

ASSIGNMENT - 2

K. Naveen Abhiram

21BCE7357

NMAP TOOL IN KALI LINUX

NMAP

A potent open-source network scanning tool for network discovery and security audits is called Nmap (Network Mapper). It is frequently included in Kali Linux, and security experts, network administrators, and ethical hackers all utilize it extensively. You may investigate networks with Nmap and find hosts, services, vulnerabilities, and more.

Command Commands:

- -p: Specifies ports or port ranges to scan.
- -A: Enables OS detection, version detection, and script scanning.
- -oN: Saves output to a file.
- -sV: Attempts to determine the version of services running on open ports.
- -v: Increases verbosity for more detailed output.

Simple Scan:

- nmap vitap.ac.in

```
(kali@kali)~[~]
$ nmap vitap.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 23:02 IST
Nmap scan report for vitap.ac.in (5.9.36.52)
Host is up (0.0000030s latency).
Other addresses for vitap.ac.in (not scanned): 64:ff9b::509:2434
rDNS record for 5.9.36.52: static.52.36.9.5.clients.your-server.de
Not shown: 502 filtered tcp ports (net-unreach), 486 filtered tcp ports (no-r
esponse)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8443/tcp   closed https-alt
Nmap done: 1 IP address (1 host up) scanned in 37.61 seconds
```

- nmap 5.9.36.52

```
(kali@kali)-[~]
$ nmap 5.9.36.52
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 23:04 IST
Nmap scan report for static.52.36.9.5.clients.your-server.de (5.9.36.52)
Host is up (0.0000030s latency).
Not shown: 781 filtered tcp ports (no-response), 205 filtered tcp ports (net-unreach)
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8443/tcp  closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 37.32 seconds
```

Scan Specific Ports:

- nmap -p 20,22 5.9.36.52

```
(kali@kali)-[~]
$ nmap -p 20,22 5.9.36.52
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 23:05 IST
Nmap scan report for static.52.36.9.5.clients.your-server.de (5.9.36.52)
Host is up (0.20s latency).
PORT      STATE SERVICE
20/tcp    closed ftp-data
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Detect OS and Service Versions:

- nmap -A 5.9.36.52

```
(kali@kali)-[~]
$ nmap -A 5.9.36.52
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 23:06 IST
Nmap scan report for static.52.36.9.5.clients.your-server.de (5.9.36.52)
Host is up (0.000016s latency).
Not shown: 559 filtered tcp ports (no-response), 428 filtered tcp ports (net-unreach)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  tcpwrapped
22/tcp    open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
25/tcp    open  tcpwrapped
|_smtp_commands: Couldn't establish connection on port 25
53/tcp    open  tcpwrapped
80/tcp    open  tcpwrapped
110/tcp   open  tcpwrapped
143/tcp   open  tcpwrapped
443/tcp   open  tcpwrapped
587/tcp   open  tcpwrapped
|_smtp_commands: Couldn't establish connection on port 587
993/tcp   open  tcpwrapped
995/tcp   open  tcpwrapped
8443/tcp  closed https-alt

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.40 seconds
```

Scan All Ports:

- nmap -p- 5.9.36.52

```
(kali@kali)-[~]
$ nmap -p- 5.9.36.52
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 23:07 IST
Nmap scan report for static.52.36.9.5.clients.your-server.de (5.9.36.52)
Host is up (0.0000020s latency).
Not shown: 64948 filtered tcp ports (net-unreach), 576 filtered tcp ports (no
-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 40.53 seconds
```

Scan UDP Ports:

- `nmap -sU 5.9.36.52`

Save Output to a File:

- `nmap -oN results.txt 5.9.36.52`

Nmap offers a wide range of additional capabilities and options, such as the scripting engine (NSE) enabling unique scanning and sophisticated scripting. Nmap can be intrusive and may cause service disruptions, so use it responsibly and only on networks and systems you are permitted to scan. Always conduct network scanning in accordance with the law and ethical principles.