NMAP

- What is Nmap?
  - Nmap is an open source utility that is used for finding vulnerable services on a network by scanning through different ports.

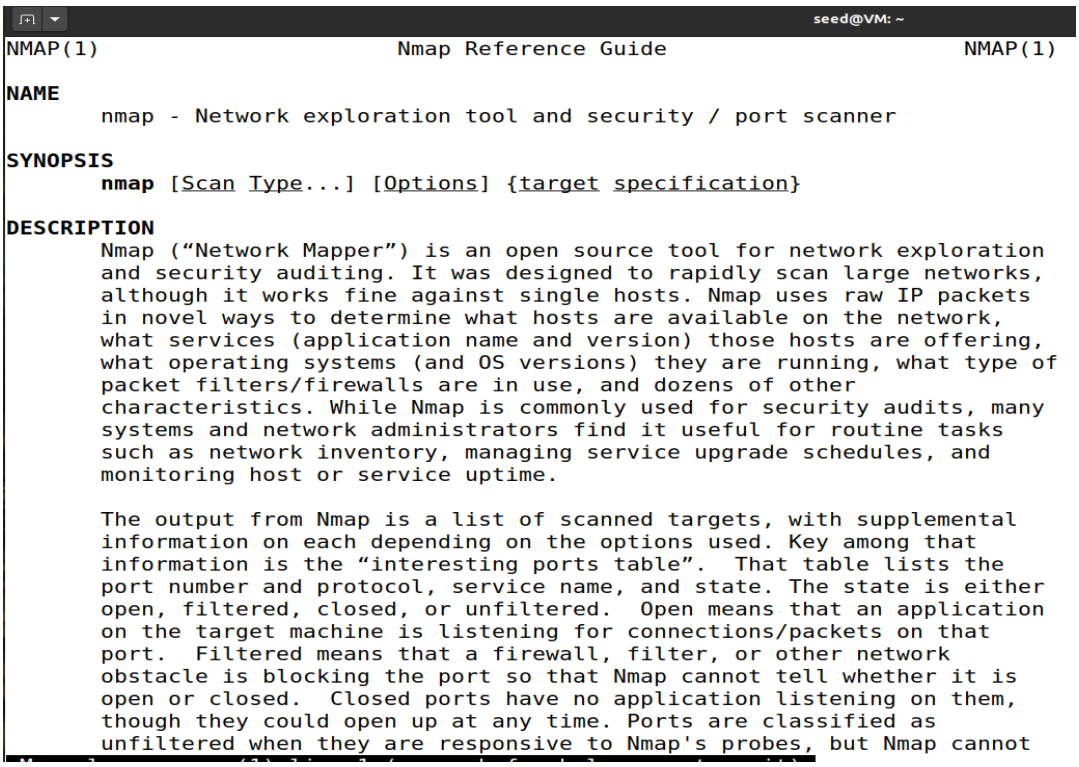
- Installation:
  - Windows OS: Nmap can be installed on the Windows workstation by visiting the official website (https://nmap.org/download.html) and downloading self-installer.

  - Linux OS: Nmap can be installed on Linux OS using following commands as per the appropriate Linux Distro:
    - "yum install nmap" / "sudo apt-get install nmap"

  - Mac OS: Nmap can be installed on Mac OS by following installation instructions mentioned on the official Nmap website: https://nmap.org/download.html#macosx

- Throughout this guide, all the commands are run on Ubuntu 20.04 OS and the outputs are taken on the same OS.

- After installing Nmap, the various options/switches can be found by running "man nmap" command on Linux which provide manual of Nmap. Below screenshot shows the output of same command:



- Nmap contains different types of switches to run a variety of scans against the target system and the usage of each switch are provided in detail in next section of this guide.
- For testing the switches, a vulnerable virtual machine setup is created in same network range as the Attacker machine (Ubuntu 20.04) and various switches are used against this target system to analyse their outputs which are as follows:

    - -sn: This option is used for scanning hosts on the network and once the available hosts are discovered nmap stops the port scan.
        - Nmap -sn 192.168.133.0/24

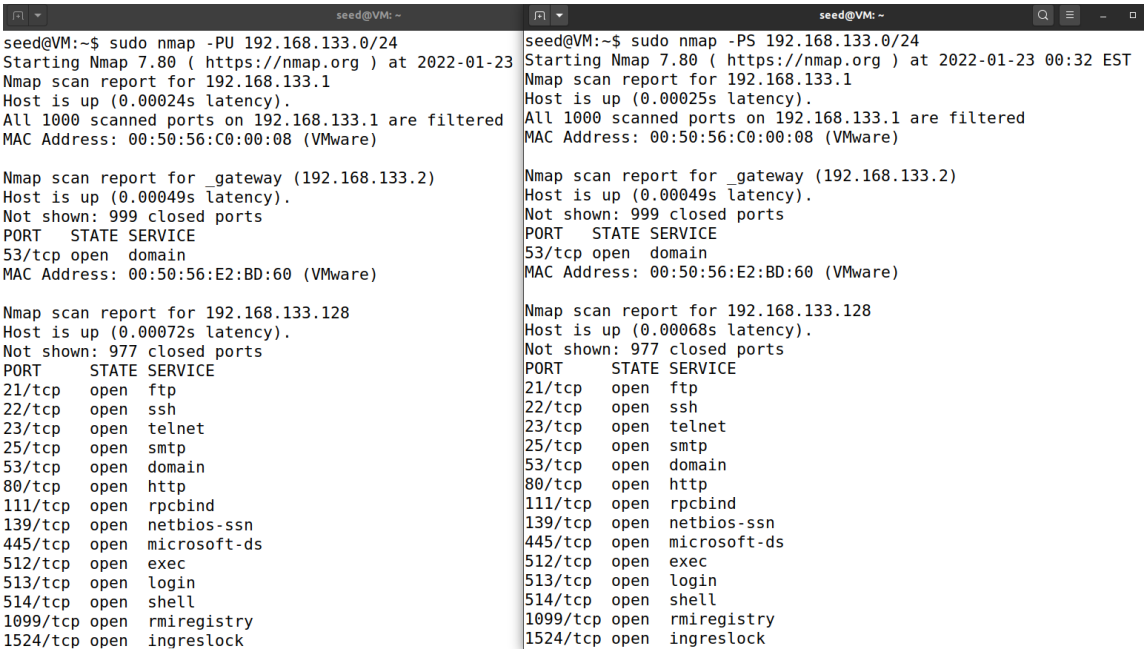
```
seed@VM:~$ nmap -sn 192.168.133.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-21 19:26 EST
Nmap scan report for _gateway (192.168.133.2)
Host is up (0.00096s latency).
Nmap scan report for 192.168.133.128
Host is up (0.00058s latency).
Nmap scan report for VM (192.168.133.131)
Host is up (0.00067s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.08 seconds
seed@VM:~$
```

    - -PO [protocol list]: This option is used for performing host discovery with the specified port number set in the IP header.
        - Nmap -PO 192.168.133.0/24

```
seed@VM: ~
seed@VM:~$ sudo nmap -PO 192.168.133.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-23 00:34 EST
Nmap scan report for 192.168.133.1
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.133.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for _gateway (192.168.133.2)
Host is up (0.00043s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E2:BD:60 (VMware)

Nmap scan report for 192.168.133.128
Host is up (0.00098s latency).
Not shown: 977 closed ports
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
```

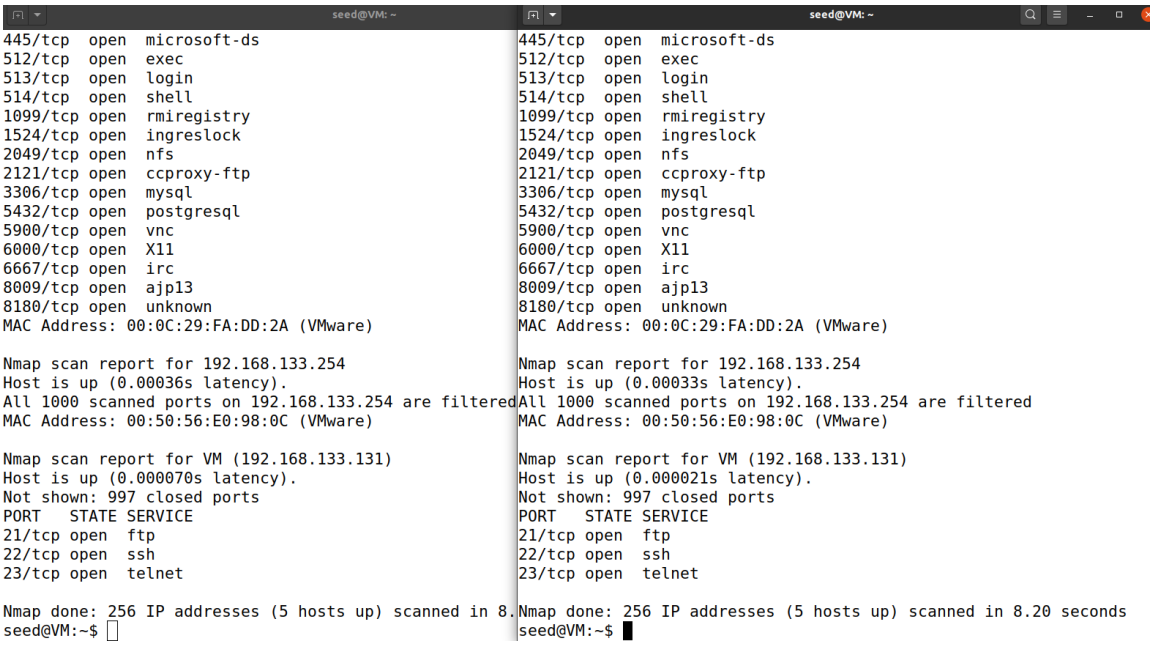
- Similar to -PO, the -PS and -PU options can also be used for performing various port scans as shown below:

    - -PS [portlist]: This option sends TCP request whereas an empty packet will be sent with SYN flag set.
    - -PU [portlist]: This option is used to send UDP packet for discovery to the given ports.
        - Nmap -PS 192.168.133.0/24
        - Nmap -PU 192.168.133.0/24



```
seed@VM:~$ sudo nmap -PU 192.168.133.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-23
Nmap scan report for 192.168.133.1
Host is up (0.00024s latency).
All 1000 scanned ports on 192.168.133.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for _gateway (192.168.133.2)
Host is up (0.00049s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E2:BD:60 (VMware)

Nmap scan report for 192.168.133.128
Host is up (0.00072s latency).
Not shown: 977 closed ports
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
```

```
seed@VM:~$ sudo nmap -PS 192.168.133.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-23 00:32 EST
Nmap scan report for 192.168.133.1
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.133.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for _gateway (192.168.133.2)
Host is up (0.00049s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E2:BD:60 (VMware)

Nmap scan report for 192.168.133.128
Host is up (0.00068s latency).
Not shown: 977 closed ports
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
```



```
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  ccproxy-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: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.133.254
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.133.254 are filtered
MAC Address: 00:50:56:E0:98:0C (VMware)

Nmap scan report for VM (192.168.133.131)
Host is up (0.000070s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.
seed@VM:~$
```

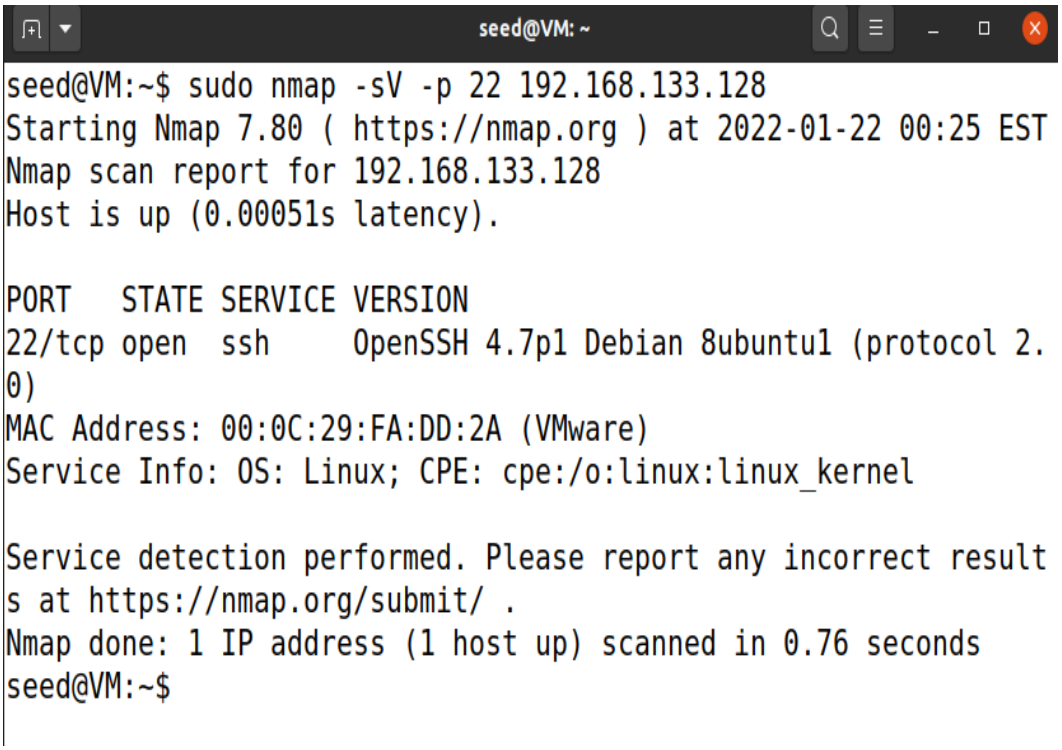
```
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.133.254
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.133.254 are filtered
MAC Address: 00:50:56:E0:98:0C (VMware)

Nmap scan report for VM (192.168.133.131)
Host is up (0.000021s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.20 seconds
seed@VM:~$
```

- -sO: This option is used for determining supported IP protocols by target machine
  - Namp -sO 192.168.133.128

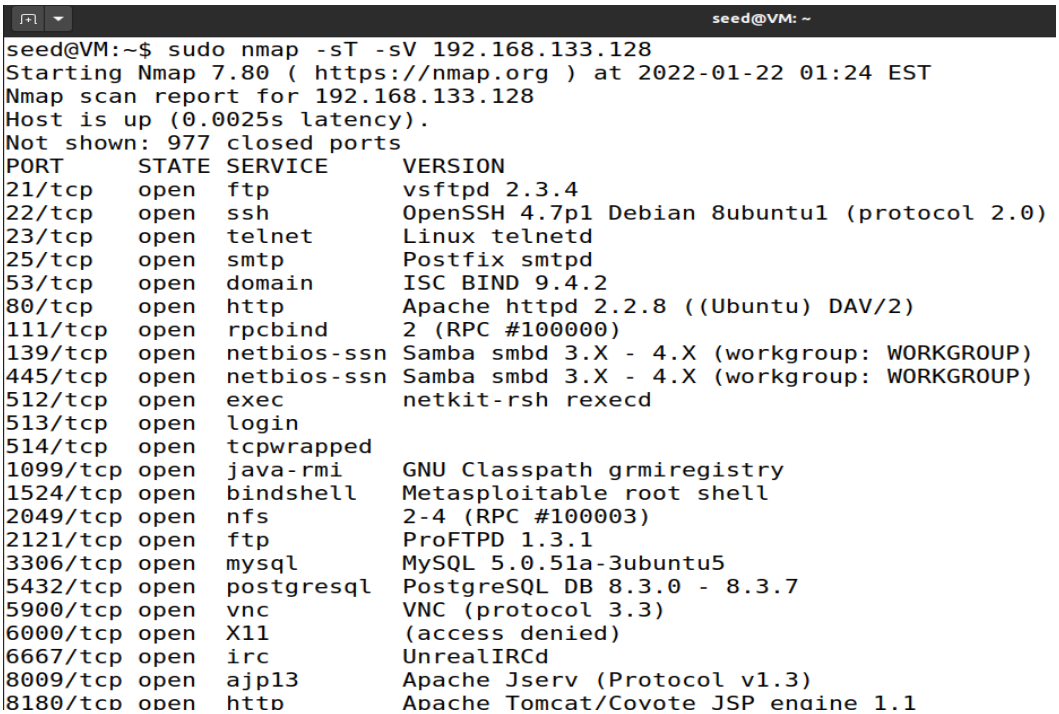
- -O: This option is used for determining OS version
  - Nmap -O 192.168.133.128

```
[01/22/22]seed@VM:~$ sudo nmap -O 192.168.133.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-22 00:06 EST
Nmap scan report for 192.168.133.128
Host is up (0.0013s latency).
Not shown: 977 closed ports
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  ccproxy-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: 00:0C:29:FA:DD:2A (VMware)
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
```

- -sV: This option probes open ports and determines service/version information
  - Nmap -sV -p 22 192.168.133.128



- -sT: This option is used for performing TCP connect scan on the target systems
  - Nmap -sT -sV 192.168.133.128



- -sS: This option is usef for performing stealth scan on target system to identify vulnerable services
  - Nmap -sS -sV 192.168.133.128

```
seed@VM:~$ sudo nmap -sS -sV 192.168.133.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-22 01:05 EST
Nmap scan report for 192.168.133.128
Host is up (0.00072s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
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
```

- sF: This option performs TCP FIN scan on target system to identify vulnerable services
  - Nmap -sF -sV 192.168.133.128

```
seed@VM: ~
seed@VM:~$ sudo nmap -sF -sV 192.168.133.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-22 01:17 EST
Nmap scan report for 192.168.133.128
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
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  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
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
```

- As observed, each scan performed results different output as per the appropriate circumstances on the target system/network and provides results in depth if used in correct way for identifying vulnerable servieces on the target network