.cloudfront.net
Not shown: 997 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-STABLE or 11.0-RELEASE (85%)
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 14.16 seconds
```

In this we are finding the operating system by **sudo nmap -O [website name]** O indicates the operating system

Nmap is very intelligent that guess the operating system correctly



```
malle@DESKTOP-S9UP5L1:~$ sudo nmap --traceroute www.edureka.co
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-22 17:13 IST
Nmap scan report for www.edureka.co (108.158.46.41)
Host is up (0.033s latency).
Other addresses for www.edureka.co (not scanned): 108.158.46.107 108.158.46.85 108.158.46.51
rDNS record for 108.158.46.41: server-108-158-46-41.bom78.r.cloudfront.net
Not shown: 997 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
1   1.07 ms  DESKTOP-S9UP5L1 (172.19.224.1)
2   ... 4
5   6.00 ms  172.20.0.50
6   12.69 ms server-108-158-46-41.bom78.r.cloudfront.net (108.158.46.41)
Nmap done: 1 IP address (1 host up) scanned in 15.54 seconds
malle@DESKTOP-S9UP5L1:~$ _
```

In this provides traceroute of the network **sudo nmap –traceroute [websitename]**

Traceroute is a process that is used to trace the path of data packets as they travel from their source to their targeted destination.

It is very helpful to keep our network safe and secure that we can see how are the request packets are going to the targeted server.