

NMAP

Creator: Aniello Giugliano

INDEX

- ▶ What is Nmap
- ▶ Features
- ▶ Functionality
- ▶ Target Discovery
- ▶ Host Discovery
- ▶ TCP protocol
- ▶ Port Scanning
- ▶ Os Fingerprinting and Version Detection
- ▶ NSE scripting

What is NMAP?

Nmap (Network Mapper) is an open-source tool for network exploration and auditing. It is designed to quickly scan large networks, but is also suitable for use on single hosts.

Nmap uses IP packets in various ways to determine which hosts are available on a network, what services are offered by these hosts, what operating system is running, what kind of firewall and packet filters are used, and many other features.

Features

- ▶ **Flexibility:** Supports dozens of advanced network mapping techniques. This includes many port scanning mechanisms (both TCP and UDP), OS detection, version detection, ping sweep, and more.
- ▶ **Power:** It is used to scan huge networks of hundreds of thousands of machines.
- ▶ **Portability:** supported by most operating systems.
- ▶ **Ease of use:** there are lots of online guides and in addition the -help command provides a very clear and detailed overview of all the options that can be used.

Features (2)

- ▶ **Free**: the main goal of the Nmap project is to help make the Internet more secure and to provide administrators / auditors / hackers with an advanced tool to explore their networks.
- ▶ **Documented**: there are books, tutorials and papers that explain their use.
- ▶ **Popular**: Thousands of people use it.

Functionality of NMAP

- ▶ **Host Discovery:** identifying hosts on a network.
- ▶ **Port Scanning:** enumeration of ports open on target hosts.
- ▶ **Version detection:** Querying network services on remote devices to determine the application name and version number.
- ▶ **Operating System Detection:** determination of the operating system and hardware characteristics of network devices.
- ▶ **NSE Scripting:** scripts that allow you to perform more advanced actions.

Target Discovery

► Single ip address scan

```
# Scan a single ip address
nmap 192.168.1.1
# Scan a host name
nmap server1.neoslab.com
```

```
(kali@kali)-[~]
$ nmap 192.168.1.254
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-04 05:34 EST
Nmap scan report for myfastgate.nexxt (192.168.1.254)
Host is up (0.010s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 39.95 seconds
```

▶ Scanning of multiple ip addresses

```
nmap 192.168.1.1 192.168.1.2 192.168.1.3  
# Works with same subnet i.e. 192.168.1.0/24  
nmap 192.168.1.1,2,3
```

▶ Scanning a range of ip addresses

```
nmap 192.168.1.1-20
```

```
nmap 192.168.1.*
```

```
nmap 192.168.1.0/24
```


- ▶ **-iL** <inputfilename>

This command is used to read input from a text file passed as input

- ▶ **-iR** <num hosts>

This command is used to scan randomly chosen and generated ip addresses

- ▶ **--exclude** or **--excludefile**

This option is used to exclude certain IP addresses from scanning

```
(kali@kali)-[~]  
$ nmap -iR 30  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-04 05:52 EST  
Stats: 0:03:20 elapsed; 28 hosts completed (2 up), 2 undergoing Connect Scan  
Connect Scan Timing: About 84.80% done; ETC: 05:56 (0:00:35 remaining)  
Nmap scan report for 27-50-87-252.as45671.net (27.50.87.252)  
Host is up (0.29s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
1/tcp    open  tcpmux  
53/tcp   open  domain  
465/tcp  open  smtps  
  
Nmap scan report for 214.210.178.170-dedicated.multacom.com (170.178.210.214)  
Host is up (0.17s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
  
Nmap done: 30 IP addresses (2 hosts up) scanned in 249.81 seconds
```

Scan Speed

-T <num>

- ▶ **0 (Paranoid):** Designed to scan so slowly that it avoids detection by IDSs, falling outside their time sampling window. Packages are sent out approximately every 5 minutes. No packets are sent in parallel.
- ▶ **1 (Sneaky):** Packets are sent one every 15 seconds. No packets are sent in parallel.
- ▶ **2 (Polite):** Packets are sent every 0.4 seconds. No packets are sent in parallel. Designed to reduce network load and prevent target system equipment crashes.
- ▶ **3 (Normal):** Designed to work quickly but without overloading the sending machine or the network, it is the default mode. It scans in parallel, simultaneously sending multiple packets to multiple destination ports.

Scan Speed (2)

- ▶ **4 (Aggressive):** Aggressive mode never waits more than 1.25 seconds for a response and scans in parallel.
- ▶ **5 (Insane):** It only takes up to 15 minutes to scan a host, waiting only 0.3 seconds to get a response from a port.

```
(kali@ kali)-[~]  
$ nmap -T2 -Pn 192.168.1.254  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-15 04:53 EST  
Nmap scan report for myfastgate.nexxt (192.168.1.254)  
Host is up (0.0083s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 899.15 seconds
```

```
(kali@ kali)-[~]  
$ nmap -T5 192.168.1.254  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-09 04:55 EST  
Nmap scan report for myfastgate.nexxt (192.168.1.254)  
Host is up (0.0097s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 3.69 seconds
```

Host Discovery

► **-sL** (List Scan)

List Scan is a trivial form of host discovery that simply lists every host on the specified networks, without sending any packets to the target hosts. The scan list is a good check to make sure you have the correct IP addresses for your scan. If hosts show unknown domain names, it's worth investigating further to avoid scanning the wrong network.

► **-PE**: (Ping Scan)

is used to determine if a host is online. ICMP messages are used for this purpose.

```
(kali@kali)-[~]
$ nmap -sL 192.168.1.250-255
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-11 10:23 EST
Nmap scan report for 192.168.1.250
Nmap scan report for 192.168.1.251
Nmap scan report for 192.168.1.252
Nmap scan report for 192.168.1.253
Nmap scan report for myfastgate.nexxt (192.168.1.254)
Nmap scan report for 192.168.1.255
Nmap done: 6 IP addresses (0 hosts up) scanned in 0.01 seconds
```

```
(kali@kali)-[~]
$ nmap -PE 192.168.1.250-255
Warning: You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-15 05:20 EST
Nmap scan report for myfastgate.nexxt (192.168.1.254)
Host is up (0.0099s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.1.255
Host is up (0.0031s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
514/tcp   filtered shell

Nmap done: 6 IP addresses (2 hosts up) scanned in 42.35 seconds
```

► **-sn** (no port scan)

This option tells Nmap not to perform a port scan after host discovery and to show hosts that have responded. This option is often known as "ping scan". It allows for a mapping of a target network without attracting much attention.

```
(kali) kali ~  
$ nmap -sn 192.168.1.1-255  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-04 05:25 EST  
Nmap scan report for myfastgate.nexxt (192.168.1.254)  
Host is up (0.022s latency).  
Nmap scan report for 192.168.1.255  
Host is up (0.0023s latency).  
Nmap done: 255 IP addresses (2 hosts up) scanned in 37.22 seconds
```

► **-Pn** (no ping)

This option completely bypasses the host discovery phase. This causes Nmap to attempt the required scan functions against each specified destination IP address (considering all hosts as up).

```
C:\WINDOWS\system32>nmap -Pn scanme.nmap.org  
Starting Nmap 7.70 ( https://nmap.org ) at 2021-02-24 16:47 Hora est8ndar Montañas (Múxico)  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.10s latency).  
Not shown: 990 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    filtered smtp  
80/tcp    open  http  
135/tcp   filtered msrpc  
139/tcp   filtered netbios-ssn  
445/tcp   filtered microsoft-ds  
1025/tcp  filtered NFS-or-IIS  
6129/tcp  filtered unknown  
9929/tcp  open  nping-echo  
31337/tcp open  Elite  
Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

TCP Protocol

The Transmission Control Protocol (TCP) is a transport layer packet network protocol.

TCP has been designed and built to use the services offered by lower level network protocols (IP and physical layer and datalink layer protocols) to build a reliable communication channel between two network application processes.

The communication channel thus constructed is composed of a bidirectional stream of bytes following the establishment of a connection at the ends between the two communicating terminals.

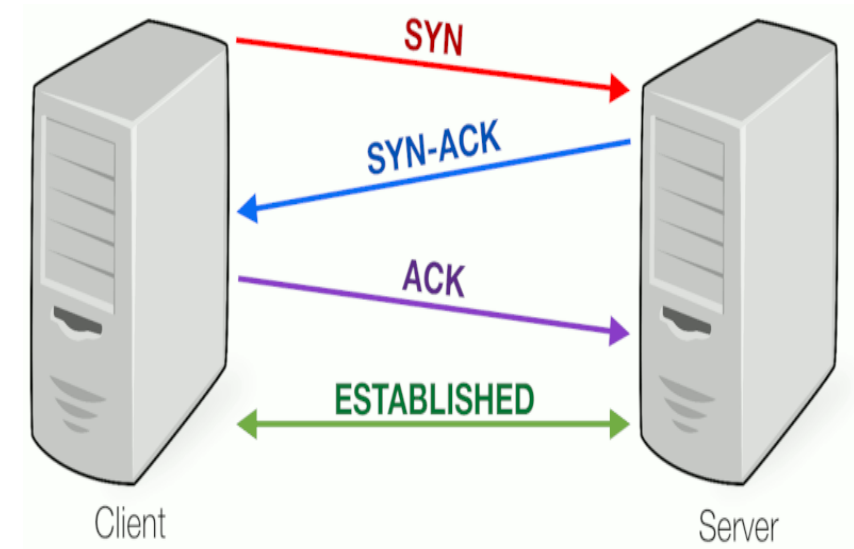
The main features of this protocol are:

- Connection oriented
- Reliability
- Error check
- Flow control
- Order

3-Way Handshake

is a method used on a TCP / IP network to create a connection between a client and a server.

- ▶ A client sends a SYN data packet over an IP network to a server on the same network or to an external network. The goal of this package is to ask if the server is available for new connections.
- ▶ The target server must have open ports that can accept and initiate new connections. When the server receives the SYN packet from the client node, it responds and returns an acknowledgment receipt, ACK packet or SYN / ACK packet.
- ▶ The client receives the SYN / ACK from the server and replies with an ACK packet.
- ▶ At the end of this process, the connection is created and the host and the server are able to communicate.



Port State

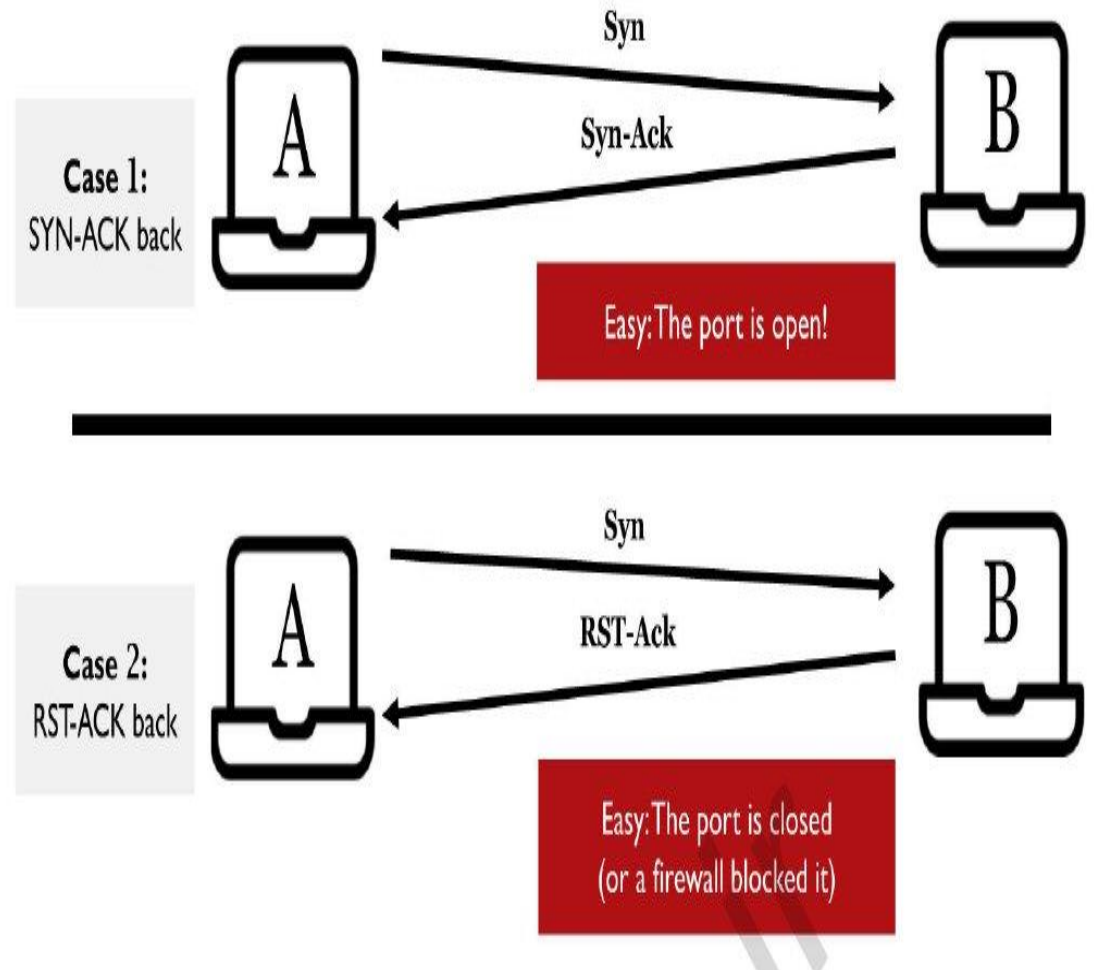
- ▶ **Open**: the port is not blocked and an application is listening on it.
- ▶ **Closed**: the port is not locked but there is no application listening on it.
- ▶ **Filtered**: a firewall blocks access to the port.

TCP Port Scanning

- ▶ **Case 1:** We get a SYN-ACK response, in which case we conclude that the door is probably open.
- ▶ **Case 2:** We receive a packet with both RST and ACK control bits set to 1. This RST-ACK packet tells us that the port is probably closed, rejecting our connection request. There is also the possibility that RST-ACK came from a firewall rather than the target system. Either way, we can't reach the door.

TCP Behavior While Port Scanning (I)

Port Scanning Basics

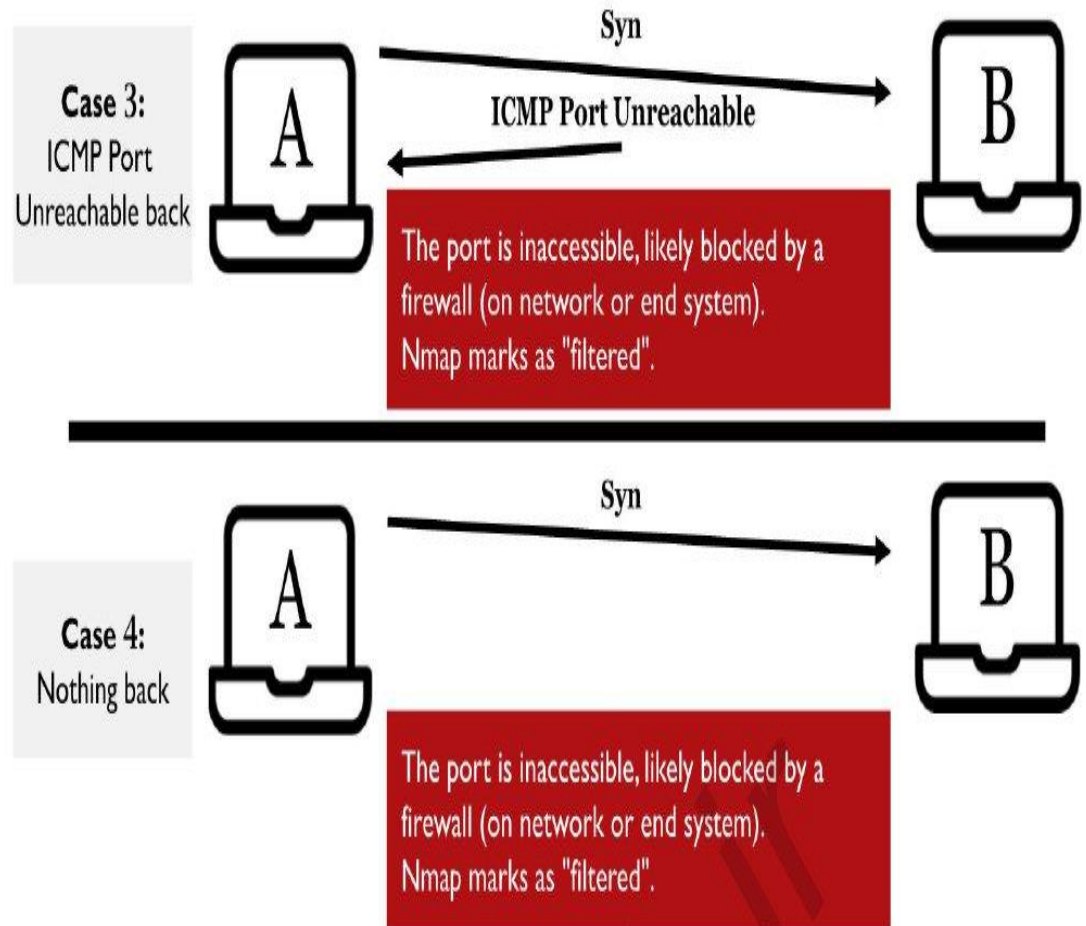


TCP Port Scanning (2)

- ▶ **Case 3:** We send a SYN packet and receive an ICMP message, such as an "ICMP Port Unreachable". The port is inaccessible, possibly because it is blocked by a firewall that is creating this message. Nmap marks this state as "filtered".
- ▶ **Case 4:** We send a SYN packet and receive nothing in return. Nmap will try to retransmit the packet, but if nothing is received within a certain timeout, the port will be marked as "filtered". Probably, either there is nothing listening on the final system or a firewall is blocking our incoming SYN packet.

TCP Behavior While Port Scanning (2)

Port Scanning Basics



Port Scanning

- ▶ Nmap by default scans the 1000 most commonly used ports on the internet. These ports are specified within the nmap-services file.
- ▶ **-F** (Fast Mode): Scan the first 100 ports
- ▶ **--top-ports**<num>: Scan the most commonly used "num" ports
- ▶ **-p -** : Scan all ports, from 1 to 65535 (excluding 0)
- ▶ **-p** <num port>: Scan only the indicated ports

```
(kali@kali)-[~]  
$ sudo nmap -p 22,25,80,443 192.168.1.254  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-07 05:25 EST  
Nmap scan report for myfastgate.nexxt (192.168.1.254)  
Host is up (0.0019s latency).  
  
PORT      STATE SERVICE  
22/tcp    filtered ssh  
25/tcp    filtered smtp  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

```
(kali@kali)-[~]  
$ nmap --top-ports 100 192.168.1.254  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-09 05:11 EST  
Nmap scan report for myfastgate.nexxt (192.168.1.254)  
Host is up (0.0090s latency).  
Not shown: 97 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 9.76 seconds
```

Port Scanning (2)

Using the command :

`grep -v '^#' /usr/share/nmap/nmap-services | sort -rk3 | head -n1000`

We can print a list of which are the 1000 most commonly used ports

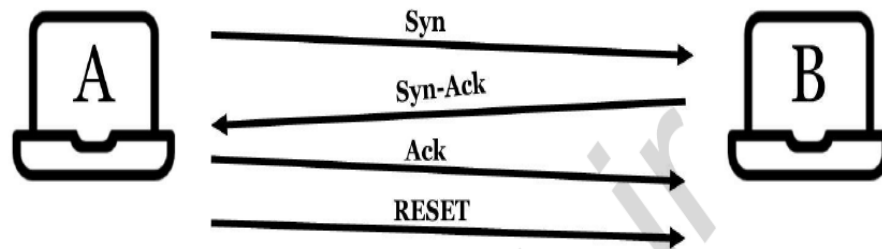
```
http      80/tcp    0.484143      # World Wide Web HTTP
ipp       631/udp    0.450281      # Internet Printing Protocol
snmp      161/udp    0.433467      # Simple Net Mgmt Proto
netbios-ns 137/udp    0.365163      # NETBIOS Name Service
ntp       123/udp    0.330879      # Network Time Protocol
netbios-dgm 138/udp    0.297830      # NETBIOS Datagram Service
ms-sql-m  1434/udp    0.293184      # Microsoft-SQL-Monitor
microsoft-ds 445/udp    0.253118
msrpc     135/udp    0.244452      # Microsoft RPC services
dhcps     67/udp     0.228010      # DHCP/Bootstrap Protocol Server
telnet    23/tcp     0.221265
domain    53/udp     0.213496      # Domain Name Server
https     443/tcp    0.208669      # secure http (SSL)
ftp       21/tcp     0.197667      # File Transfer [Control]
netbios-ssn 139/udp    0.193726      # NETBIOS Session Service
ssh       22/tcp     0.182286      # Secure Shell Login
isakmp    500/udp    0.163742
dhcpc     68/udp     0.140118      # DHCP/Bootstrap Protocol Client
route     520/udp    0.139376      # router routed -- RIP
upnp      1900/udp    0.136543      # Universal PnP
smtp      25/tcp     0.131314      # Simple Mail Transfer
```

Port Scanning (3)

Nmap TCP Port Scan Types: Connect Scan

Nmap

- TCP Connect Scan, invoked with `-sT`
 - Completes three-way handshake
 - Connection then torn down using RESET
 - Safer on more fragile systems
 - Can run with or without root or admin privileges



```
root@kali:~/Desktop# nmap -sT 192.168.1.38 -p 21-8080
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:52 EDT
Nmap scan report for 192.168.1.38
Host is up (0.00067s latency).
Not shown: 8053 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
4848/tcp  open  appserv-http
5985/tcp  open  wsman
8020/tcp  open  intu-ec-svcdisc
8027/tcp  open  unknown
8080/tcp  open  http-proxy
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 23.92 seconds
root@kali:~/Desktop#
```

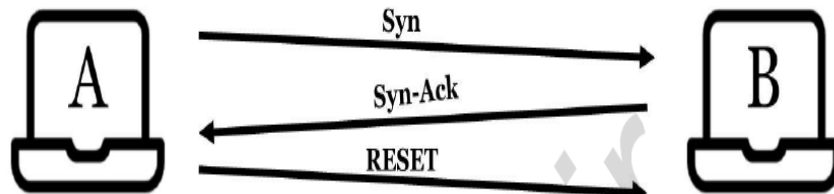

Port Scanning (4)

Nmap TCP Port Scan Types: SYN Scan

Nmap

- SYN scan (default or with **-sS**), also called "half-open" or "SYN Stealth" scan
 - SYN-ACK response = open
 - RST response = closed
 - No response = filtered
- Requires root privileges

The idea is that the handshake never completes so the connection won't be logged, but this activity is rare in a normal network and IPS/IDS/Firewalls are often tuned to detect this scan. Also, the half-open nature of the scan can cause issues on older or fragile systems.



```
root@kali:~/Desktop# nmap -sS 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:56 EDT
Nmap scan report for 192.168.1.38
Host is up (0.00026s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
4848/tcp  open  appserv-http
8080/tcp  open  http-proxy
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.14 seconds
root@kali:~/Desktop#
```

Flag in TCP Package

The flags in the TCP packet are 8 bits which can be set to 0 or 1:

CWR: if set to 1 it indicates that the source host has received a TCP segment with the ECE flag set to 1

ECE: if set to 1 it indicates that the host supports ECN during the 3-way handshake

URG: if set to 1 it indicates that urgent data is present in the stream

ACK: if set to 1 it indicates that the Acknowledgment number field is valid

PSH: if set to 1 it indicates that the incoming data must not be buffered but immediately passed to the upper levels of the application

RST: if set to 1 it indicates that the connection is not valid

SYN: if set to 1 it indicates that the sender host of the segment wants to open a TCP connection with the recipient host

FIN: if set to 1 it indicates that the sender host of the segment wants to close the open TCP connection with the recipient host

Port Scanning (5)

- ▶ **-sA** (Ack Scan): Set the "Ack" control bit inside the tcp package to 1
- ▶ **-sF** (Fin Scan): Set the "Fin" control bit inside the tcp package to 1
- ▶ **-sN** (Null Scan): Set all control bits to 0
- ▶ **-sX** (Xmas Tree Scan): Set the control bits Fin, Psh, Urg to 1
- ▶ **-sM** (Maimon Scan): Set the Fin and Ack bits to 1

```
(kali@kali)-[/usr/share/nmap]
$ sudo nmap -sA 192.168.1.254
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-09 05:53 EST
Nmap scan report for myfastgate.nexxt (192.168.1.254)
Host is up (0.00012s latency).
All 1000 scanned ports on myfastgate.nexxt (192.168.1.254) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

```
(kali@kali)-[/usr/share/nmap]
$ sudo nmap -sN 192.168.1.254
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-09 05:54 EST
Nmap scan report for myfastgate.nexxt (192.168.1.254)
Host is up (0.00079s latency).
All 1000 scanned ports on myfastgate.nexxt (192.168.1.254) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds
```


UDP Protocol

"User Datagram Protocol" is a data transmission protocol on the network.

Unlike TCP, UDP uses a transmission model with no assurance of data reliability, ordering, or integrity; therefore, UDP provides unreliable service and data packets can arrive in disorder, duplicate, or get lost in transmission.

UDP is used in those services that have such stringent timing requirements as to prefer communication with any missing data to a delay in communication (such as real-time systems).

Port Scanning (6)

► -sU (Udp Scan)

```
root@kali:~/Desktop# nmap -sU 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 19:26 EDT
Nmap scan report for 192.168.1.38
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.1.38 are open|filtered
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.13 seconds
```

OS Finger Print and Version Scan

- ▶ **-sV** (Version Scan): this is the command to search for the running service. Nmap contains a database of approximately 2,200 known services and associated ports. Examples of these services are HTTP (port 80), SMTP (port 25), DNS (port 53) and SSH (port 22)
- ▶ **-O** (OS Finger Printing): Scan and search for the operating system

```
root@kali:~/Desktop# nmap -O -sV 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:34 EDT
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.42% done; ETC: 18:36 (0:00:00 remaining)
Nmap scan report for 192.168.1.38
Host is up (0.00033s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
22/tcp    open  ssh          OpenSSH 7.1 (protocol 2.0)
4848/tcp  open  ssl/appserv-http?
8080/tcp  open  http         Sun GlassFish Open Source Edition 4.0
8383/tcp  open  ssl/http     Apache httpd
9200/tcp  open  wap-wsp?
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint :
in/submit.cgi?new-service :
SF-Port9200-TCP:V=7.80%I=7%D=5/25%Time=5ECC47FD%P=x86_64-pc-linux-gnu%r(Ge
```

OS Fingerprint and Version Scan (2)

- **-traceroute**: obtain the path followed by the packets on the computer networks, i.e. the IP address of each router crossed to reach the recipient.

```
C:\WINDOWS\system32>nmap -traceroute scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2021-02-24 17:01 Hora estándar Montañas (MÚxic
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.093s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
1025/tcp   filtered NFS-or-IIS
6129/tcp   filtered unknown
9929/tcp   open  nping-echo
31337/tcp  open  Elite

TRACEROUTE (using port 587/tcp)
HOP RTT      ADDRESS
1  57.00 ms  10.208.64.1
2  25.00 ms  10.0.16.62
3  25.00 ms  10.2.16.186
4  17.00 ms  10.0.81.182
5  18.00 ms  10.1.81.209
6  15.00 ms  10.0.81.169
7  17.00 ms  pe-lmm.megared.net.mx (189.199.117.145)
8  ...
9  28.00 ms  10.3.5.13
10 ... 11
12 39.00 ms  10.3.0.72
13 66.00 ms  201-174-24-209.transtelco.net (201.174.24.209)
14 70.00 ms  201-174-250-5.transtelco.net (201.174.250.5)
15 62.00 ms  201-174-250-75.transtelco.net (201.174.250.75)
16 80.00 ms  201-174-251-30.transtelco.net (201.174.251.30)
17 61.00 ms  ae7.cr7-dal3.ip4.gtt.net (208.116.218.89)
18 102.00 ms ae2.cr5-sjc1.ip4.gtt.net (89.149.180.26)
19 102.00 ms ip4.gtt.net (208.116.213.134)
20 90.00 ms  173.230.159.69
21 88.00 ms  scanme.nmap.org (45.33.32.156)

Nmap done: 1 IP address (1 host up) scanned in 28.67 seconds
```

OS Fingerprint and Version Scan (3)

- **-A:** It performs both the OS Fingerprint and the Version Detection and the traceroute.

```
(kali kali)~[~]
$ sudo nmap -A 192.168.1.254
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-07 05:28 EST
WARNING: Service 192.168.1.254:80 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
WARNING: Service 192.168.1.254:443 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
Nmap scan report for myfastgate.nexxt (192.168.1.254)
Host is up (0.0018s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
| dns-nsid:
|_ bind.version: dnsmasq-2.78
80/tcp    open  rtsp
fingerprint-strings:
  GetRequest:
    HTTP/1.0 302 Found
    Server:
    Date: Mon, 07 Feb 2022 10:29:06 GMT
    Cache-Control: no-cache,no-store,max-age=0
    Pragma: no-cache
    X-Frame-Options: DENY
    Expires: 0
    X-Content-Type-Options: nosniff
    X-XSS-Protection: 1; mode=block
    Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' api-cdn.amazon.com na.account.amazon.com
    Content-Language: en
    Location: /login.html
    Content-Type: text/html
    Connection: close
    <HTML>
    <HEAD><TITLE>302 Found</TITLE></HEAD>
    <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
    <H4>302 Found</H4>
    Moved Temporary.
  HTTPOptions:
    HTTP/1.0 501 Not Implemented
    Server:
```

Output

- ▶ **-oN** : Saves the NMAP command to an output file in the specified format
- ▶ **-oA**: Save the NMAP command in all possible output files. This option creates three output files

.gnmap

.nmap

.xml

```
root@EthicalHaks:~# nmap -oN outputfile.txt 192.168.0.12

Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-23 22:00 PDT
Nmap scan report for 192.168.0.12
Host is up (0.0000020s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

```
(kali@ kali)-[~]
$ sudo nmap -oA 192.168.1.250-255
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-11 10:56 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
```

```
(kali@ kali)-[~]
$ ls | grep "192.168*"
192.168.1.250-255.gnmap
192.168.1.250-255.nmap
192.168.1.250-255.xml

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

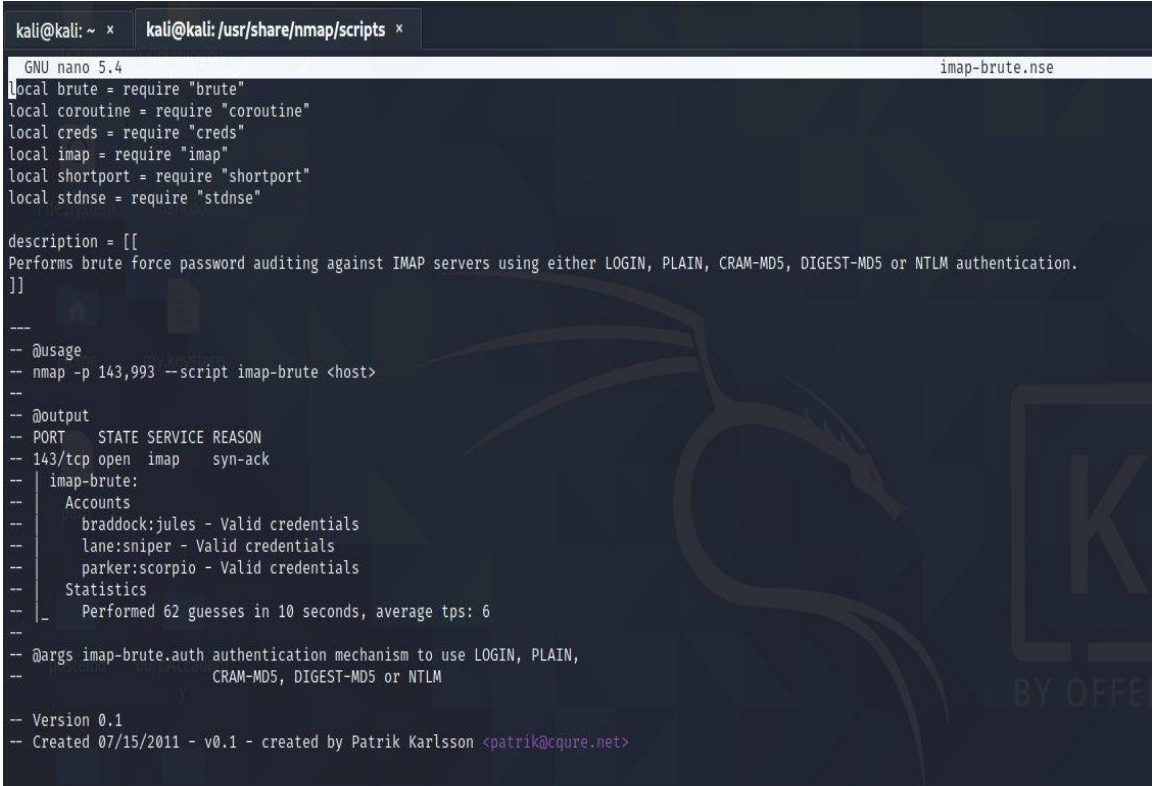
NSE

Nmap uses scripts that allow you to perform more advanced actions on the target host.

Scripts can be invoked via the command:

- ▶ **-sC**: Default category
- ▶ **--script**: Allows you to specify a specific script to use

All scripts are located in the `/usr/share/nmap/scripts` folder (the default ones). Other scripts can also be downloaded and used from external sources (e.g. GitHub)



```
kali@kali: ~ x  kali@kali: /usr/share/nmap/scripts x
GNU nano 5.4
imap-brute.nse
local brute = require "brute"
local coroutine = require "coroutine"
local creds = require "creds"
local imap = require "imap"
local shortport = require "shortport"
local stdnse = require "stdnse"

description = [[
Performs brute force password auditing against IMAP servers using either LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 or NTLM authentication.
]]

-- @usage
-- nmap -p 143,993 --script imap-brute <host>

-- @output
-- PORT      STATE SERVICE REASON
-- 143/tcp    open  imap    syn-ack
-- |imap-brute:
-- |  Accounts
-- |    braddock:jules - Valid credentials
-- |    lane:sniper - Valid credentials
-- |    parker:scorpio - Valid credentials
-- |  Statistics
-- |    Performed 62 guesses in 10 seconds, average tps: 6
-- |
-- @args imap-brute.auth authentication mechanism to use LOGIN, PLAIN,
--                        CRAM-MD5, DIGEST-MD5 or NTLM

-- Version 0.1
-- Created 07/15/2011 - v0.1 - created by Patrik Karlsson <patrik@cqure.net>
```


NSE (2)

--script ssl-enum-ciphers: This script checks what kind of ciphers are used by a target host

```
(kali@kali)~$ nmap -sV --script ssl-enum-ciphers -p 443 192.168.1.254
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-11 11:27 EST
WARNING: Service 192.168.1.254:443 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
Nmap scan report for myfastgate.nexxt (192.168.1.254)
Host is up (0.0064s latency).

PORT      STATE SERVICE VERSION
443/tcp   open  ssl/rtsp
|_ fingerprint-strings:
|_   GetRequest:
|_     HTTP/1.0 302 Found
|_     Server:
|_     Date: Fri, 11 Feb 2022 16:27:25 GMT
|_     Cache-Control: no-cache,no-store,max-age=0
|_     Pragma: no-cache
|_     X-Frame-Options: DENY
|_     Expires: 0
|_     X-Content-Type-Options: nosniff
|_     X-XSS-Protection: 1; mode=block
|_     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' api-cdn.amazon.com na.account.amazon.com
|_     Content-Language: en
|_     Location: /login.html
|_     Content-Type: text/html
|_     Connection: close
|_     <HTML>
|_     <HEAD><TITLE>302 Found</TITLE></HEAD>
|_     <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
|_     <H4>302 Found</H4>
|_     Moved Temporary.
|_   HTTPOptions:
|_     HTTP/1.0 501 Not Implemented
```


NSE (3)

There are some Nmap projects that have been developed by users and allow you to carry out Vulnerability Assessments on target hosts. Two of the most famous are Vulscan and Nmap-Vulners.

- ▶ github.com/scipag/vulscan
- ▶ github.com/vulnersCom/nmap-vulners

```
alexis@ubuntu:~$ sudo nmap -sV -p21-8080 --script vulners 192.168.1.217
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-08-11 03:48 EAT
Nmap scan report for 192.168.1.217
Host is up (0.00026s latency).
Not shown: 8036 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
|     CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778
|     CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906
|     CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708
|     CVE-2010-4755 4.0 https://vulners.com/cve/CVE-2010-4755
|     CVE-2008-5161 2.6 https://vulners.com/cve/CVE-2008-5161
|_
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
```

Sources

- ▶ <https://medium.com/nerd-for-tech/nmap-learn-the-essentials-7e4b5316dfa5>
- ▶ networkcomputing.com/networking/nmap-tutorial-common-commands/page/0/2
- ▶ <https://osric.com/chris/accidental-developer/2021/02/nmap-scans-the-top-1000-ports-by-default-but-which-1000/>
- ▶ medium.com/@songchai.d01/the-most-usefull-nmap-commands-examples-for-linux-c28604da5f2
- ▶ <https://medium.com/@dandobusiness/a-guide-to-ethical-hacking-understanding-nmap-7aea71f65554>
- ▶ <https://nmap.org/man/it/index.html>