

Network Scanning

Scanning:

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, identifying Vulnerabilities and threats in the network. Network Scanning is used in identifying active devices on a network by employing features in the network protocol.

What will we get After Scanning:

- Active computer
- Identifying open port and close port
- Operating system Information
- Services and version
- Vulnerabilities
- All Process (Ports) running in networks

Networks and data are transferred with the help of conceptual model (OSI and TCP/IP Model).

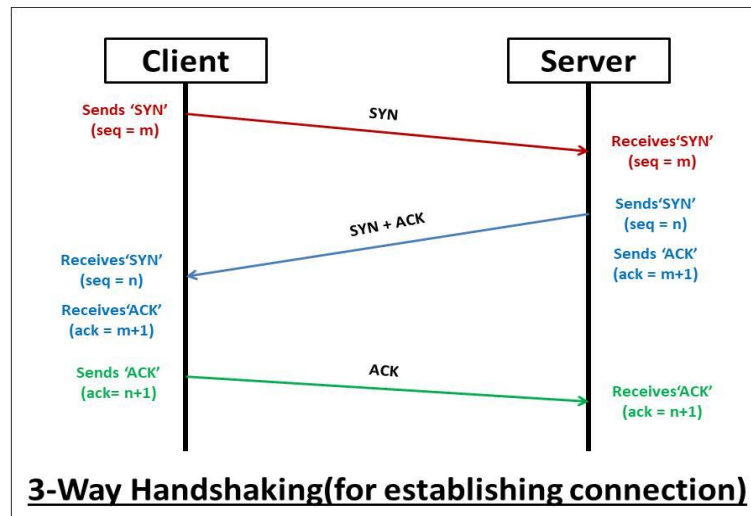
TCP:

- Connection oriented Protocol.
- Connection established between ends of transmission.
- Generate a virtual circuit between Sender and Receiver for the duration of transmission.

UDP:

- Connectionless protocol. Simple protocol and provides non-sequenced transport functionality.
- Reliability and security are less important than speed and size.

TCP Handshake:



Steps:

1. SYN (Synchronize):

- **Client** sends a **SYN** (Synchronize) message to the server.
- It includes an initial **sequence number (m)**, which will be used for ordering packets in future communications.

2. SYN + ACK (Synchronize and Acknowledge):

- **Server** receives the **SYN** request from the client.
- The server responds with its own **SYN** (sequence number = n) to establish communication.
- Along with the SYN, the server also sends an **ACK** (acknowledgment) of the client's sequence number (m+1), confirming that it received the client's request.

3. ACK (Acknowledge):

- **Client** receives the server's SYN and ACK.
- The client sends an **ACK** back to the server to confirm the server's sequence number (n+1).

- Once this is done, the connection is fully established, and communication can begin.

NMAP:

- **nmap <target ip-address> :**

used to scan the open ports.

```
(kali㉿kali)-[~]  
$ nmap 192.168.1.1  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 09:42 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.00065s 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  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  
  
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

- **arp:**

used to get the arp table of the system (contains MAC and ip-address).

```
(kali@kali)-[~]
$ arp
Address      HWtype  HWaddress  Flags Mask  Iface
192.168.1.254 ether    00:50:56:e0:95:68  C        eth0
192.168.1.133 ether    00:0c:29:14:72:41  C        eth0
192.168.1.1  ether    00:50:56:c0:00:08  C        eth0
192.168.1.2  ether    00:50:56:e8:6a:ab  C        eth0

(kali@kali)-[~]
$
```

- **sudo nmap -sN <target ip-address> -PR:**

```
(kali@kali)-[~]
$ sudo nmap -sN 192.168.1.133 -PR

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 10:00 EDT
Nmap scan report for 192.168.1.133
Host is up (0.00080s latency).
Not shown: 977 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
53/tcp    open|filtered domain
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:29:14:72:41 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds

(kali@kali)-[~]
$
```

- The open|filtered state suggests these ports may be protected by a firewall or access control.
- **Null Scan (-sN):** Sends TCP packets with no flags set. It helps determine port status:
- **Closed ports** send back RST (reset) packets.
- **Open ports** don't respond, making this scan stealthy.
- **ARP Ping (-PR):** Sends ARP (Address Resolution Protocol) requests to the target IP to discover if the host is active. This is used only on local networks.

- **Superuser Privileges (sudo):** Allows Nmap to send raw packets, which is required for both the Null scan and ARP ping.
- **sudo nmap -sN --traceroute <target ip-address>-PR :**
 - The open|filtered state suggests these ports may be protected by a firewall or access control.
 - **Null Scan (-sN):** Sends TCP packets with no flags set to detect open/closed ports. Closed ports respond with RST (reset) packets, and open ports do not respond.
 - **Traceroute (--traceroute):** Maps the path (hops) that packets take from your machine to the target IP. It helps in identifying network devices and intermediate routers along the path.
 - **ARP Ping (-PR):** Sends ARP requests to discover active hosts on a local network (used for host discovery).
 - **Superuser Privileges (sudo):** Required to send raw packets for the scan and perform ARP requests.

```
(kali㉿kali)-[~]
$ sudo nmap -sN --traceroute 192.168.1.133 -PR

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 10:11 EDT
Nmap scan report for 192.168.1.133
Host is up (0.0027s latency).
Not shown: 977 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
53/tcp    open|filtered domain
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:29:14:72:41 (VMware)

TRACEROUTE
HOP RTT      ADDRESS
1 2.73 ms 192.168.1.133

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
(kali㉿kali)-[~]
```

- **sudo nmap -O <target ip-address> :**
 - **-O:** This option enables OS detection. Nmap tries to determine the operating system of the target by analyzing TCP/IP stack characteristics.
 - **-PR** can be used at the end, then ARP scanning works when ICMP or TCP/UDP ping requests are blocked by a firewall.

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.1.133 -PR

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 10:22 EDT
Nmap scan report for 192.168.1.133
Host is up (0.00065s 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: 00:0C:29:14:72:41 (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 any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds

(kali@kali)-[~]
```

- **nmap -sV <target ip-address> :**
 - **-sV:** This option enables version detection. Nmap attempts to determine the version of services (like web servers, FTP, SSH, etc.) running on open ports.
 - **-PR** can be used at the end, then ARP scanning works when ICMP or TCP/UDP ping requests are blocked by a firewall.

```

(kali@kali)-[~]
$ nmap -sV 192.168.1.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 10:26 EDT
Nmap scan report for 192.168.1.133
Host is up (0.84s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
Service Info: Hosts: metasploitable.localdomain, irc.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 13.36 seconds

```

- **nmap -A <target ip-address> :**
 - **-A:** This option enables several advanced features:
 - **OS detection:** Attempts to determine the operating system of the target.
 - **Version detection:** Identifies the versions of services running on open ports.
 - **Script scanning:** Runs a set of Nmap scripts against the target to gather more information (e.g., checking for vulnerabilities).
 - **Traceroute:** Determines the network path to the target by performing a traceroute.

```

(kali@kali)-[~]
$ nmap -A 192.168.1.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 10:39 EDT
Nmap scan report for 192.168.1.129
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.1.129
|_  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 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-09-26T14:39:41+00:00; -1s from scanner time.
|_sslsv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

```

```
File Actions Edit View Help
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 50421/tcp mountd
| 100005 1,2,3 59994/udp mountd
| 100021 1,3,4 49197/udp nlockmgr
| 100021 1,3,4 58651/tcp nlockmgr
| 100024 1 34850/tcp status
| 100024 1 45851/udp status
| 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| 445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (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
| 1024/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
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 14
| Capabilities flags: 43564
| Some Capabilities: SwitchToSSLAfterHandshake, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, SupportsCompression, LongColumnFlag, Support41Auth
| Status: Autocommit
| Salt: MAr:gWj2jDwL57#TA
| 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| ssl-date: 2024-09-26T14:39:42+00:00: -1s from scanner time.
| 5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
| VNC Authentication (2)
| 6000/tcp open X11 (access denied)
```

PORTS:

- Port is a virtual point where network connections start and end.
- Ports allow computers to easily differentiate between different kinds of traffic.
- Ports are standardized across all network-connected devices, with each port assigned a number. Ports are reserved for certain protocols

Ex. Http – Port 80

- Port numbers allow targeting specific services or applications within those devices.

Types:

1. Open

- The port is open and accepting connections.
- Indicates that a service is actively running and can be accessed.

2. Closed

- The port is closed and not accepting connections.
- The service is not running on that port, but the port is reachable, meaning the target is aware of it.

3. Filtered

- Nmap cannot determine whether the port is open or closed because a firewall or network device is blocking the scan.
- The packets sent to the port are being dropped or rejected, preventing Nmap from receiving a response.

4. Unfiltered

- The port is reachable, but Nmap cannot determine whether it is open or closed.
- This usually occurs when there's a firewall that does not filter traffic but does not respond to the scan.

5. Open/Filtered

- Nmap cannot determine if the port is open or filtered.
- This typically happens when no response is received from the port; it may either be open but not responding or filtered by a firewall.

6. Closed/Filtered

- This is a less common state that indicates that the port is likely closed, but a firewall is also blocking the scan, so Nmap cannot confirm its state.
- Similar to filtered, but it suggests more strongly that the port is closed.

- **nmap -p <port-number/numbers> <target ip-address> :**
 - **-p 80:** This option specifies that Nmap should only scan port 80.
 - Works for single port in this case.

```
(kali㉿kali)-[~]
$ nmap -p 80 192.168.1.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 21:41 EDT
Nmap scan report for 192.168.1.133
Host is up (0.00078s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

(kali㉿kali)-[~]
$
```

- **-p 80,21,23:** This option specifies that Nmap should scan port 80,21,23.

- Works for multiple port in this case. (can specify multiple ports)

```
(kali㉿kali)-[~]
$ nmap -p 80,21,22,23 192.168.1.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 21:53 EDT
Nmap scan report for 192.168.1.133
Host is up (0.0050s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

- **-p 1-1000**: This option specifies that Nmap should scan from port 1 to port 1000.
- Scanning port ranges.

- **nmap -p- <target ip-address> :**

- **-p-**: This tells Nmap to scan **all ports**, from port 1 through port 65,535. By default, Nmap only scans the 1,000 most common ports, but this option forces a full range scan.
- Shows open state and which services are running.

```
(kali㉿kali)-[~]
$ nmap -p- 192.168.1.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 22:03 EDT
Nmap scan report for 192.168.1.133
Host is up (0.0016s latency).
Not shown: 65505 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  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
32814/tcp open  unknown
46611/tcp open  unknown
47057/tcp open  unknown
50186/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.34 seconds

(kali㉿kali)-[~]
```

- **sudo nmap -sU <target ip-address> :**

- **-sU:** This option tells Nmap to perform a **UDP scan**, scanning for open UDP ports rather than TCP ports.
- Takes a little time to scan ports.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.80.133
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 22:09 EDT
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 4.54% done; ETC: 22:19 (0:09:07 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 16.56% done; ETC: 22:24 (0:12:26 remaining)
Stats: 0:05:54 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 35.86% done; ETC: 22:26 (0:10:31 remaining)
Stats: 0:09:36 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 56.06% done; ETC: 22:26 (0:07:31 remaining)
Stats: 0:13:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 76.46% done; ETC: 22:26 (0:04:00 remaining)
Stats: 0:15:59 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 94.26% done; ETC: 22:26 (0:00:58 remaining)
Nmap scan report for 192.168.80.133
Host is up (0.00052s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT      STATE      SERVICE
53/udp    open       domain
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
2049/udp   open       nfs
34796/udp open       unknown
MAC Address: 00:0C:29:14:72:41 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1033.60 seconds
```