Nmap Part -1

What is Nmap

Nmap is a footprinting or a reconnaissance tool
So here in using nmap we can gather the information about the target
this free open source tool can be installed from the nmap.org

It can be any command in linux we can get the information of how we can use the command and figuring it out how it can be helpful by
" man command_name " or "command_name --help"

In this case the command is "nmap --help"

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --help
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
```

```
NMAP(1)                          Nmap Reference Guide                          NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS

       nmap [Scan Type ...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are
       available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is
       commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table".  That table lists the port number and protocol, service name, and state. The
       state is either open, filtered, closed, or unfiltered.  Open means that an application on the target machine is listening for connections/packets on that port.  Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap
       cannot tell whether it is open or closed.  Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or
       closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP
       protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

       A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.

       Example 1. A representative Nmap scan

           # nmap -A -T4 scanme.nmap.org

           Nmap scan report for scanme.nmap.org (74.207.244.221)
           Host is up (0.029s latency).
           rDNS record for 74.207.244.221: li86-221.members.linode.com
           Not shown: 995 closed ports
           PORT     STATE    SERVICE     VERSION
           22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
           | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
           |_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
           80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
           |_http-title: Go ahead and ScanMe!
           646/tcp  filtered ldp
           1720/tcp filtered H.323/Q.931
           9929/tcp open     nping-echo  Nping echo
           Device type: general purpose
           Running: Linux 2.6.X
           OS CPE: cpe:/o:linux:linux_kernel:2.6.39
           OS details: Linux 2.6.39
           Network Distance: 11 hops
           Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

           TRACEROUTE (using port 53/tcp)
           HOP RTT      ADDRESS
           [Cut first 10 hops for brevity]
Manual page nmap(1) line 1 (press h for help or q to quit)
```

we can practice the nmap scanner with the given scanme.Nmap.org or need to setup a vm of metasploitable 2 which is an vuln machine

We can scan for a specific port number rather than the scanning for all the ports

we can also do a grep able output with : nmap -oG target_ip -vv path(where the file need to be saved)

Aggressive Scanning

nmap -A -sV target_ip

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -sV  10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 02:57 EST
Stats: 0:03:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.62% done; ETC: 03:00 (0:00:02 remaining)
Stats: 0:03:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.34% done; ETC: 03:00 (0:00:01 remaining)
Nmap scan report for 10.0.2.7
Host is up (0.0012s 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 8ubuntu1 (protocol 2.0)
```

```
Host is up (0.0012s 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 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?
|_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: Metasploitable2 - 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      57338/udp   mountd
|   100005  1,2,3      57819/tcp   mountd
|   100021  1,3,4      39730/udp   nlockmgr
|   100021  1,3,4      50081/tcp   nlockmgr
|   100024  1          47454/udp   status
|_  100024  1          59434/tcp   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
1524/tcp open  bindshell   Metasploitable root shell
```

```
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
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 25
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, SwitchToSSLAfterHandshake, ConnectWithDatabase, LongColumnFlag, Support
sTransactions, Support41Auth, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: {|",XX/~R_e`0lR5On\d
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-02-07T10:27:34+00:00; -21h33m15s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
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)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:69:F2:E9 (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: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
```


```
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)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:69:F2:E9 (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: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-02-07T05:26:54-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: -19h53m13s, deviation: 2h53m14s, median: -21h33m15s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   1.25 ms 10.0.2.7

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 234.96 seconds
```


Host Discovery with ping sweep

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 02:57 EST
Nmap scan report for 10.0.2.7
Host is up (0.00098s latency).
MAC Address: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 10.0.2.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 03:01 EST
Nmap scan report for 10.0.2.1
Host is up (0.00080s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00065s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00057s latency).
MAC Address: 08:00:27:A4:85:1C (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.0012s latency).
MAC Address: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.14 seconds
```

-sn uses only icmp protocol and it is for host discovery and also scans for tcp port 443 and SYN and ACK to port 80

-Pn Disabling basically skips host discovery.

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn 10.0.2.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 03:08 EST
Stats: 0:00:18 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.14% done; ETC: 03:08 (0:00:00 remaining)
Stats: 0:00:18 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.58% done; ETC: 03:08 (0:00:00 remaining)
Stats: 0:00:18 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.91% done; ETC: 03:08 (0:00:00 remaining)
Nmap scan report for 10.0.2.1
Host is up (0.00085s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
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 10.0.2.3
Host is up (0.00019s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:A4:85:1C (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.7
Host is up (0.00043s 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
```

```
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: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 256 IP addresses (5 hosts up) scanned in 19.40 seconds
```

Nmap OS and Service Version Scanning

We now know the systems which are up in our network now we must check for the operating systems versions which is the -O option

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -sV  10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 03:28 EST
Nmap scan report for 10.0.2.7
Host is up (0.0017s 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
```

We can combine both -O and -sV for more information

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O  -sV 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 03:33 EST
Nmap scan report for 10.0.2.7
Host is up (0.0014s 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
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
MAC Address: 08:00:27:69:F2:E9 (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

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 12.93 seconds
```

TCP connect and Stealth(SYN) scanning

In this scan it establishes a three way connection to give the accuracy of the information but these scans are slow and can be detectable

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 09:46 EST
Nmap scan report for 10.0.2.7
Host is up (0.0039s 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
MAC Address: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)
```

nmap -sT target_ip

In this scan the full tcp connection is established when it comes to the stealth scan a tcp connection is not established fully

nmap -sS target_ip

```
└─# nmap -sS 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 09:50 EST
Nmap scan report for 10.0.2.7
Host is up (0.00020s 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: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

Udp Scanning

When dealing with Udp that means we are not dealing with connection oriented services since udp is a connection less protocol and we need to look after the responses based on ICMP messages

if we do not get any response from the target or the server then the port is open if we get a icmp unreachable response then it means the port is closed

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 10.0.2.7 --reason
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 09:59 EST
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 8.59% done; ETC: 10:13 (0:13:07 remaining)
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 8.69% done; ETC: 10:13 (0:13:08 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 9.09% done; ETC: 10:13 (0:13:10 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 10.09% done; ETC: 10:14 (0:13:13 remaining)
Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 10.19% done; ETC: 10:14 (0:13:13 remaining)
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 10.29% done; ETC: 10:14 (0:13:13 remaining)
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 12.00% done; ETC: 10:14 (0:13:27 remaining)
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.10% done; ETC: 10:14 (0:13:23 remaining)
Stats: 0:02:15 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.20% done; ETC: 10:14 (0:13:22 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 16.20% done; ETC: 10:15 (0:13:06 remaining)
Stats: 0:03:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 17.91% done; ETC: 10:15 (0:13:04 remaining)
Stats: 0:03:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 18.01% done; ETC: 10:15 (0:13:03 remaining)
Stats: 0:03:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 18.11% done; ETC: 10:15 (0:13:02 remaining)
Stats: 0:03:07 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
```

```
UDP Scan Timing: About 40.51% done; ETC: 10:16 (0:10:01 remaining)
Stats: 0:07:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.61% done; ETC: 10:16 (0:10:00 remaining)
sendto in send_ip_packet_sd: sendto(5, packet, 68, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51879 > 10.0.2.7:34577 ttl=57 id=5023 iplen=68
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51862 > 10.0.2.7:2345 ttl=46 id=61298 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51864 > 10.0.2.7:2345 ttl=38 id=22452 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51866 > 10.0.2.7:2345 ttl=56 id=26730 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51868 > 10.0.2.7:2345 ttl=56 id=49717 iplen=28
Stats: 0:22:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 52.85% done; ETC: 10:42 (0:20:08 remaining)
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51870 > 10.0.2.7:2345 ttl=58 id=1615 iplen=28
Stats: 0:22:48 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 52.86% done; ETC: 10:42 (0:20:08 remaining)
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51872 > 10.0.2.7:2345 ttl=59 id=16314 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51874 > 10.0.2.7:2345 ttl=57 id=51802 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51876 > 10.0.2.7:2345 ttl=47 id=9722 iplen=28
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 10.0.2.7, 16) => Network is unreachable
Offending packet: UDP 10.0.2.15:51878 > 10.0.2.7:2345 ttl=45 id=3047 iplen=28
Omitting future Sendto error messages now that 10 have been shown.  Use -d2 if you really want to see them.
```

Inverse TCP Flag Scanning

It is similar to not sending any tcp flags , it is important though it is nothing to do with tcp handshake
The main reason is to avoid the detection from the IDS so in an event to make the scan evade or trying not to detected by the IDS

Fin scan is where we are sending a packet with fin tco header
Xmas scan which sends the fin urgent push tcp flags all together so that is why it is blowing the target
Null scan essentially is where you are not sending any tcp flags at all and then based on the response the nmap determines whether the port is open or not

When using inverse tcp flag scanning if we do not get the response then the port is open if it is closed you will get the RST or ACK

Xmas scan which combines both Fin Urge and Push flags

```
└─# nmap -sX  10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 04:17 EST
Nmap scan report for 10.0.2.7
Host is up (0.0021s 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
```

We need to remember that these Inverse scans does not support for windows because tcp ip stack does not support these types of requests

we can see the results are like open|filtered that is because this scan does not depend on the flags that are part of tcp 3 way handshake the result may be same for the Fin scan because we are seeing if the port is open then no response if not it will return RST or ACK

we can analyze the result in the port-by-port basis

-sX for xmas scan
-sF for Fin scan
-sN for Null scan

With the reason option we can see how and why the nmap concluded that this port is open or closed

```
└─# nmap -sN  10.0.2.7 --reason
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 04:31 EST
Nmap scan report for 10.0.2.7
Host is up, received arp-response (0.00066s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE     REASON
21/tcp   open|filtered ftp         no-response
22/tcp   open|filtered ssh         no-response
23/tcp   open|filtered telnet      no-response
25/tcp   open|filtered smtp        no-response
53/tcp   open|filtered domain      no-response
80/tcp   open|filtered http        no-response
111/tcp  open|filtered rpcbind     no-response
139/tcp  open|filtered netbios-ssn no-response
445/tcp  open|filtered microsoft-ds no-response
512/tcp  open|filtered exec        no-response
513/tcp  open|filtered login       no-response
514/tcp  open|filtered shell       no-response
1099/tcp open|filtered rmiregistry no-response
1524/tcp open|filtered ingreslock  no-response
```

Output and verbosity

Output which is the result of the scans we have done so far is a important aspect has it holds all the information as a result about the target

One must know how to use this effectively , How to generate it effectively , verbosity where Controlling how much output you want in your scans

Nmap has three types of output
1.xml
2.Normal nmap human readable
3.grepable output

using -oA we can have all the three formats at a time

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 10.0.2.7 -oA /home/kali/results.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-08 11:34 EST
Nmap scan report for 10.0.2.7
Host is up (0.00067s 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
```

```
10.0.2.7.gnmap  10.0.2.7.nmap  10.0.2.7.xml
```

-oN for normal format
-oG for grep able format
-oX for xml format

for verbosity three levels
-v
-vv
-vvv
for debugging
-dd

--open for showing only opened ports

Checking for firewalls using ack probing (detection)

we need to send the ack packets and then analyze the response
if we do not get a response which means that there is a firewall and if we receive a RST response this means there is no firewall

nmap -sA 10.0.2.7 --reason

```
# nmap -sA  10.0.2.7 --reason
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 04:47 EST
Nmap scan report for 10.0.2.7
Host is up, received arp-response (0.0014s latency).
All 1000 scanned ports on 10.0.2.7 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Firewall invasion (Decoys, MTU & Fragmentation)

There are two techniques to evading the firewalls

First way is to work with techniques like spoofing using decoys changing the minimum transmission unit
Second is to using the decoys fragmenting packets which really does not work

Simply using decoys and showing that the ip scan is from another ip address and this can work on the internet or the local area network and spoof an ip address that belongs to an admin or a network admin

decoy scan is simply running a syn scan and service version and a fast scan
nmap -sS -sV -F -D

when we are in local network use the ip address we are willing to spoof and if we are in internet use the RND option you can check the ip which is whitelisted in the server or for the website and use that to evade the firewall

if we get RST back it means the port is open