Practical-3

➔ **Identify all active hosts on a local network using Nmap.**

```
root@kali:~# nmap -sn 192.168.182.1/24
Starting Nmap 7.94SVN ( https://nmap.o
Nmap scan report for 192.168.182.1
Host is up (0.00021s latency).
MAC Address: 00:50:56:C0:00:08 (VMware
Nmap scan report for 192.168.182.2
Host is up (0.000089s latency).
MAC Address: 00:50:56:E5:9B:8C (VMware
Nmap scan report for 192.168.182.129
Host is up (0.00064s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware
Nmap scan report for 192.168.182.130
Host is up (0.00021s latency).
MAC Address: 00:0C:29:38:F9:16 (VMware
Nmap scan report for 192.168.182.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:F1:30:2E (VMware
Nmap scan report for 192.168.182.128
Host is up.
Nmap done: 256 IP addresses (6 hosts u
```

➔ **Detects open TCP ports on a remote server using a SYN scan.**

```
root@kali:~# nmap -sS 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.o
Nmap scan report for 192.168.182.129
Host is up (0.0011s latency).
Not shown: 978 closed tcp ports (reset
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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

Nmap done: 1 IP address (1 host up) sc
```

➔ **Determine the versions of services running on open ports of a target host.**

```
root@kali:~# nmap -sV 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.o
Nmap scan report for 192.168.182.129
Host is up (0.0017s latency).
Not shown: 978 closed tcp ports (reset
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.
22/tcp   open  ssh         OpenSSH 4.7
23/tcp   open  telnet      Linux telne
25/tcp   open  smtp        Postfix smt
80/tcp   open  http        Apache http
111/tcp  open  rpcbind     2 (RPC #100
139/tcp  open  netbios-ssn Samba smbd
445/tcp  open  netbios-ssn Samba smbd
512/tcp  open  exec        netkit-rsh
513/tcp  open  login       OpenBSD or
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpa
1524/tcp open  bindshell   Metasploita
2049/tcp open  nfs         2-4 (RPC #1
2121/tcp open  ftp         ProFTPD 1.3
3306/tcp open  mysql       MySQL 5.0.5
5432/tcp open  postgresql  PostgreSQL
5900/tcp open  vnc         VNC (protoc
6000/tcp open  X11         (access den
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jser
8180/tcp open  http        Apache Tomc
MAC Address: 00:0C:29:FA:DD:2A (VMware
Service Info: Hosts:  metasploitable.l
nix, Linux; CPE: cpe:/o:linux:linux_ke
```

➔ **Perform OS detection to identify the operating system of a network device.**

```
root@kali:~# nmap -O 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.o
Nmap scan report for 192.168.182.129
Host is up (0.00066s latency).
Not shown: 978 closed tcp ports (reset
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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

OS detection performed. Please report
submit/ .
Nmap done: 1 IP address (1 host up) sc
```

➔ **Conduct an aggressive scan to gather comprehensive information about a target system.**

```
root@kali:~# nmap -A 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.o
Nmap scan report for 192.168.182.129
Host is up (0.00056s latency).
Not shown: 978 closed tcp ports (reset
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.
|_ftp-anon: Anonymous FTP login allowe
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.182.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 3
|      Control connection is plain tex
|      Data connections will be plain
|      vsFTPd 2.3.4 - secure, fast, st
|_End of status
22/tcp   open  ssh         OpenSSH 4.7
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae
23/tcp   open  telnet      Linux telne
25/tcp   open  smtp        Postfix smt
| ssl-cert: Subject: commonName=ubuntu
A/stateOrProvinceName=There is no such
| Not valid before: 2010-03-17T14:07:4
|_Not valid after:  2010-04-16T14:07:4
|_ssl-date: 2024-08-06T05:14:51+00:00;
|_smtp-commands: metasploitable.locald
RN, STARTTLS, ENHANCEDSTATUSCODES, 8BI
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_M
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
80/tcp   open  http        Apache http
```

➔ **Scan for open UDP ports on a given host to identify active UDP services.**

```
root@kali:~# nmap -sU 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:08 EDT
Nmap scan report for 192.168.182.129
Host is up (0.00064s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
639/udp  open|filtered msdp
2049/udp open          nfs
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1043.00 seconds
```

→ **Execute a ping sweep to find live devices within a specific subnet.**

```
root@kali:~# nmap -sn 192.168.182.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:24 EDT
Nmap scan report for 192.168.182.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.182.2
Host is up (0.00016s latency).
MAC Address: 00:50:56:E5:9B:8C (VMware)
Nmap scan report for 192.168.182.129
Host is up (0.00020s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.182.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:F1:30:2E (VMware)
Nmap scan report for 192.168.182.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 10.10 seconds
```

→ **Compare the results of a TCP connect scan with a SYN scan on a target host.**

```
root@kali:~# nmap -sT 192.168.182.129 && nmap -sS 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:29 EDT
Nmap scan report for 192.168.182.129
Host is up (0.00071s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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)

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:29 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0012s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
```

→ **Use a decoy scan to obscure the source of the network scan from detection.**

```
root@kali:~# nmap -D RND:10 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:30 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0081s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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)

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
```

➔ **Map the network path to a target host using Nmap's traceroute functionality.**

```
root@kali:~# nmap --traceroute 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:31 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0012s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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)

TRACEROUTE
HOP RTT     ADDRESS
1   1.16 ms 192.168.182.129

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

➔ **Conduct an Xmas scan to test the stealthiness of a target's firewall.**

```
root@kali:~# nmap -sX 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:40 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0036s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.49 seconds
```

➔ **Run an Nmap scan with custom port ranges to identify services running on non-standard ports.**

```
root@kali:~# nmap -p 1000-2000 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:41 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0027s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
```

➔ **Compare the results of a TCP connect scan with a SYN scan on a target host.**

```
root@kali:~# nmap -sS 192.168.182.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 23:55 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0026s latency).
Not shown: 979 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

➔ **Analyze the impact of different Nmap timing templates on scan speed and accuracy.**

```
root@kali:~# nmap 192.168.182.129 -T3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 23:58 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0017s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```