

**Experiment No. 3**  
**Title: Active Reconnaissance**

Batch:SY-IT(B3)

Roll No.:16010423076

Experiment No.: 3

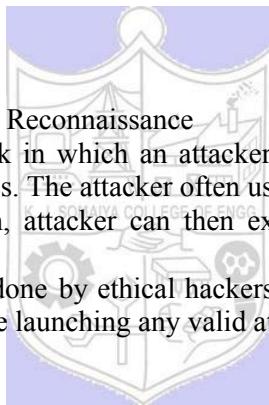
**Aim: To understand and perform Active Reconnaissance with tools****Resources needed:** Internet access**Theory:**

Reconnaissance is the act of collecting information. It can be said as act of military observation of a region to locate an enemy or ascertain strategic features.

In Cyber Security, Reconnaissance (or recon. In short) refers to act of collecting information about the target system and looking for weaknesses to exploit

There are 2 types of Recon,

- Active Recon
- Passive Recon



Today, we will only discuss about Active Reconnaissance

Active Recon is a type of attack in which an attacker engages with the target system to gather information about possible vulnerabilities. The attacker often uses port scanning, for example, to discover any vulnerable ports. After a port scan, attacker can then exploit the known vulnerabilities of those services associated with open ports

Active Reconnaissance is also done by ethical hackers as it is also necessary for a pen tester to understand and observe the system before launching any valid attack.

Let's look at tools to perform the attack

- nmap
- netcat (nc)

**NMAP**

The Network Mapper is a network scanner created by Gordon Lyon. It is an open source tool used for network discovery and auditing. The tool searches for directories and services in a network by sending packets and analyzing their responses.

Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules and monitoring host or service uptime.

Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what OS (and their versions) they are running, what type of packet filters/firewalls are in use and dozens of other characteristics

It was primarily designed to scan large networks, but works well against single hosts. Nmap runs on all major computer operating systems and official binary packages are available for linux, Windows and MacOS X.

**Characteristics of NMAP:****-Flexible**

Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers and other obstacles (includes port scanning w/ TCP and UDP, OS detection, version detection, ping sweeps and more).

**-Powerful**

Allows you to scan large networks

**-Portable**

Open source software that can be used on Most Oss

-Easy

Even though it provides a wide range of features, beginners can start with simply nmap -v -A  
<target\_hostname\_or\_IPAddress>

-Free

Primary goal being to make internet a safer place, giving admins, auditors and hackers a tool to assess the network. It is free to download and opensourced.

-Well Documented

A lot of effort has been put in the whitepapers, tutorials, up to date manual pages, etc

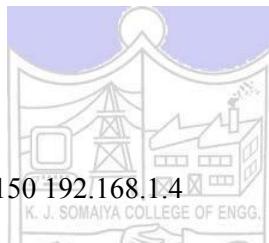
## Procedure

### Working with NMAP

#### 1) Nmap 1

##### 1. Vulners Script

```
nmap --script vulners -sV -p 21-150 192.168.1.4
```



```
rishi@vbox:~$ nmap --script vulners -sV -p 21-150 192.168.1.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-02-03 22:00 IST
Nmap scan report for 192.168.1.4
Host is up (0.0000s latency).
Not shown: 122 closed TCP ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ssh      OpenSSH 4.1.1p2 Debian Subuntu (protocol 2.0)
| vulners:
|_ vsftpd 2.3.4:
  PACKETSTORM:162149 10.0 https://vulners.com/packetstorm/PACKETSTORM:162149      *EXPLOIT*
  ZC119F9A-ECE0-5E14-AAA4-354A2C38071A 10.0 https://vulners.com/githubexploit/C119F9A-ECE0-5E14-AAA4-354A2C38071A      *EXPLOIT*
  CVE-2011-2523 9.8 https://vulners.com/cve/CVE-2011-2523      *EXPLOIT*
  137DAY-ID-36095 9.8 https://vulners.com/zdt/137DAY-ID-36095      *EXPLOIT*
22/tcp    open  ssh      OpenSSH 4.1.1p2 Debian Subuntu (protocol 2.0)
| vulners:
|_ vsftpd 2.3.4:
  PACKETSTORM:162149 10.0 https://vulners.com/packetstorm/PACKETSTORM:162149      *EXPLOIT*
  ZC119F9A-ECE0-5E14-AAA4-354A2C38071A 10.0 https://vulners.com/githubexploit/C119F9A-ECE0-5E14-AAA4-354A2C38071A      *EXPLOIT*
  CVE-2011-2523 9.8 https://vulners.com/cve/CVE-2011-2523      *EXPLOIT*
  B8190CDB-3EB9-5631-928B-0864A175B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-928B-0864A175B23      *EXPLOIT*
  BFC9C34B-3968-5F3C-B25E-E0B05379A623 9.8 https://vulners.com/githubexploit/BFC9C34B-3968-5F3C-B25E-E0B05379A623      *EXPLOIT*
  B87E8570-7D03-11EE-AD8A-C80A09A93978 9.8 https://vulners.com/githubexploit/B87E8570-7D03-11EE-AD8A-C80A09A93978      *EXPLOIT*
  5E69688A-0B06-57FA-BF6E-09B2219B027A 9.8 https://vulners.com/githubexploit/5E69688A-0B06-57FA-BF6E-09B2219B027A      *EXPLOIT*
  33D623F7-98E0-5F79-BF8A-8103E601340 9.8 https://vulners.com/githubexploit/33D623F7-98E0-5F79-BF8A-8103E601340      *EXPLOIT*
  023E8A89-8480-5370-92D0-809E6601597 9.8 https://vulners.com/githubexploit/023E8A89-8480-5370-92D0-809E6601597      *EXPLOIT*
  CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600      *EXPLOIT*
  5B74A5BC-348F-11E5-BA05-C80A09A93978 8.5 https://vulners.com/githubexploit/5B74A5BC-348F-11E5-BA05-C80A09A93978      *EXPLOIT*
  FBF35DE1-404C-558C-A107-00602883514 8.1 https://vulners.com/githubexploit/FBF35DE1-404C-558C-A107-00602883514      *EXPLOIT*
  FA3992CE-9CAC-5358-8134-1771266E8B03F 8.1 https://vulners.com/githubexploit/FA3992CE-9CAC-5358-8134-1771266E8B03F      *EXPLOIT*
  F9891437-1287-5B69-93F1-657D0B1DCE59 8.1 https://vulners.com/githubexploit/F9891437-1287-5B69-93F1-657D0B1DCE59      *EXPLOIT*
  F50308E9-4080-5B80-9000-000000000000 8.1 https://vulners.com/githubexploit/F50308E9-4080-5B80-9000-000000000000      *EXPLOIT*
  F1A0012-2-1797-1-1EF-B611-8A493BAE975 8.1 https://vulners.com/githubexploit/F1A0012-2-1797-1-1EF-B611-8A493BAE975      *EXPLOIT*
  EFD615F8-BF17-5471-A483-0F491FD497AF 8.1 https://vulners.com/githubexploit/EFD615F8-BF17-5471-A483-0F491FD497AF      *EXPLOIT*
  EC2089C2-B857-5848-B48A-AFF43013EEB 8.1 https://vulners.com/githubexploit/EC2089C2-B857-5848-B48A-AFF43013EEB      *EXPLOIT*
  E64061A8-1-1E7-5F23-1-1E7-5F23 8.1 https://vulners.com/githubexploit/E64061A8-1-1E7-5F23-1-1E7-5F23      *EXPLOIT*
  E543E274-C20A-582A-8F8E-F8E3F3B1C345 8.1 https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F3B1C345      *EXPLOIT*
  E34FCCEC-2261-5446-981C-BCD6E703257 8.1 https://vulners.com/githubexploit/E34FCCEC-2261-5446-981C-BCD6E703257      *EXPLOIT*
  E34FCCEC-2261-5446-981C-BCD6E703257 8.1 https://vulners.com/githubexploit/E34FCCEC-2261-5446-981C-BCD6E703257      *EXPLOIT*
  DC79BE9B-8A77-5F86-9C16-0CFCD504E0BB 8.1 https://vulners.com/githubexploit/DC79BE9B-8A77-5F86-9C16-0CFCD504E0BB      *EXPLOIT*
  DC473880-F54C-BF76-B8F0-0175E400C1D 8.1 https://vulners.com/githubexploit/DC473880-F54C-BF76-B8F0-0175E400C1D      *EXPLOIT*
  D053F88ED-BD9E-5E99-B8D2-227880BF36B 8.1 https://vulners.com/githubexploit/D053F88ED-BD9E-5E99-B8D2-227880BF36B      *EXPLOIT*
  D53F88ED-BD9E-5E99-B8D2-227880BF36B 8.1 https://vulners.com/githubexploit/D53F88ED-BD9E-5E99-B8D2-227880BF36B      *EXPLOIT*
  D1E049F1-9392-5520-8001-67902826911 8.1 https://vulners.com/githubexploit/D1E049F1-9392-5520-8001-67902826911      *EXPLOIT*
  CFBF7AF-651A-5302-8088-F814605B33A6 8.1 https://vulners.com/githubexploit/CFBF7AF-651A-5302-8088-F814605B33A6      *EXPLOIT*
  CF880D04-2E7-5E06-80A8-84C72658E191 8.1 https://vulners.com/githubexploit/CF880D04-2E7-5E06-80A8-84C72658E191      *EXPLOIT*
  CB292E61-2355-5C82-A42A-04F72F14F9B 8.1 https://vulners.com/githubexploit/CB292E61-2355-5C82-A42A-04F72F14F9B      *EXPLOIT*
```



```

rakesh@vbox: ~
File Actions Edit View Help
| SSV:1158 4.3 https://vulners.com/sebug/SSV:1158 *EXPLOIT*
| PACKETSTORM:109284 4.3 https://vulners.com/packetstorm/PACKETSTORM:109284 *EXPLOIT+
| EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE 4.3 https://vulners.com/exploitdb/EDB-ID:35738 *EXPLOIT*
EDB-ID:35738 4.3 https://vulners.com/exploitdb/EDB-ID:35738 *EXPLOIT*
CVE-2013-2525 4.3 https://vulners.com/cve/CVE-2013-2525
CVE-2014-8118 4.3 https://vulners.com/cve/CVE-2014-8118
CVE-2013-1896 4.3 https://vulners.com/cve/CVE-2013-1896
CVE-2012-4558 4.3 https://vulners.com/cve/CVE-2012-4558
CVE-2012-0059 4.3 https://vulners.com/cve/CVE-2012-0059
CVE-2012-0053 4.3 https://vulners.com/cve/CVE-2012-0053
CVE-2011-4317 4.3 https://vulners.com/cve/CVE-2011-4317
CVE-2011-0639 4.3 https://vulners.com/cve/CVE-2011-0639
CVE-2010-1849 4.3 https://vulners.com/cve/CVE-2010-1849
CVE-2010-0434 4.3 https://vulners.com/cve/CVE-2010-0434
CVE-2009-0023 4.3 https://vulners.com/cve/CVE-2009-0023
CVE-2008-2393 4.3 https://vulners.com/cve/CVE-2008-2393
CVE-2007-2055 4.3 https://vulners.com/cve/CVE-2007-2055
CVE-2007-6420 4.3 https://vulners.com/cve/CVE-2007-6420
SSV:1262 2.4 https://vulners.com/sebug/SSV:1262 *EXPLOIT*
CVE-2007-2687 2.4 https://vulners.com/cve/CVE-2007-2687
CVE-2009-3894 2.6 https://vulners.com/cve/CVE-2009-3894
CVE-2008-0456 2.6 https://vulners.com/cve/CVE-2008-0456
SSV:60250 1.2 https://vulners.com/sebug/SSV:60250 *EXPLOIT*
CVE-2008-1415 1.2 https://vulners.com/cve/CVE-2008-1415
137DAY-ID-9602 0.0 https://vulners.com/zdt/137DAY-ID-9602 *EXPLOIT*
137DAY-ID-21346 0.0 https://vulners.com/zdt/137DAY-ID-21346 *EXPLOIT*
137DAY-ID-17257 0.0 https://vulners.com/zdt/137DAY-ID-17257 *EXPLOIT*
137DAY-ID-13263 0.0 https://vulners.com/zdt/137DAY-ID-13263 *EXPLOIT*
137DAY-ID-13268 0.0 https://vulners.com/zdt/137DAY-ID-13268 *EXPLOIT*
137DAY-ID-11185 0.0 https://vulners.com/zdt/137DAY-ID-11185 *EXPLOIT*
111/tcp open rpcbind 2 (RPC #100000)
  Fingerprint:
    program version port/proto service
    100000 2           111/tcp  rpcbind
    100000 2           10000/tcp rpcbind
    100000 3,4         2049/udp nfs
    100003 2,3,4       34607/tcp mountd
    100005 1,2,3       51602/tcp modrd
    100021 1,2,3       65132/udp lockmgr
    100021 1,3,4       51602/tcp lockmgr
    100021 1           4478/tcp status
    100024 1           4500/tcp nis
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
(rakesh@vbox) [~]
$ 

```

## 2. HTTP Enum Script

```
nmap --script http-enum -sV -p 80 192.168.1.4
```



```

rakesh@vbox: ~
File Actions Edit View Help
| (rakesh@vbox) [~]
|   nmap --script http-enum -sV -p 80 192.168.1.4
Starting Nmap 7.7.0 ( https://nmap.org ) at 2025-02-03 22:04 IST
Nmap scan report for 192.168.1.1
Host is up (0.018s latency).

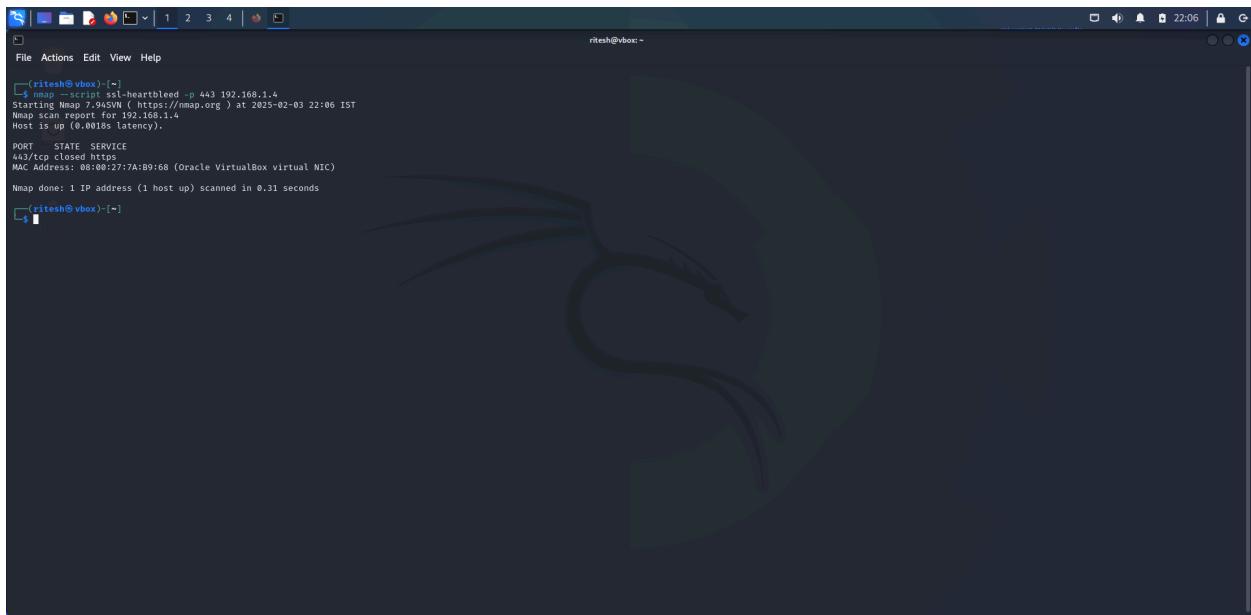
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-enum:
|_ /test/: Test page
|_ /phpinfo.php: Possible information file
|_ /phpMyAdmin/: phpMyAdmin
|_ /icons/: Potentially interesting directory w/ listing on 'apache/2.1.8 (ubuntu) dav/2'
|_ /index/: Potentially interesting folder
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.33 seconds
(rakesh@vbox) [~]
$ 

```

## 3. Heartbleed Script

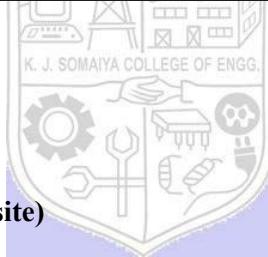
```
nmap --script ssl-heartbleed -p 443 192.168.1.4
```



```
(ritesh@vbox) [~]
$ nmap -script ssl-heartbleed -p 443 192.168.1.4
Starting Nmap 7.94SWM ( https://nmap.org ) at 2025-02-03 22:06 IST
Nmap scan report for 192.168.1.4
Host is up (0.0001s latency).

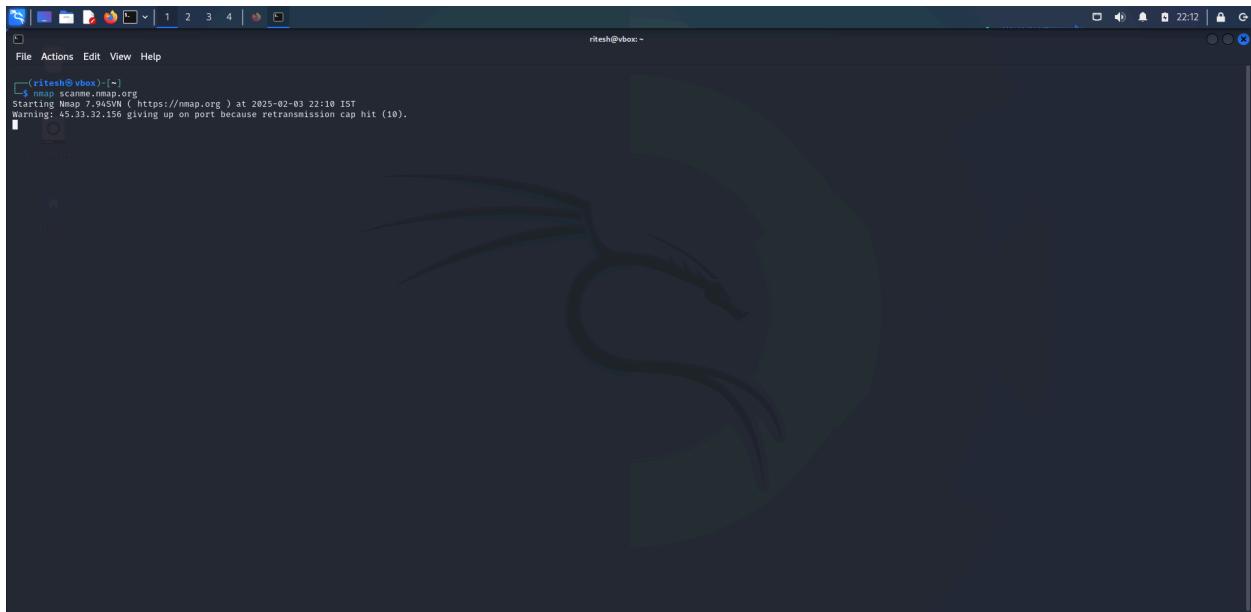
PORT      STATE SERVICE
443/TCP   closed https
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
(ritesh@vbox) [~]
```



## 2) Nmap 2

# 1. Basic Nmap scan (targeting a website)  
nmap scanme.nmap.org



```
(ritesh@vbox) [~]
$ nmap scanme.nmap.org
Starting Nmap 7.94SWM ( https://nmap.org ) at 2025-02-03 22:10 IST
Warning: 45.33.32.159 giving up on port because retransmission cap hit (10).

(ritesh@vbox) [~]
```

# 2. Gathering IP Addresses  
nmap 192.168.1.4



```
(ritesh@vbox) ~]
$ nmap 192.168.1.4
Starting Nmap 7.94SWM ( https://nmap.org ) at 2025-02-03 22:13 IST
Nmap scan report for 192.168.1.4
Host is up (0.0002s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7A:B9:88 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
[ritesh@vbox] ~]
```

nmap 192.168.1.0-255



```
(ritesh@vbox) ~]
$ nmap 192.168.1.0-255
Starting Nmap 7.94SWM ( https://nmap.org ) at 2025-02-03 22:13 IST
Nmap scan report for 192.168.1.1
Host is up (0.00076s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.1.2
Host is up (0.0016s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.1.3
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:06:fc:a9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.4
Host is up (0.0002s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

```

nmap 192.168.1.0/24

```
(ritesh@vbox) ~]$ nmap 192.168.1.0/24
Starting Nmap 7.94SWM ( https://nmap.org ) at 2025-02-03 22:14 IST
Nmap scan report for 192.168.1.1 (192.168.1.1)
Host is up (0.000005s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.1.2
Host is up (0.000005s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:D0:FC:A9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.3
Host is up (0.00003s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D0:FC:A9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.4
Host is up (0.00001s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  netbios-ns
139/tcp   open  netbios-smb
445/tcp   open  microsoft-ds
512/tcp   open  exec
535/tcp   open  logon
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2000/tcp  open  ircd
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8080/tcp  open  apache2
8180/tcp  open  unknown
```

```
(ritesh@vbox) ~]$ nmap 192.168.1.0/24
Starting Nmap 7.94SWM ( https://nmap.org ) at 2025-02-03 22:14 IST
Nmap scan report for 192.168.1.2 (192.168.1.2)
Host is up (0.000005s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

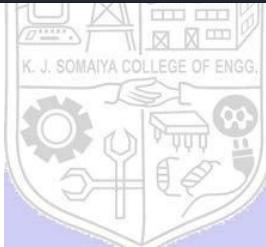
Nmap scan report for 192.168.1.3
Host is up (0.00001s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D0:FC:A9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.4
Host is up (0.00001s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  netbios-ns
139/tcp   open  netbios-smb
445/tcp   open  microsoft-ds
512/tcp   open  exec
535/tcp   open  logon
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2000/tcp  open  ircd
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8080/tcp  open  apache2
8180/tcp  open  unknown

Nmap done: 256 IP addresses (5 hosts up) scanned in 12.96 seconds
```

nmap google.com

```
(ritesh@vbox) [~]
$ nmap google.com
Starting Nmap 7.94 ( https://nmap.org ) at 2025-02-03 22:14 IST
Nmap scan report for google.com (142.250.192.46)
Host is up (0.0025s latency).
Other addresses for google.com (not scanned): 2004:6800:4009:828::200e
rDNS record for 142.250.192.46: b012s15-in-f14.1e100.net
Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
(ritesh@vbox) [~]
```



### # 3. Running Different Scan Types

# Ping Scan (detects which hosts are up)  
nmap -sn 192.168.1.4

```
(ritesh@vbox) [~]
$ nmap -sn 192.168.1.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-02-03 22:15 IST
Nmap scan report for 192.168.1.4
Host is up (0.023s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
(ritesh@vbox) [~]
```

# TCP Connect Scan (3-way handshake)  
nmap -sT 192.168.1.4



```
(ritesh@vbox) ~]
$ nmap -sT 192.168.1.4
Starting Nmap 7.94SWN ( https://nmap.org ) at 2025-02-03 22:16 IST
Nmap scan report for 192.168.1.4
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1899/tcp  open  windows-registry
1924/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  proxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
(ritesh@vbox) ~]
```

# SYN Scan (stealth scan)  
 sudo nmap -sS 192.168.1.4



```
(ritesh@vbox) ~]
$ sudo nmap -sS 192.168.1.4
[sudo] password for ritesh:
Starting Nmap 7.94SWN ( https://nmap.org ) at 2025-02-03 22:16 IST
Nmap scan report for 192.168.1.4
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1899/tcp  open  windows-registry
1924/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  proxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
(ritesh@vbox) ~]
```

# Service Version Detection  
 nmap -sV 192.168.1.4



```
(ritesh@vbox) ~]
$ nmap -sV 192.168.1.4
Starting Nmap 7.94SWN ( https://nmap.org ) at 2025-02-03 22:18 IST
Nmap scan report for 192.168.1.4
Host is up (0.041s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 4.7p1 Debian Bubuntul (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix/mtpd
37/tcp    open  domain  bind 9.3.4
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec   netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  raw-dump
1999/tcp  open  java-rmi GNU Classpath gmrregistry
1924/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
2121/tcp  open  ftp
3306/tcp  open  mysql  MySQL 5.0.51a-Subversive5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc    UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7A:B9:B8 (Oracle VirtualBox virtual NIC)
Service Info: Hostname: metasploitable.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.74 seconds
(ritesh@vbox) ~]
```

## # OS Detection

nmap -O 192.168.1.4



```
(ritesh@vbox) ~]
$ nmap -O 192.168.1.4
Starting Nmap 7.94SWN ( https://nmap.org ) at 2025-02-03 22:18 IST
Nmap scan report for 192.168.1.4
Host is up (0.044ms latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE OS
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1999/tcp  open  java-rmi
1924/tcp  open  bindshell
2049/tcp  open  nfs
2121/tcp  open  proxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7A:B9:B8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds
(ritesh@vbox) ~]
```

## # 4. Different Types of Port Scans

# Port Range Scan (scans specific range of ports)

nmap -p 1-100 192.168.1.4

```
(ritesh@vbox) ~]$ nmap -p 80 192.168.1.4
Starting Nmap 7.94SWN ( https://nmap.org ) at 2025-02-03 22:19 IST
Nmap scan report for 192.168.1.4
Host is up (0.016s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
(ritesh@vbox) ~]
```

# Specific Ports Scan (scans selected ports)

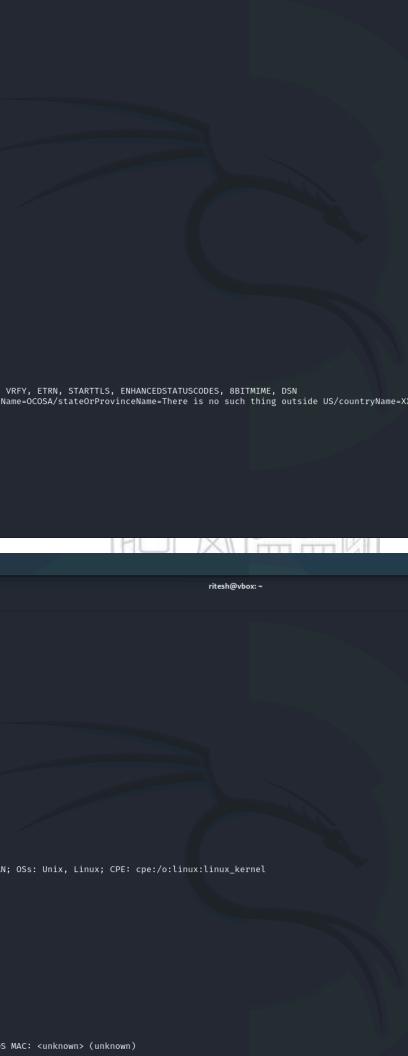
nmap -p 22,80,443 192.168.1.4

```
(ritesh@vbox) ~]$ nmap -p 22,80,443 192.168.1.4
Starting Nmap 7.94SWN ( https://nmap.org ) at 2025-02-03 22:19 IST
Nmap scan report for 192.168.1.4
Host is up (0.016s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  nntp
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  rsh
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6001/tcp  open  xdmcp
6007/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
3473/tcp  open  vnc-vz
3480/tcp  open  unknown
44770/tcp open  unknown
44894/tcp open  unknown
51603/tcp open  unknown
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.44 seconds
(ritesh@vbox) ~]
```

# All Ports Scan

nmap -p- 192.168.1.4



```
(ritesh@vbox)-[~]
$ nmap -A 192.168.1.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-02-03 22:20 IST
Nmap scan report for 192.168.1.4
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 4.7p1 Debian Bubuntui (protocol 2.0)
| ssh-keygen: RSA-2048 SHA256:ec1e:cb:5f:6a:74:d6:90:7a:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:62:24:0f:21:1d:de:a7:2b:a6:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
|_smtp-date: 2025-02-03T16:31:06+00:00; +7s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXTRACTRC4_WITH_MD5
|     SSL2_RC4_128_CBC_RC4_40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SMB-enum-share: Metasploitable.localdomain, PIPELINING, SIZE_10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_smb3-enum-sessions: [redacted] - Linux
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain  ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000 2          111/tcp  rpcbind
[...]
```

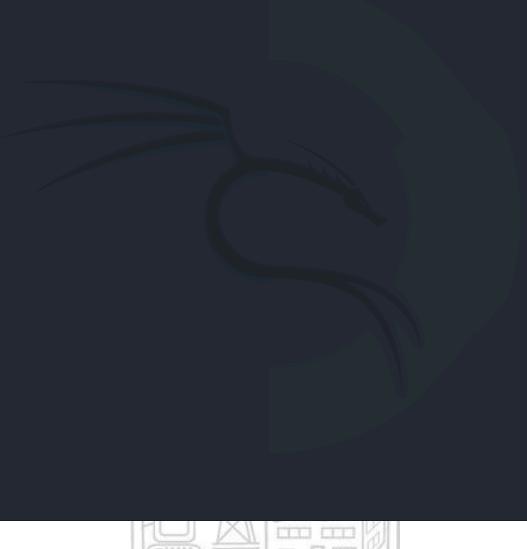
```
(ritesh@vbox)-[~]
File Actions Edit View Help
6667/tcp open  irc    UnrealIRCd
| ircd:
|   users: 1
|   servers: 1
|   users: 1
|   servers: 0
|   Server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1 irc.Metasploitable.LAN
|   uptime: 0 days, 0:13:7:35
|   source host: fc41889c.780ed367.ffffad09.ip
|   error: Closing Link: umzughvvcy[192.168.1.5] (Quit: uzmughvvcy)
8009/tcp open  http  Apache Jserv (Protocol v1.3)
|_http-error: 502 Bad Gateway. Failed to get a valid response for the OPTION request
8180/tcp open  http  Apache Tomcat/8.0.33
|_http-favicon: Apache Tomcat
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-server-software: Apache/2.4.41 (Ubuntu)
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.x
OS: CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account lock limit: 1000
|   authentication level: user
|   challenge-response: supported
|   message-signing: disabled (dangerous, but default)
| smb3-authentication:
|   OS: Unix (Samba 3.0.20-Debian)
|     Computer name: metasploitable
|     NetBIOS computer name: metasploitable
|     FQDN: metasploitable.localdomain
|   System time: 2025-02-03T11:50:58-05:00
|   clock-skew: mean: 1151ms, deviation: 1000ms, median: 55
|   SMB3 auth attempt failed (CMB2)
|_nbstat: NetBIOS name: METASPOILITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1  3.50 ms 192.168.1.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.79 seconds
```

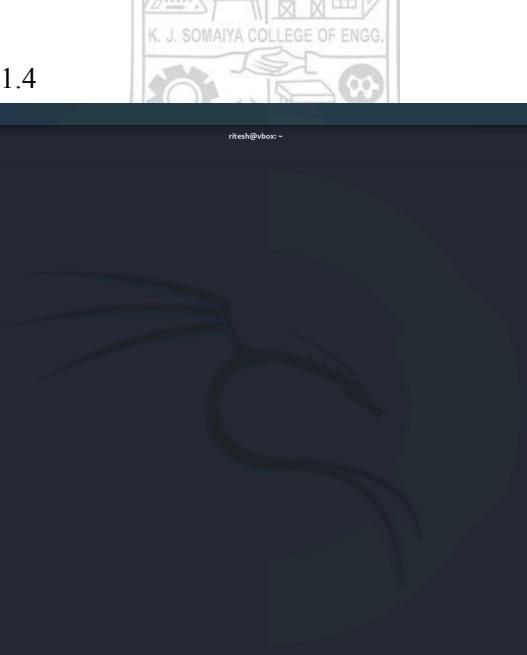
# Aggressive Scan (includes OS, version, and script scanning)  
nmap -A 192.168.1.4



```
(ritesh@vbox) ~]$ nmap --top-ports 100 192.168.1.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-02-03 22:21 IST
Nmap scan report for 192.168.1.4
Host is up (0.010ms latency).
Not shown: 82 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  vsftpd
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  cifs
2721/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5800/tcp  open  xdm
6800/tcp  open  x11
8009/tcp  open  ajp13
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
(ritesh@vbox) ~]$
```

# Top Ports Scan  
nmap --top-ports 100 192.168.1.4



```
(ritesh@vbox) ~]$ nmap --top-ports 100 192.168.1.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-02-03 22:21 IST
Nmap scan report for 192.168.1.4
Host is up (0.0077s latency).

PORT      STATE SERVICE
80/tcp    open  http
81/tcp    closed host2s-ns
82/tcp    closed kfree
83/tcp    closed net-ml-dev
84/tcp    closed ctf
85/tcp    closed net-ml-dev
86/tcp    closed mcobol
87/tcp    closed priv-term-l
88/tcp    closed kerberos-sec
89/tcp    closed su-mit-tg
90/tcp    closed mit-serv
91/tcp    closed mit-dov
92/tcp    closed npn
93/tcp    closed dixie
94/tcp    closed objcall
95/tcp    closed supdup
96/tcp    closed dixie
97/tcp    closed cryptof
98/tcp    closed linuxconf
99/tcp    closed metagram
100/tcp   closed newacct
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
(ritesh@vbox) ~]$
```

**# 5. Combining Different Scan and Port Scan Types**  
# SYN scan with specific port range  
nmap -sS -p 80-100 192.168.1.4

```
(ritesh@vbox) ~]
$ nmap -script vulners -sv -p 21-150 192.168.1.4
Starting Nmap 7.94SWM ( https://nmap.org ) at 2025-02-03 22:00 IST
Nmap scan report for 192.168.1.4
Host is up (0.00002s latency).
Not shown: 122 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 7.4.1p1 Debian (protocol 2.0)
vulners:
cpe:/o:openbsd:openbsd-4.7p1:
95PACKETST080M:162145 10.0 https://vulners.com/packetst080/162145 *EXPLOIT*
EDB-ID:49757 9.8 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
CVE-2011-2523 9.8 https://vulners.com/cve/CVE-2011-2523 *EXPLOIT*
1337DAY-ID-36095 9.8 https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
22/tcp open ssh      OpenSSH 7.4.1p1 Debian (protocol 2.0)
vulners:
cpe:/o:openbsd:openbsd-4.7p1:
95PACKETST080M:162145 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A248633A *EXPLOIT*
EDB-ID:49757 9.8 https://vulners.com/cve/CVE-2023-3840V
CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
B819W-CDB-3EB9-5631-9E93-0A4A-020A2175B23 9.8 https://vulners.com/githubexploit/819W-CDB-3EB9-5631-9E93-0A4A-020A2175B23 *EXPLOIT*
B809W-CDB-3EB9-5631-9E93-0A4A-020A2175B23 9.8 https://vulners.com/githubexploit/809W-CDB-3EB9-5631-9E93-0A4A-020A2175B23 *EXPLOIT*
RADB01159-546F-546F-AAB7-2D8F03F027FC 9.8 https://vulners.com/githubexploit/0ADB01159-546F-546F-AAB7-2D8F03F027FC *EXPLOIT*
887EB879-2703-11EE-ADBA-C80AA9043978 9.8 https://vulners.com/githubexploit/887EB879-2703-11EE-ADBA-C80AA9043978 *EXPLOIT*
SE696884-B0B0-57FA-BF6E-D9B2219B027A 9.8 https://vulners.com/githubexploit/SE696884-B0B0-57FA-BF6E-D9B2219B027A *EXPLOIT*
3306237F-9799-5799-9120-F49E201B587 9.8 https://vulners.com/githubexploit/3306237F-9799-5799-9120-F49E201B587 *EXPLOIT*
0221252F-07F5-5799-9120-F49E201B587 9.8 https://vulners.com/githubexploit/0221252F-07F5-5799-9120-F49E201B587 *EXPLOIT*
CVE-2015-5606 8.5 https://vulners.com/cve/CVE-2015-5606
PAE015F-07F5-5799-9120-F49E201B587 8.5 https://vulners.com/githubexploit/PAE015F-07F5-5799-9120-F49E201B587 *EXPLOIT*
FB2E9BD1-43D7-563C-A197-006628820134 8.1 https://vulners.com/githubexploit/FB2E9BD1-43D7-563C-A197-006628820134 *EXPLOIT*
FA3992C2-9C4C-5359-8134-177126E6B03F 8.1 https://vulners.com/githubexploit/FA3992C2-9C4C-5359-8134-177126E6B03F *EXPLOIT*
F8981437-1287-563D-93F1-6575B1B1CE59 8.1 https://vulners.com/githubexploit/F8981437-1287-563D-93F1-6575B1B1CE59 *EXPLOIT*
F519E848-5665-5665-915E-915E 8.1 https://vulners.com/githubexploit/F519E848-5665-5665-915E-915E *EXPLOIT*
F1A0012-2-11EF-BE11-84A93843B75 8.1 https://vulners.com/freesbsd/F1A0012-2-11EF-BE11-84A93843B75
EFD615F0-0717-5471-AA83-0491FD4079AF 8.1 https://vulners.com/githubexploit/EFD615F0-0717-5471-AA83-0491FD4079AF *EXPLOIT*
ECD99C9C-6C91-563D-91E8-A0F4A13E1EB 8.1 https://vulners.com/githubexploit/ECD99C9C-6C91-563D-91E8-A0F4A13E1EB *EXPLOIT*
EB12C950-563D-563D-91E8-0A85A10772 8.1 https://vulners.com/githubexploit/EB12C950-563D-563D-91E8-0A85A10772 *EXPLOIT*
E660E1AF-TA87-57E2-AEEF-C1A4E1FEFFCD 8.1 https://vulners.com/githubexploit/E660E1AF-TA87-57E2-AEEF-C1A4E1FEFFCD *EXPLOIT*
E543E274-C20A-582A-8F8E-F8E3F3B1C345 8.1 https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F3B1C345 *EXPLOIT*
E53013-1938-552D-8001-675922B26911 8.1 https://vulners.com/githubexploit/E53013-1938-552D-8001-675922B26911 *EXPLOIT*
E1AE4ECA-40F7-58BC-9EAD-7813522F915 8.1 https://vulners.com/githubexploit/E1AE4ECA-40F7-58BC-9EAD-7813522F915 *EXPLOIT*
DC79E899-B877-5F86-9C16-0CF8C0540E8B8 8.1 https://vulners.com/githubexploit/DC79E899-B877-5F86-9C16-0CF8C0540E8B8 *EXPLOIT*
DC473885-554C-5776-BA0D-0175EA09C1D 8.1 https://vulners.com/githubexploit/DC473885-554C-5776-BA0D-0175EA09C1D *EXPLOIT*
D672258A-8E94-5910-9E84-A04C9C8AC47 8.1 https://vulners.com/githubexploit/D672258A-8E94-5910-9E84-A04C9C8AC47 *EXPLOIT*
DIE049F1-1938-552D-8001-675922B26911 8.1 https://vulners.com/githubexploit/DIE049F1-1938-552D-8001-675922B26911 *EXPLOIT*
CFEBF7AF-F51A-5302-8088-F814D05B33A6 8.1 https://vulners.com/githubexploit/CFEBF7AF-F51A-5302-8088-F814D05B33A6 *EXPLOIT*
CF00800A-0227-5E06-0048-84C27258E191 8.1 https://vulners.com/githubexploit/CF00800A-0227-5E06-0048-84C27258E191 *EXPLOIT*
CB2936E1-2358-5628-AC2A-04772F14F9B 8.1 https://vulners.com/githubexploit/CB2936E1-2358-5628-AC2A-04772F14F9B *EXPLOIT*
File Actions Edit View Help
SSV-11558 3 https://vulners.com/seebug/SSV:11558 *EXPLOIT*
PAE015F-07F5-5799-9120-F49E201B587 4.3 https://vulners.com/githubexploit/PAE015F-07F5-5799-9120-F49E201B587 *EXPLOIT*
PAE015F-07F5-5799-9120-F49E201B587 4.3 https://vulners.com/exploitpack/PAE015F-07F5-5799-9120-F49E201B587 *EXPLOIT*
EDB-ID:35738 4.3 https://vulners.com/cve/CVE-2016-8612
CVE-2016-8612 4.3 https://vulners.com/cve/CVE-2016-8612
CVE-2016-1896 4.3 https://vulners.com/cve/CVE-2016-1896
CVE-2013-1896 4.3 https://vulners.com/cve/CVE-2013-1896
CVE-2012-4558 4.3 https://vulners.com/cve/CVE-2012-4558
CVE-2012-4549 4.3 https://vulners.com/cve/CVE-2012-4549
CVE-2012-4549 4.3 https://vulners.com/cve/CVE-2012-4549
CVE-2011-4317 4.3 https://vulners.com/cve/CVE-2011-4317
CVE-2011-13639 4.3 https://vulners.com/cve/CVE-2011-13639
CVE-2011-0419 4.3 https://vulners.com/cve/CVE-2011-0419
CVE-2010-8943 4.3 https://vulners.com/cve/CVE-2010-8943
CVE-2009-0023 4.3 https://vulners.com/cve/CVE-2009-0023
CVE-2008-2939 4.3 https://vulners.com/cve/CVE-2008-2939
CVE-2008-0455 4.3 https://vulners.com/cve/CVE-2008-0455
CVE-2008-0455 4.3 https://vulners.com/cve/CVE-2008-0455
SSV-12628 2.6 https://vulners.com/seebug/SSV:12628 *EXPLOIT*
CVE-2012-2687 2.6 https://vulners.com/cve/CVE-2012-2687
CVE-2009-0394 2.6 https://vulners.com/cve/CVE-2009-0394
CVE-2009-0456 2.6 https://vulners.com/cve/CVE-2009-0456
SSV-60250 1.2 https://vulners.com/seebug/SSV:60250 *EXPLOIT*
CVE-2011-4415 1.2 https://vulners.com/cve/CVE-2011-4415
1337DAY-ID-21300 0.0 https://vulners.com/zdt/1337DAY-ID-21300 *EXPLOIT*
1337DAY-ID-21346 0.0 https://vulners.com/zdt/1337DAY-ID-21346 *EXPLOIT*
1337DAY-ID-17257 0.0 https://vulners.com/zdt/1337DAY-ID-17257 *EXPLOIT*
1337DAY-ID-16843 0.0 https://vulners.com/zdt/1337DAY-ID-16843 *EXPLOIT*
1337DAY-ID-11185 0.0 https://vulners.com/zdt/1337DAY-ID-11185 *EXPLOIT*
111/tcp open rpcbind 2 (RPC #100000)
rpcinfo:
   port/proto service
  100000 2 111/tcp rpcbind
  100000 2 111/udp rpcbind
  100003 2,3,4 2049/tcp nfs
  100003 2,3,4 2049/udp nfs
  100005 1,2,3 34607/tcp mountd
  100005 1,2,3 51295/udp mountd
  100021 1,3,4 41032/tcp nlockmgr
  100021 1,3,4 51432/tcp nlockmgr
  100024 1,3,4 64770/tcp status
  100024 1,3,4 64770/tcp status
  100024 1,3,4 64801/udp status
  100024 1,3,4 64801/udp status
139/tcp open netbios-ssn 4.0 (Microsoft Windows 4.0 (Workgroup: WORKGROUP)
MAC Address: 00:0C:27:7A:B9:68 (Oracle VirtualBox Virtual NIC)
Service Info: Host: metasploitable (Metasploitable Domain: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.89 seconds
(ritesh@vbox) ~]
```

**Outcomes:**

CO2: Comprehend purpose of Anonymity and Foot printing.

---

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

From this experiment, I learned how to perform Active Reconnaissance using tools like Nmap and Netcat. I understood the importance of gathering information about a target system to identify potential vulnerabilities. Using Nmap, I was able to explore various scanning techniques such as port scanning, service version detection, and OS detection, which are crucial for ethical hacking and penetration testing. Active Reconnaissance helps in identifying weaknesses in a system that can later be exploited, but it also emphasizes the need for ethical usage of these tools. Overall, this experiment enhanced my knowledge of network security and reinforced the significance of recon in cybersecurity.

---

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

---

**References:**

- <https://nmap.org/book/>
- <https://nmap.org/book/nse.html>
- <https://www.geeksforgeeks.org/introduction-to-nmap/>
- <https://www.tutorialspoint.com/netcat>