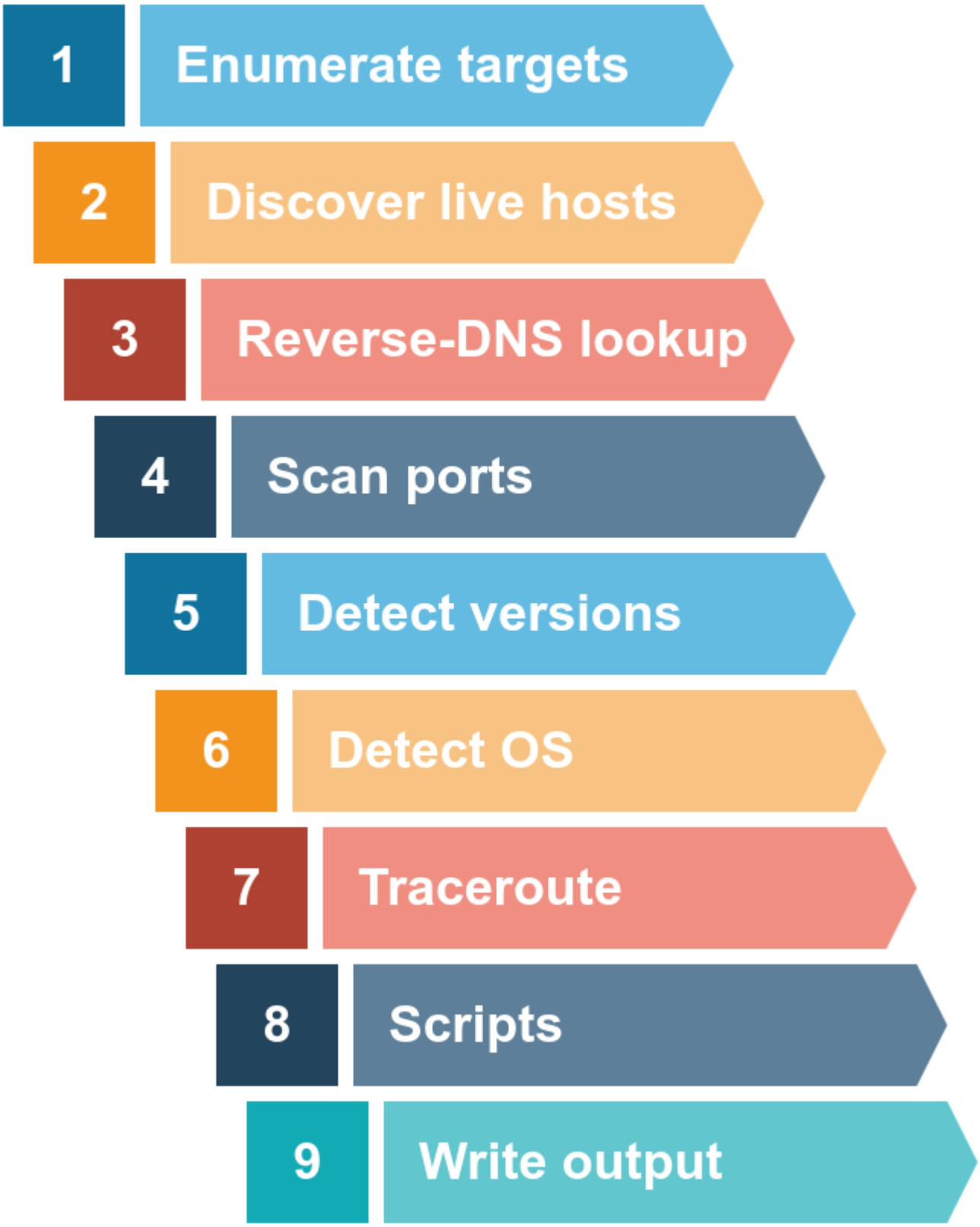
_Port Scanner/VulScanner__

Nmap



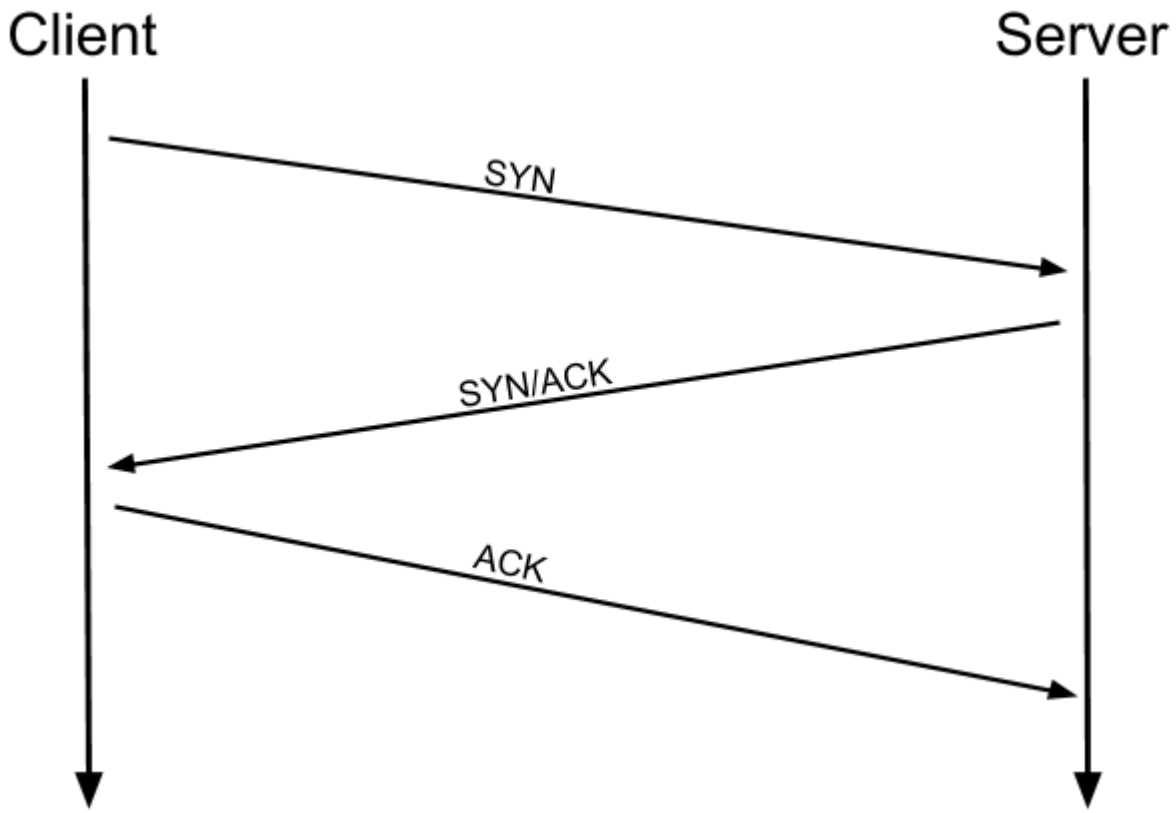
nmap [OPTION] [TARGET] [PORT\S]

Scan types

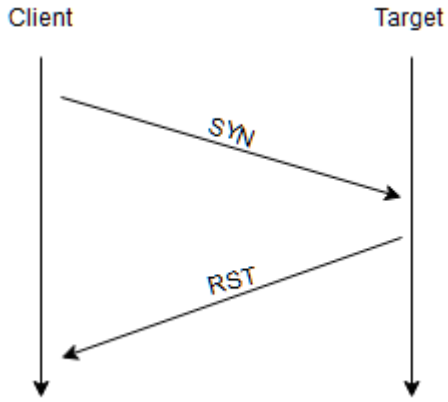
When port scanning with Nmap, there are three basic scan types. These are:

- TCP Connect Scans " Full connect " (-sT)

In this type of scan we try to do a full handshake with the target port to check if the port is open or not if the target responded with RST flag that means the port is closed if we managed to do the full handshake that means the port is opened if we didn't get either that means the port is open|filtered which means the port is either closed or blocked by a firewall



Opened



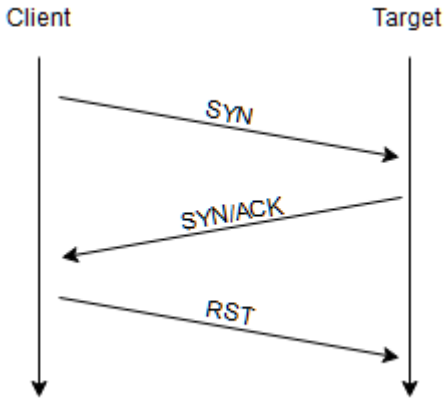
Closed

`Many firewalls are configured to simply drop incoming packets. Nmap sends a TCP SYN request, and receives nothing back. This indicates that the port is being protected by a firewall and thus the port is considered to be filtered.``

- SYN Scans "Half-open/Stealth Scan" (-sS)

in this type of scan we send the target a SYN flag and if we got a respond we send the target a RST flag to close the connection and mark it as open port

and if we got RST the port is closed and nothing means filtered



Opened

Advantages :

- Faster than full connect scan
- it can bypass older versions of IDS systems
- SYN scans are often not logged by applications listening on open ports,most of the time systems log a connection once it's been fully established.
- UDP Scans (-sU)

In UDP scan there is no handshake because UDP is stateless
when the packet is sent to an open most of the time the port won't respond and it will be marked by nmap open|filtered or open if the port responded which is unusual
when a packet is sent to a closed UDP port, the target should respond with an ICMP (ping) packet containing a message that the port is unreachable. This clearly identifies closed ports, which Nmap marks as such and moves on.

`UDP scan tend to be very slow scan because Nmap has to double check for each port to see if it's actually opened or closed When scanning UDP ports, Nmap usually sends completely empty requests -- just raw UDP packets. That said, for ports which are usually occupied by well-known services, it will instead send a protocol-specific payload which is more likely to elicit a response from which a more accurate result can be drawn.`

Host Discovery

- ARP scan: This scan uses ARP requests to discover live hosts

`ARP query aims to get the hardware MAC so that communication over the link-layer becomes possible and we can use the to check if the target is up or not ARP only to discover the devices within that subnet ARP queries won’t be routed and hence cannot cross the subnet router`

- ICMP scan: This scan uses ICMP requests to identify live hosts

- TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

-sn
Disable port scanning. Host discovery only.

-Pn
Disable host discovery, Port scan only

-PS
TCP SYN discovery

-PA
TCP ACK discovery

-PU
UDP discovery

-PR
ARP discovery

Port Specification

to specify ports
-p
nmap 192.168.1.1 -p 21
specific port

-p
nmap 192.168.1.1 -p 21-100
Port range

-p
nmap 192.168.1.1 -p U:53,T:21-25,80
Port scan multiple TCP and UDP ports

-p-
Port scan all ports

Service and Version Detection

-sV
Attempts to determine the version of the service running on port

-A
Enables OS detection, version detection, script scanning, and traceroute

OS Detection

-O
Remote OS detection using TCP/IP
stack fingerprinting

-A
Enables OS detection, version detection, script scanning, and traceroute

Speed

-T1-5

-T3 is the default speed

Types of TCP scans

- TCP Null Scans (-sN)

Null scan is a TCP request sent to the target with no flags set at all the target should respond with RST if the port is closed

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	54	36717 → 80 [<None>] Seq=1 Win=1024 Len=0
2	0.000012387	127.0.0.1	127.0.0.1	TCP	54	80 → 36717 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
Acknowledgment number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x000 (<None>)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
```

- TCP FIN Scans (-sF)

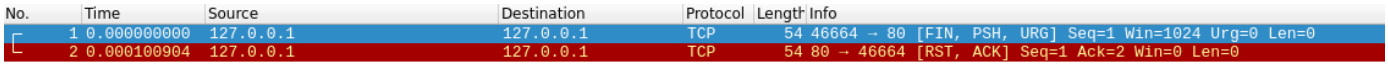
a request is sent with the FIN flag Nmap expects a RST if the port is closed.

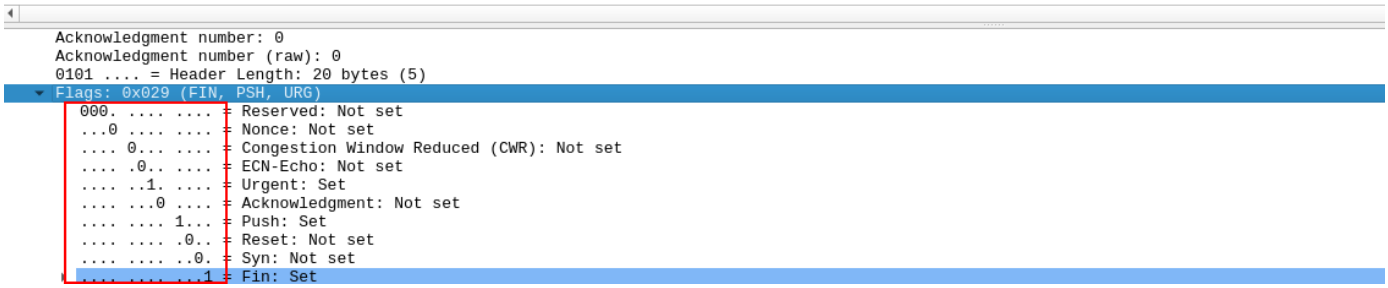
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	54	33952 → 80 [FIN] Seq=1 Win=1024 Len=0
2	0.000013391	127.0.0.1	127.0.0.1	TCP	54	80 → 33952 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

```
Acknowledgment number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x001 (FIN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...1 = Fin: Set
```

- TCP Xmas Scans (-sX)

send a malformed TCP packet and expects a RST response for closed ports.
It's referred to as an xmas scan as the flags that it sets (PSH, URG and FIN)





If the ports are opened in the previous scan types it's similar to UDP f the port is open then there is no response to the malformed packet

NULL, FIN and Xmas scans will only ever identify ports as being open|filtered, closed, or filtered. If a port is identified as filtered with one of these scans then it is usually because the target has responded with an ICMP unreachable packet.

`` It's also worth noting that while RFC 793 mandates that network hosts respond to malformed packets with a RST TCP packet for closed ports and don't respond at all for open ports

the goal here is, of course, firewall evasion. Many firewalls are configured to drop incoming TCP packets to blocked ports which have the SYN flag set (thus blocking new connection initiation requests). By sending requests which do not contain the SYN flag, we effectively bypass this kind of firewall. Whilst this is good in theory, most modern IDS solutions are savvy to these scan types, so don't rely on them to be 100% effective when dealing with modern systems.``

Scripts (NSE) Nmap Scripting Engine

can be used to do a variety of things: from scanning for vulnerabilities, to automating exploits for them

Script types

safe:- Won't affect the target
intrusive:- Not safe: likely to affect the target
vuln:- Scan for vulnerabilities
exploit:- Attempt to exploit a vulnerability
auth:- Attempt to bypass authentication for running services (e.g. Log into an FTP server anonymously)
brute:- Attempt to bruteforce credentials for running services
discovery:- Attempt to query running services for further information about the network (e.g. query an SNMP server).

-sC to Scan with default NSE scripts

we can specify which type of scripts we can run by doing --script=SCRIPT_TYPE e.g --script=safe

to run a specific script we would use --script= e.g --script=ftp-anon.nse
we can do multiple scripts by separating them with , e.g --script=smb-enum-users,smb-enum-shares

some scripts use or require arguments These can be given with the --script-args or --script-args-file to provide a file as args

example:
nmap -p 80 --script http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php'

to look for help for specific script we do nmap --script-help