NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

LAB 11

LAB 11: Download, install Nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan, etc.

ROLL NO	52
NAME	Sarvesh Patil
CLASS	D15A
SUBJECT	Internet Security Lab
LO MAPPED	LO4: Use tools like sniffers, port scanners, and other related tools for analyzing packets in a network.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

AIM:
Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan, etc.

INTRODUCTION:

NMAP:
Nmap, short for Network Mapper, is a free and open source tool used for vulnerability checking, port scanning and, of course, network mapping. Despite being created back in 1997, Nmap remains the gold standard against which all other similar tools, either commercial or open source, are judged.

Nmap has maintained its preeminence because of the large community of developers and coders who help to maintain and update it. The Nmap community reports that the tool, which anyone can get for free, is downloaded several thousand times every week.

Because of its flexible, open source code base, it can be modified to work within most customized or heavily specialized environments. There are distributions of Nmap specific to Windows, Mac and Linux environments, but Nmap also supports less popular or older operating systems like Solaris, AIX or AmigaOS. The source code is available in C, C++, Perl and Python.

The last major update was Nmap 7.90 in October, 2020, which included more than 70 bug fixes and improvements, as well as various build system upgrades and code quality improvements.

ZENMAP:
To deploy Nmap, users originally had to have some advanced programming skills, or at least know their way around console commands or non-graphical interfaces. That changed recently with the introduction of the Zenmap tool for Nmap, which adds a graphical interface that makes launching the program and analyzing the returned output it generates much more accessible.

Zenmap was created to allow beginners to use the tool. Like Nmap, Zenmap is free and the source code is both open and available to anyone who wants to use or modify it.

Here are some of the capabilities that are enabled by Zenmap: Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. And the results of recent scans can be stored in a searchable database.

Rise of NMAP:
The tool was originally created using the C++ computer language by Gordon Lyon. He released the tool through Phrack Magazine under the pseudonym Fyodor Vaskovitch, which he created after reading Fyodor Dostoevsky's Notes from Underground. Although everyone today knows who Lyon is, he still uses the Fyodor name to identify his work within the Nmap community.

And it's not just computer professionals and the IT community that consider Nmap to be a star. It's been featured in popular culture including books, television shows and blockbuster movies. It's a safe bet that no other tool has had so many cameo appearances in major motion pictures.

Nmap has been featured in thriller movies set in modern day like Ocean's 8, Die Hard 4 and The Girl with the Dragon Tattoo. And even though the tool is 25 years old, if Hollywood has it correct, it will still be used well into the future, even a dystopian one. That's because Nmap is also showcased in Matrix Reloaded, Dredd, Fantastic Four and Elysium. It even has the dubious distinction of being prominently featured in the softcore pornography series HaXXXor.

The community of developers that maintains Nmap, as well as Lyon himself, has extended an open invitation to directors and film writers, offering to provide technical advice to help make movies that feature Nmap a little more realistic. They also maintain an active and ever-expanding filmography about the tool.

One of the reasons why Nmap is featured in so many movies is because of its ability to uncover unknown information about computer networks, meaning that it makes for a great tool for hackers. Ironically, it was designed to help administrators map, protect and defend their networks, but it's powerful enough that the bad guys can also use it for reconnaissance to capture information about the networks they have targeted for nefarious activities.

How does Nmap work?

The heart of Nmap is port scanning. How it works is that users designate a list of targets on a network that they want to learn information about. Users don't need to identify specific targets, which is good because most administrators don't have a complete picture of everything that is using the potentially thousands of ports on their network. Instead, they compile a range of ports to scan.

It's also possible to scan all network ports, although that would potentially take a lot of time and eat up quite a bit of available bandwidth. Plus, depending on the type of passive defenses that are in use on the network, such a massive port scan would likely trigger security alerts. As such, most people use Nmap in more limited deployments or divide different parts of their network up for scheduled scanning over time.

In addition to setting up a range targets to be scanned, users can also control the depth of each scan. For example, a light or limited scan might return information about which ports are open and which have been closed by firewall settings. More detailed scans could additionally capture information about what kind of devices are using those ports, the operating systems they are running and even the services that are active on them. Nmap can also discover deeper information, like the version of those discovered services. That makes it a perfect tool for finding vulnerabilities or assisting with patch management efforts.

Controlling the scans used to require console commands, which of course means that some training was required. But the new Zenmap graphical interface makes it easy for just about everyone to tell Nmap what they want it to discover, with or without formal training. Meanwhile, professionals can continue to use the console commands they always have, making it a useful tool for both experts and novices alike.

Is Nmap a security risk?

While one could make the argument that Nmap is a perfect hacking tool, many of the deeper scan activities require root access and privileges. Someone from outside can't just point Nmap at a target network they don't have permission to access and have it magically uncover vulnerabilities for them to exploit. Not only that, but the attempt would likely trigger a critical security alert by any defensive or network monitoring tools.

That is not to say that Nmap could not be dangerous in the wrong hands, especially if deployed by a turncoat system administrator or someone using stolen credentials. This was demonstrated in the 2016 Oliver Stone movie Snowden (another film that featured Nmap) about the accused traitor Edward Snowden.

What does Nmap do?

When used properly, Nmap can be invaluable for both optimizing and protecting networks and information. All of the return data sent back by ports scanned using Nmap is collected and complied by the program. Based on that information, there are several key activities that most people use the tool to help accomplish. They include:

Network Mapping: This is the core reason why Nmap was created, and remains one of the top uses. Called host discovery, Nmap will identify the types of devices actively using scanned ports. This includes servers, routers, switches and other devices. Users can also see how those devices are connected, and how they link together to form a network map.

Port Rules Discovery: Nmap can easily tell, even with a low-level scan, if a port is open or closed by something like a firewall. In fact, many IT professionals use Nmap to check their work when programming firewalls. They can see if their policies are having the desired effect, and if their firewalls are working properly.

Shadow IT Hunting: Because Nmap discovers the type and location of devices on a network, it can be used to identity things that should not be there at all. These devices are called shadow IT because their presence on a network isn't officially authorized, or sometimes may be intentionally hidden. Shadow IT can be dangerous because such devices are not part of a security audit or program. For example, if someone secretly places an Xbox game server on a corporate network, not only will that potentially drain bandwidth, but could act as a springboard for an attack, especially if it's not maintained with all the latest security patches.

Operating System Detection: Nmap can discover the types of operating systems running on discovered devices in a process called OS fingerprinting. This generally returns information about the name of the vendor of the device (Dell, HP, etc.) and the operating system. With a deeper Nmap scan, you can even discover things like the patch level of the OS and the estimated uptime of the device.

Service Discovery: The ability to discover services elevates Nmap above the level of a common mapping tool. Instead of simply discovering that a device exists, users can trigger a deeper scan in order to find out what roles discovered devices are performing. This includes identifying if they are acting as mail server, a web server, a database repository, a storage device or almost anything else. Depending on the scan, Nmap can also report on which specific applications are running, and what version of those applications are being used.

Vulnerability Scanning: Nmap is not a dedicated vulnerability scanning tool in that it does not maintain a database of known vulnerabilities or any kind of artificial intelligence that could identify potential threats. However, organizations that regularly ingest security information from threat feeds or other sources can use Nmap to check their susceptibility to specific threats.

For example, if a newly uncovered vulnerability only affects a certain application or service running an older version of the software, Nmap can be used to check to see if any programs currently operating on network assets meet those conditions. If anything is found, then presumably IT teams could prioritize getting those systems patched as quickly as possible to eliminate the vulnerability before an attacker could discover the same thing.

What is the future of Nmap?

Although the Nmap tool is 25 years old, it continues to evolve. Like other seemingly ancient technologies such as Ethernet or Spanning Tree, it is well maintained by an active community of experts that keep it relevant and up to date. And in the case of Nmap, that community includes its very active creator, who still goes by his Fyodor guise online.

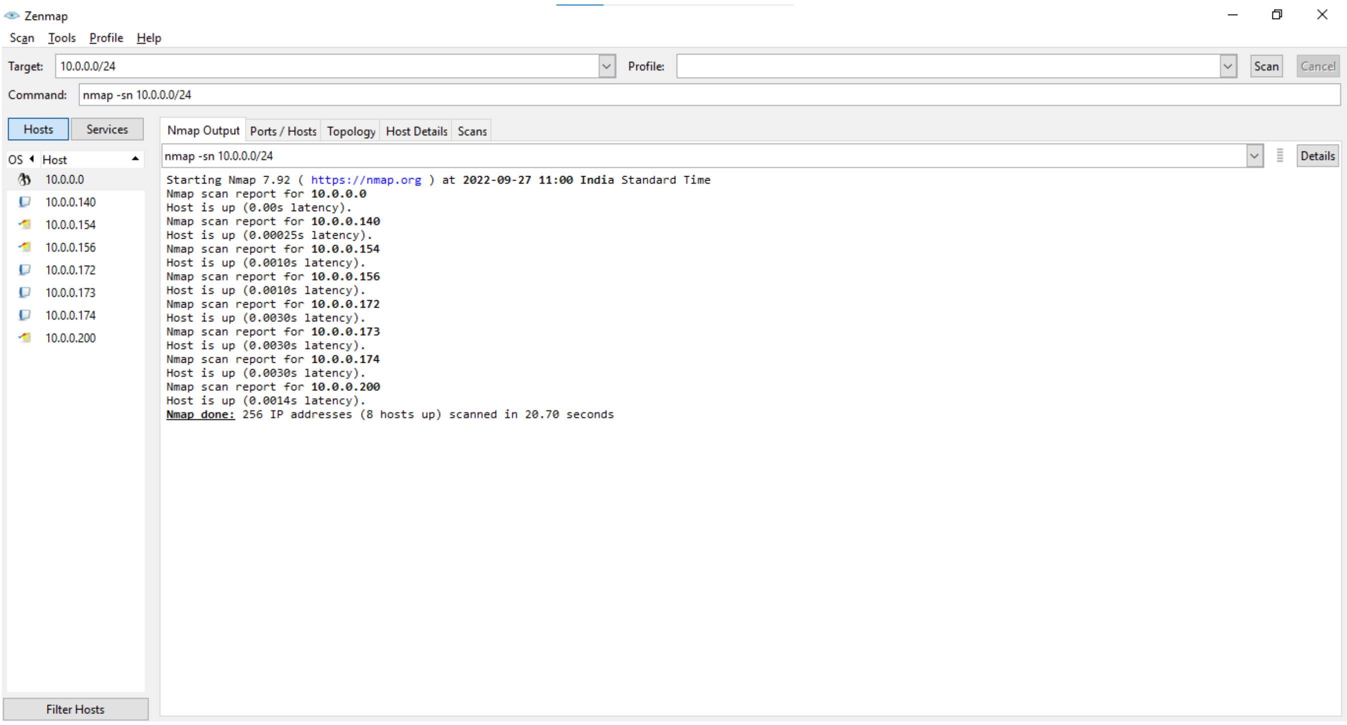
Other advancements like the new Zenmap tool make it even more useful, especially for those who don’t like working with console or command lines. The graphical interface for Zenmap allows users to quickly set up targets and configure desired scans with just a few clicks. That will help Nmap find an even bigger user base.

And finally, while there are many other tools these days that can perform similar functions, none of them have the proven track record of Nmap. Not only that, but Nmap has always been completely free and ready to download. Because of all of these factors, it’s almost a sure thing that Nmap will be just as useful and relevant over the next 25 years as it has been for past quarter century.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

RESULTS:

1. **Ping scan:**
   Scans the list of devices up and running on a given subnet.
   nmap -sP 10.0.0.0/24



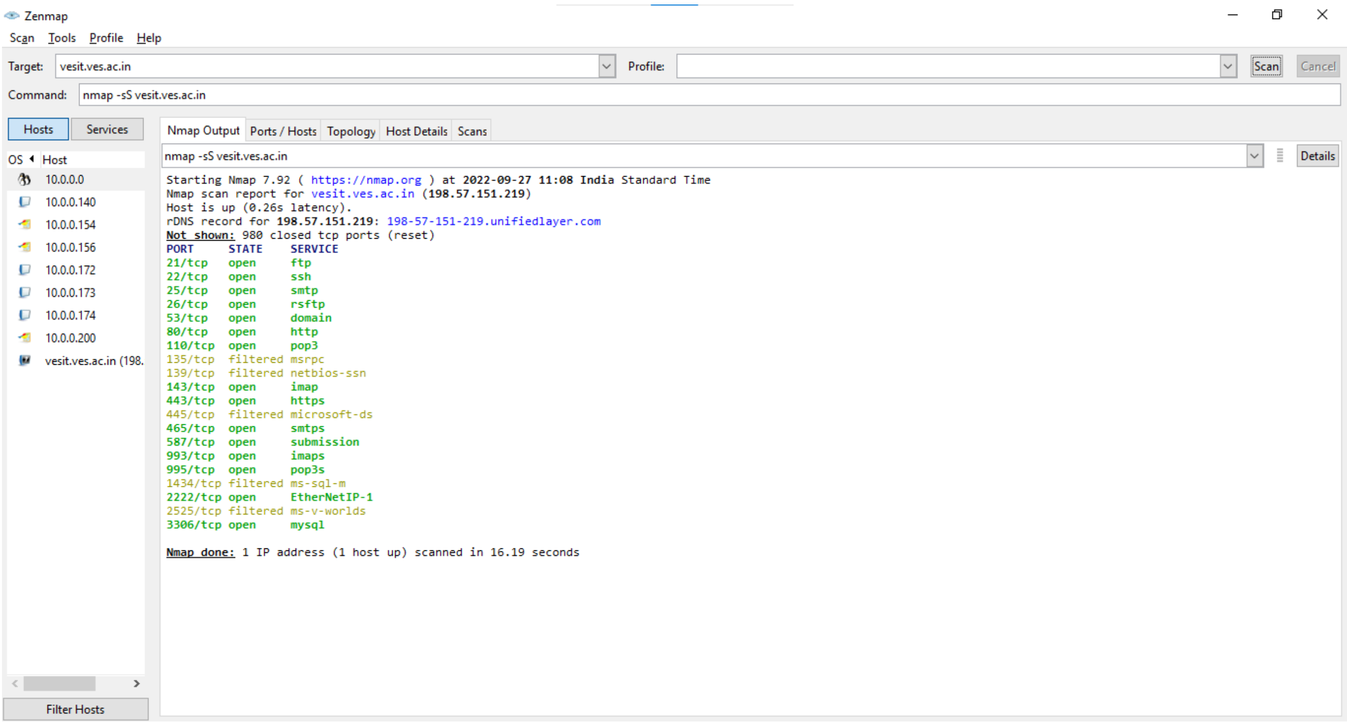
Target: 10.0.0.0/24

Command: nmap -sn 10.0.0.0/24

```
10.0.0.0
10.0.0.140
10.0.0.154
10.0.0.156
10.0.0.172
10.0.0.173
10.0.0.174
10.0.0.200
```

```
nmap -sn 10.0.0.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 11:00 India Standard Time
Nmap scan report for 10.0.0.0
Host is up (0.00s latency).
Nmap scan report for 10.0.0.140
Host is up (0.00025s latency).
Nmap scan report for 10.0.0.154
Host is up (0.0010s latency).
Nmap scan report for 10.0.0.156
Host is up (0.0010s latency).
Nmap scan report for 10.0.0.172
Host is up (0.0030s latency).
Nmap scan report for 10.0.0.173
Host is up (0.0030s latency).
Nmap scan report for 10.0.0.174
Host is up (0.0030s latency).
Nmap scan report for 10.0.0.200
Host is up (0.0014s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 20.70 seconds
```

2. **Stealth Scan**:
   Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.
   nmap -sS vesit.ves.ac.in



Target: vesit.ves.ac.in

Command: nmap -sS vesit.ves.ac.in

```
10.0.0.0
10.0.0.140
10.0.0.154
10.0.0.156
10.0.0.172
10.0.0.173
10.0.0.174
10.0.0.200
vesit.ves.ac.in (198.
```

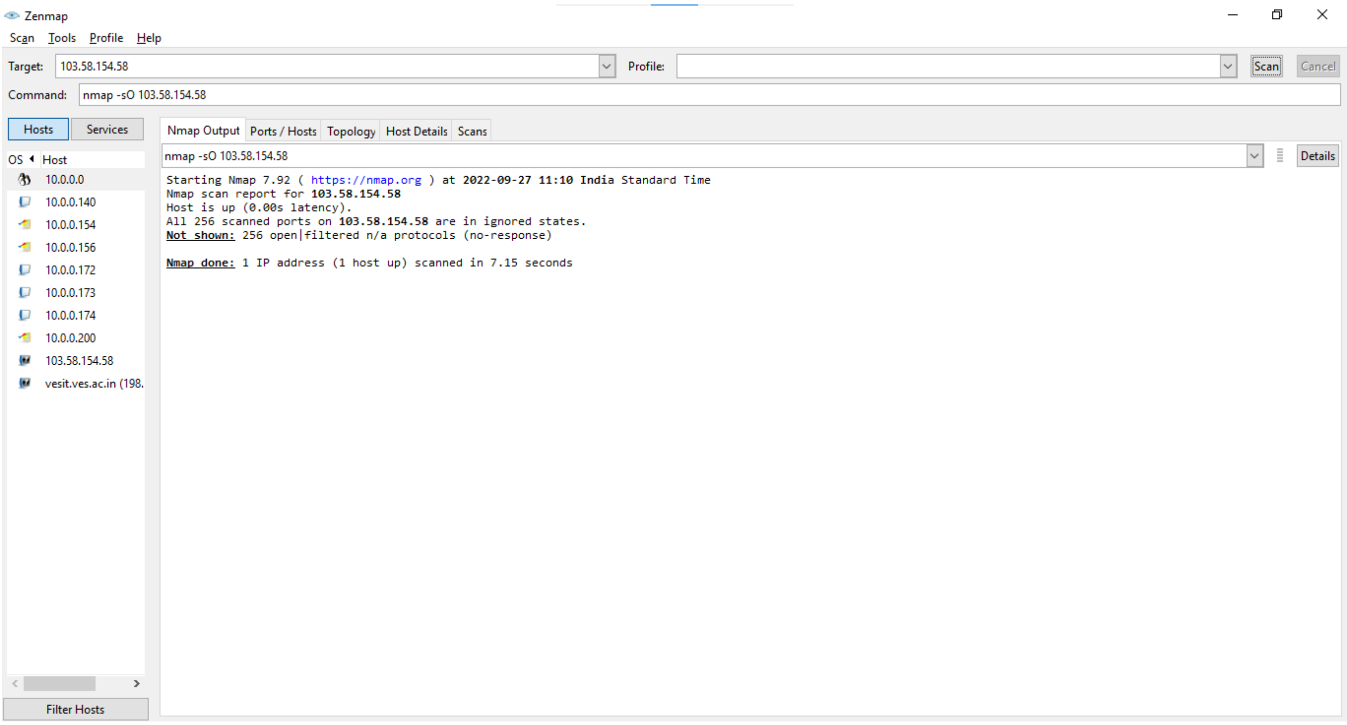
```
nmap -sS vesit.ves.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 11:08 India Standard Time
Nmap scan report for vesit.ves.ac.in (198.57.151.219)
Host is up (0.26s latency).
rDNS record for 198.57.151.219: 198-57-151-219.unifiedlayer.com
Not shown: 980 closed tcp ports (reset)
PORT     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
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
1434/tcp filtered ms-sql-m
2222/tcp open     EtherNetIP-1
2525/tcp filtered ms-v-worlds
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 16.19 seconds
```

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

3. IP Protocol Scan:

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines.

nmap -sO 103.58.154.58



Target: 103.58.154.58

Profile:

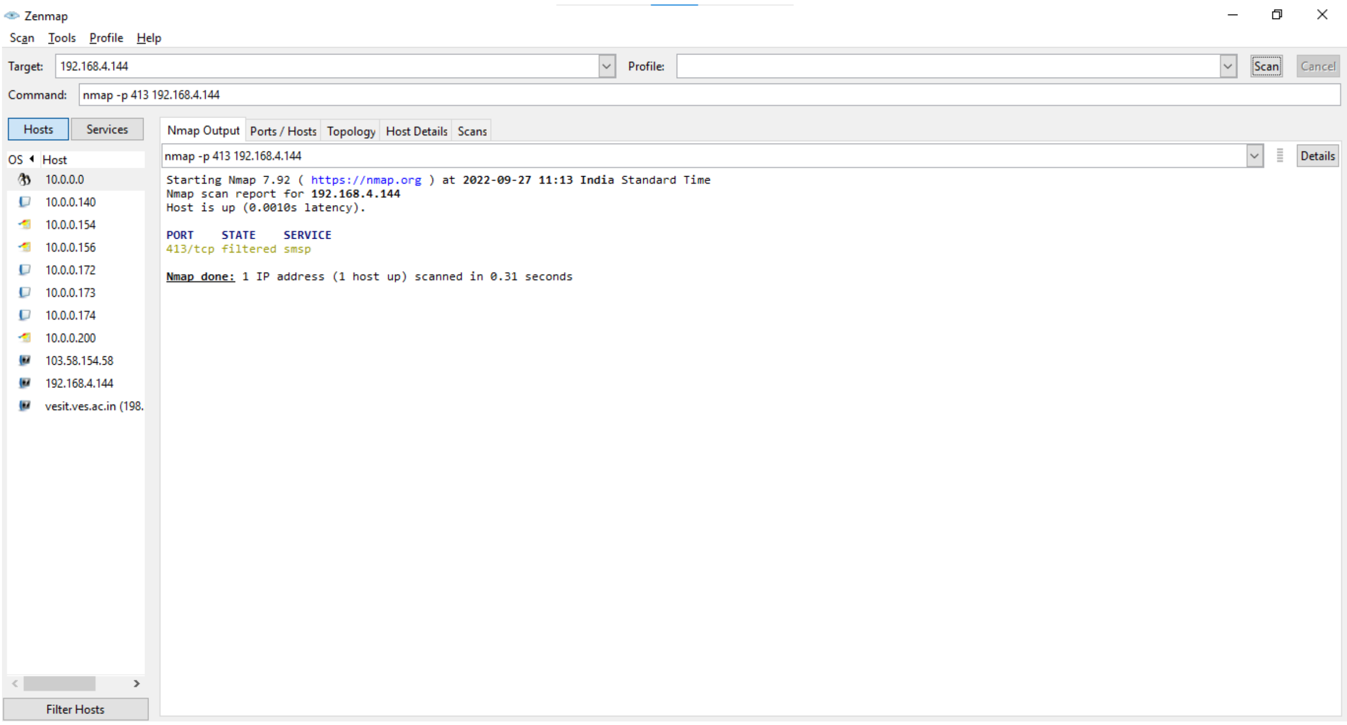
Command: nmap -sO 103.58.154.58

```
nmap -sO 103.58.154.58
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 11:10 India Standard Time
Nmap scan report for 103.58.154.58
Host is up (0.00s latency).
All 256 scanned ports on 103.58.154.58 are in ignored states.
Not shown: 256 open|filtered n/a protocols (no-response)

Nmap done: 1 IP address (1 host up) scanned in 7.15 seconds
```

4. Port Scanning:

Port scanning is one of the most fundamental features of Nmap. You can scan for ports in several ways.

nmap -p 413 192.168.4.144



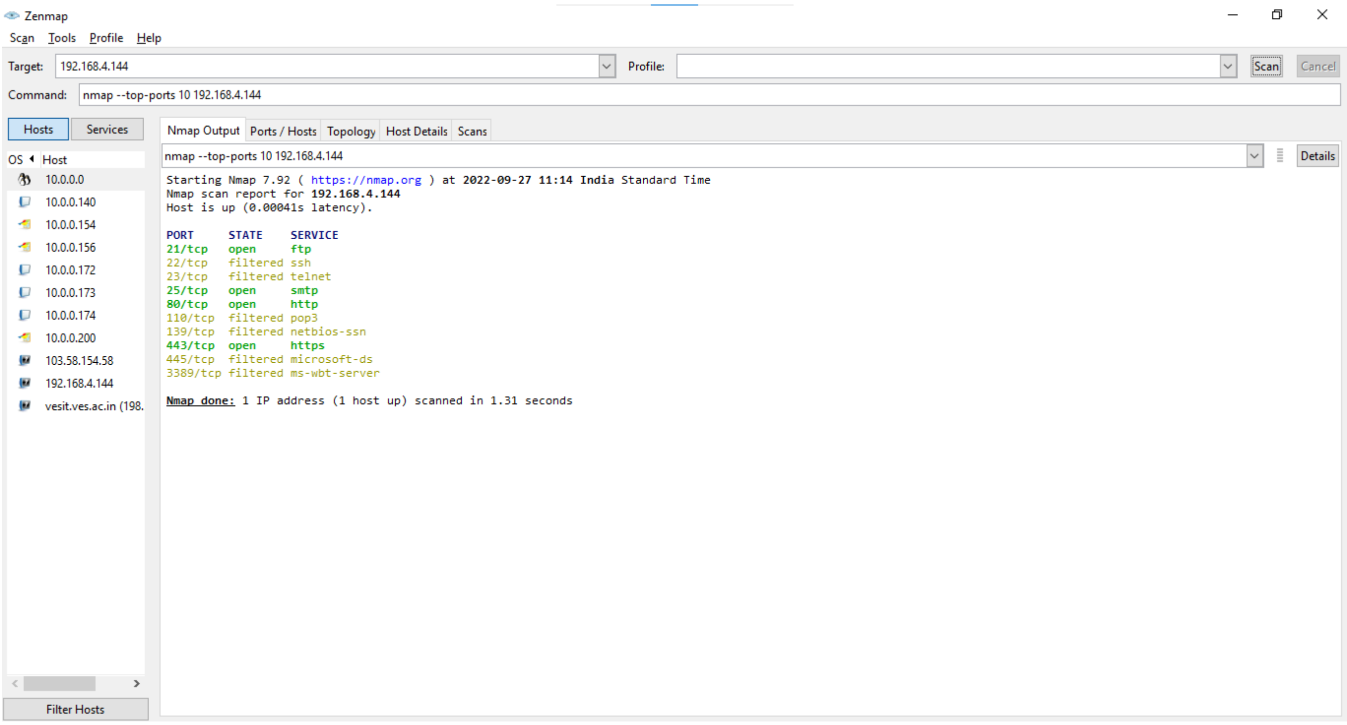
Target: 192.168.4.144

Profile:

Command: nmap -p 413 192.168.4.144

```
nmap -p 413 192.168.4.144
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 11:13 India Standard Time
Nmap scan report for 192.168.4.144
Host is up (0.0010s latency).

PORT    STATE    SERVICE
413/tcp filtered smsp

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

5. **Scan top ports:**
   The –top-ports option lets you specify the number of ports you wish to scan in each protocol, and will pick the most popular ports for you based on the new frequency data. For both TCP and UDP, the top 10 ports get you roughly half of the open ports.
   nmap –top-ports 10 192.168.4.144

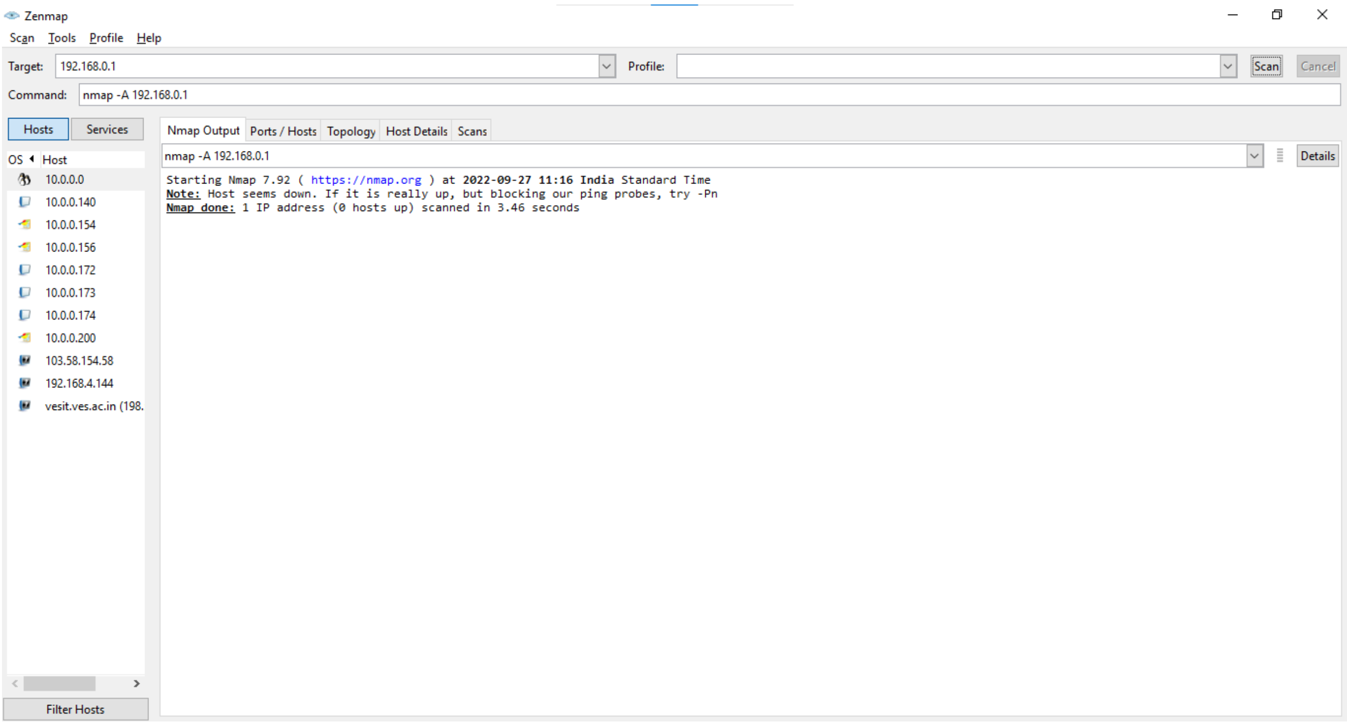


Target: 192.168.4.144

Command: nmap --top-ports 10 192.168.4.144

```
nmap --top-ports 10 192.168.4.144
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 11:14 India Standard Time
Nmap scan report for 192.168.4.144
Host is up (0.00041s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   open     smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

6. **Aggressive Scanning:**
   Nmap has an aggressive mode that enables OS detection, version detection, script scanning, and traceroute. You can use the -A argument to perform an aggressive scan.
   nmap -A 192.168.0.1



Target: 192.168.0.1

Command: nmap -A 192.168.0.1

```
nmap -A 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 11:16 India Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.46 seconds
```

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

CONCLUSION:

Thus, we successfully installed Zenmap, understood its functionalities, and executed several commands.