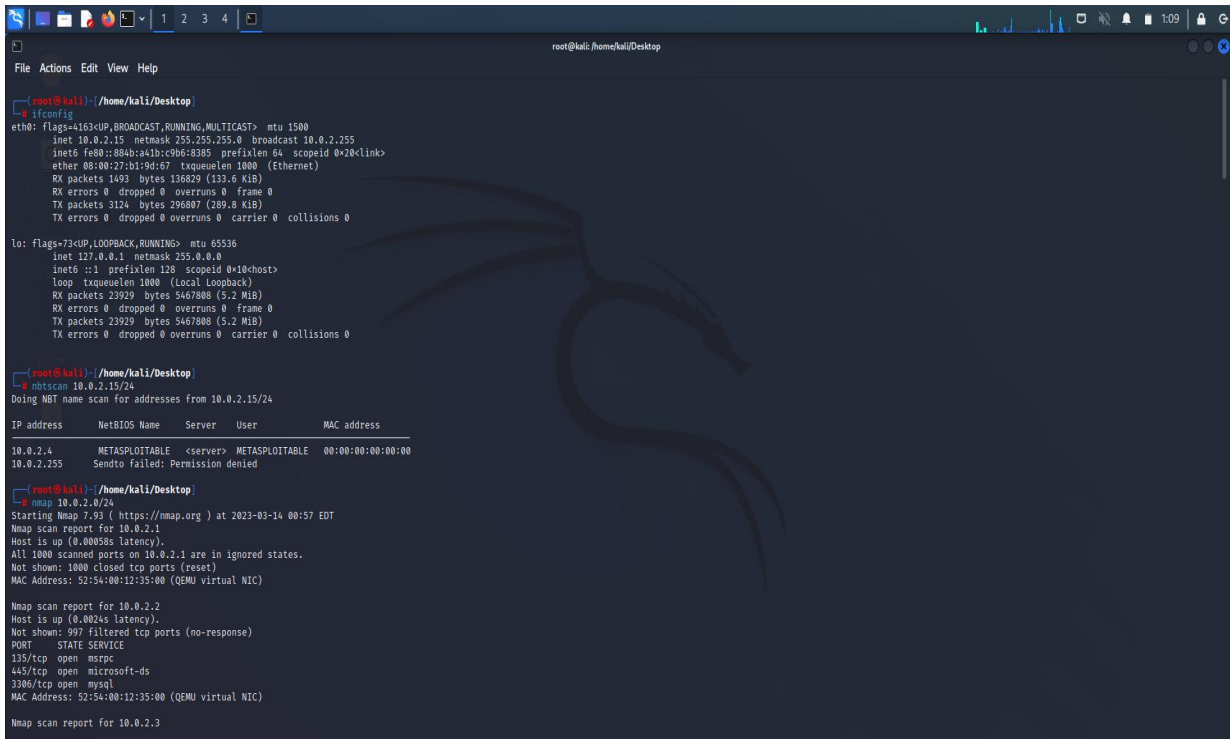


NETWORK SCANNING

Nmap is the most famous reconnaissance tool among Pentesters and Hacker. It is essentially a port scanner that helps you scan networks and identify various ports and services available in the network, besides also providing further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

A screenshot of a Kali Linux terminal window. The terminal shows the output of the 'ifconfig' command for the 'eth0' and 'lo' interfaces. The 'eth0' interface is connected to the network 10.0.2.15. The 'lo' interface is the loopback address 127.0.0.1. Below this, the 'nbtscan' command is used to scan the 10.0.2.15/24 network, showing results for 10.0.2.4 and 10.0.2.255. Finally, the 'nmap' command is used to scan 10.0.2.0/24, showing detailed scan reports for 10.0.2.1, 10.0.2.2, and 10.0.2.3. The scan for 10.0.2.1 shows it is up and has no open ports. The scan for 10.0.2.2 shows it is up and has three open ports: 135/tcp (marpc), 445/tcp (microsoft-ds), and 3306/tcp (mysql). The scan for 10.0.2.3 shows it is up and has no open ports.

```
(root@kali) ~/home/kali/Desktop
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::80ab:2a1b:c9b6:8385 prefixlen 64 scopeid 0<link>
    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
    RX packets 1493 bytes 136829 (133.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3124 bytes 296807 (289.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 23929 bytes 5467808 (5.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23929 bytes 5467808 (5.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali) ~/home/kali/Desktop
# nbtscan 10.0.2.15/24
Doing NBT name scan for addresses from 10.0.2.15/24
IP address NetBIOS Name Server User MAC address
10.0.2.4 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
10.0.2.255 Sendto failed: Permission denied

(root@kali) ~/home/kali/Desktop
# nmap 10.0.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 00:57 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00058s latency).
All 1000 scanned ports on 10.0.2.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.00024s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  marpc
445/tcp    open  microsoft-ds
3306/tcp    open  mysql
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
```

- -sV: Probe open ports to determine service/version info
- -O: Enable OS detection
- -A: Enables “aggressive” scanning. Presently this enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (-traceroute)
- -p: Specify the ports to scan. It can be a single port as well as a range of ports.
- -sT: In this type of scan, Nmap sends a TCP packet to a port with the SYN flag set.

```
root@kali: /home/kali/Desktop

File Actions Edit View Help

root@kali: /home/kali/Desktop
# nmap -p 21,22,23 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 01:00 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00076s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 08:00:27:BB:76:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds

root@kali: /home/kali/Desktop
# nmap -sT 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 01:01 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00070s 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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
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
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:BB:76:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

root@kali: /home/kali/Desktop
```

```
root@kali: /home/kali/Desktop

File Actions Edit View Help

MAC Address: 08:00:27:BB:76:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

root@kali: /home/kali/Desktop
# nmap -A 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 01:01 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00006s latency).
Not shown: 977 closed tcp ports (reset)

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 10.0.2.15
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 600fcef1c09f6a74d69024fac4d56ccd (DSA)
|_2048 5656240f211ddea72bae61b1243d8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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_server_header: Apache/2.2.8 (Ubuntu) DAV/2
|_http_title: Metasploitab2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_program version 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 33322/tcp mountd
|_100005 1,2,3 36222/udp mountd
|_100021 1,3,4 33115/udp nlockmgr
|_100021 1,3,4 41995/tcp nlockmgr
|_100024 1 43783/udp status
```

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
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 147.92 seconds

root@kali: /home/kali/Desktop
nmap -O 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 01:06 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00100s 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  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: 08:00:27:BB:76:1E (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 15.51 seconds

root@kali: /home/kali/Desktop
```

```
10.0.2.255    Sendto failed: Permission denied

root@kali: /home/kali
nmap -sV 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 01:08 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00049s latency).
Not shown: 977 closed tcp ports (reset)
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)
```