How To Scan a Network With Nmap

How To Scan With Nmap

Nmap is a great tool to learn, the application have the ability to scan and map networks and much more, it is a great tool for everybody that works in IT.

It is the first tool i use when i want troubleshot, we can do regular ping or a ping sweeps that scans a range of the subnet or the whole subnet.

The application also offers host discovery, port discovery, operating system version discovery, MAC address, services, exploit and vulnerability detection.

Another great tool to use while learning nmap is Wireshark, It is highly recommended to run Wireshark wile using nmap, following the flow of network traffic will help you analyze and visuals the scans.

We will try some of the popular scanning method that can be used with nmap.

This guide is just meant to give you high level understanding on how to use the different scanning techniques.

Please don’t scan networks or host you are not authorized to do. The networks and hosts scanned in the guide is my home lab.

If you want a more in-depth explanation on how you can use nmap and the switches, i recommend that you read “The Official Nmap Project Guide to Network Discovery and Security Scanning”.

Save Output To Txt/Xml File

Description	Command	Example
Save output to file	nmap -oN [file.txt] [Target]	nmap -oN file.txt 192.168.100.11
Save output as XML	nmap -oX [file.xml] [Target]	nmap -oX file.xml192.168.100.11
Save in all formats	nmap -oA [file] [Target]	nmap -oA file 192.168.100.11

Basic Scanning

Description	Command	Example
Scan a single host	nmap [Target]	nmap 192.168.100.100
Scan multiple targets	nmap [Target1, Target2]	nmap 192.168.100.10,192.168.100.100
Scan a range of IP address	nmap [IP Range]	nmap 192.168.100.10-99
Scan a Class C subnet	nmap [IP/CDIR]	nmap 192.168.100.0/24
Resolve FQDN	nmap [FQDN]	nmap www.eaxmple.com

Quick Scans

Description	Command	Example
Ping scan	nmap -sP [Target]	nmap -sP 192.168.100.11
Ping Scan – disable port scanining	nmap -sn [Target]	nmap -sn 192.168.100.0/24

-sP switch can be used when you want to make a quick ping, the host or hosts will replay to ICMP ping packets.

```
nmap -sP 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:05 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
```

The **-sn** switch is used to to sweep a network without doing any port scans.

```
nmap -sn 192.168.100.0/24

Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-02 00:02 W. Europe Daylight Time
Nmap scan report for 192.168.100.1
Host is up (0.0010s latency).
Nmap scan report for srv1.online-it.nu (192.168.100.11)
Host is up (0.0020s latency).
Nmap scan report for 192.168.100.13
Host is up (0.0010s latency).
Nmap scan report for srv7.home.local (192.168.100.17)
Host is up (0.0011s latency).
Nmap scan report for 192.168.100.100
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 10.82 seconds
```

Banner Grabbing & Service Detection

Description	Command	Example
Detect OS	nmap -O [Target]	nmap -O 192.168.100.11
Detect OS & Services	nmap -A [Target]	nmap -A 192.168.100.11
Detect Services	nmap -sV [Target]	nmap -sV 192.168.100.11

The **-O** switch scans for operating system details. This type of scan can be used to identify the operating system of the scanned host and the services the host is running.

```
nmap -O 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:12 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.00032s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.96 seconds
```

Port Scans Types

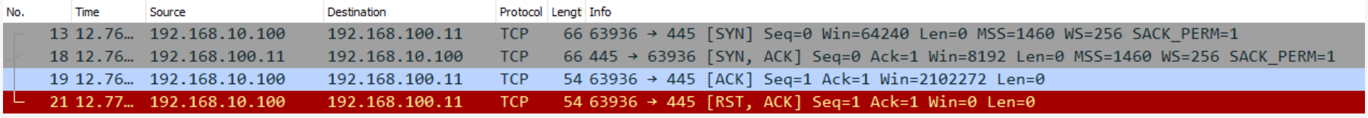
Description	Command	Example
Scan a single Port	nmap -p [Port] [Target]	nmap -p 80 192.168.100.11
Scan a range of ports	nmap -p [Port-Port] [Target]	nmap -p 20-99 192.168.100.11
Scan the first 100 ports	nmap -F [Port] [Target]	nmap -F 192.168.100.11
Scan using TCP Handshake	nmap -sT [Target]	nmap -sT 192.168.100.11
Scan using TCP SYN (Stealth)	nmap -sS [Target]	nmap -sS 192.168.100.11
Scan UDP port	nmap -sU [Target]	nmap -sU 192.168.100.11

The **-sT** switch creates a full TCP handshake with the target. This is considered more accurate than SYN scan but is slower and can be easy detected by firewalls and IDS.

```
nmap -sT 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:18 W. Europe Daylight Time

Nmap scan report for 192.168.100.11
Host is up (1.0s latency).
Not shown: 986 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
53/tcp   open     domain
88/tcp   open     kerberos-sec
110/tcp  filtered pop3
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
389/tcp  open     ldap
445/tcp  open     microsoft-ds
464/tcp  open     kpasswd5
593/tcp  open     http-rpc-epmap
636/tcp  open     ldapssl
3268/tcp open     globalcatLDAP
3269/tcp open     globalcatLDAPssl
3389/tcp open     ms-wbt-server
```

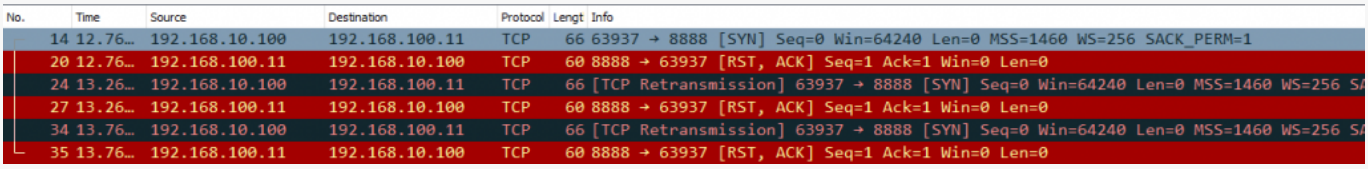
```
Nmap done: 1 IP address (1 host up) scanned in 219.83 seconds
```

Analysing the scan in wireshark we can see that the open port is responding to the handshake.



No.	Time	Source	Destination	Protocol	Lengt	Info
13	12.76…	192.168.10.100	192.168.100.11	TCP	66	63936 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	12.76…	192.168.100.11	192.168.10.100	TCP	66	445 → 63936 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	12.76…	192.168.10.100	192.168.100.11	TCP	54	63936 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
21	12.77…	192.168.10.100	192.168.100.11	TCP	54	63936 → 445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

If the port is closed on the host, then the target host will respond with a RST+ACK packets.



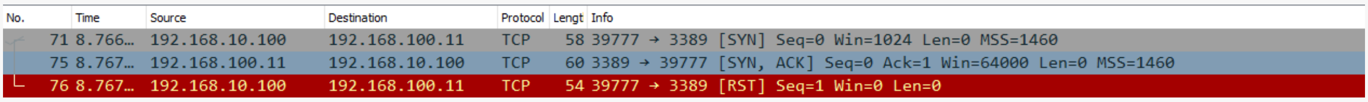
No.	Time	Source	Destination	Protocol	Lengt	Info
14	12.76…	192.168.10.100	192.168.100.11	TCP	66	63937 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	12.76…	192.168.100.11	192.168.10.100	TCP	60	8888 → 63937 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	13.26…	192.168.10.100	192.168.100.11	TCP	66	[TCP Retransmission] 63937 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
27	13.26…	192.168.100.11	192.168.10.100	TCP	60	8888 → 63937 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	13.76…	192.168.10.100	192.168.100.11	TCP	66	[TCP Retransmission] 63937 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
35	13.76…	192.168.100.11	192.168.10.100	TCP	60	8888 → 63937 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The **-sS** switch sends only a TCP SYN packet and waits for a TCP ACK. If it receives an ACK on the specific probed port then it response with a RST packet, in this way the scan can be undetected by the firewall. If the scanned port is closed on the target host, then target will only respond with a RST packet.

```
nmap -sS 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:24 W. Europe Daylight Time
Nmap scan report for 192.168.100.11

Host is up (0.0013s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
```

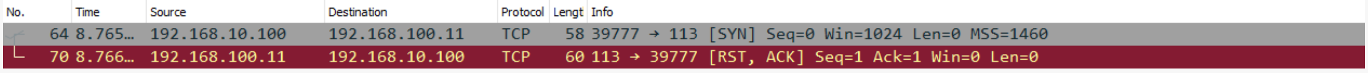
```
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.31 seconds
```

Analysing the packets in wireshark we can see that we first send a SYN packet to the scanned port on the target host, if it port is opened the target will response wit a SYN+ACK packet and we respond back with a RST packet.



No.	Time	Source	Destination	Protocol	Lengt	Info
71	8.766…	192.168.10.100	192.168.100.11	TCP	58	39777 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
75	8.767…	192.168.100.11	192.168.10.100	TCP	60	3389 → 39777 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
76	8.767…	192.168.10.100	192.168.100.11	TCP	54	39777 → 3389 [RST] Seq=1 Win=0 Len=0

If the port is closed on the scanned target the we will get a RST+ACK back.



No.	Time	Source	Destination	Protocol	Lengt	Info
64	8.765…	192.168.10.100	192.168.100.11	TCP	58	39777 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
70	8.766…	192.168.100.11	192.168.10.100	TCP	60	113 → 39777 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The **-sU** switch will scan after UDP ports, UDP is a connectionless protocol, UDP packets dose not have any ACK flag set, the UDP protocol don’t require the reviser to confirm that he revised a UDP packet.

If the there is a firewall enabled on the host or on the network you will get a response back “open|filtered ports” and a list of ports that are blocked by the firewall.

```
nmap -sU 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 19:58 W. Europe Daylight Time

Nmap scan report for 192.168.100.11
Host is up (0.0016s latency).
Not shown: 997 open|filtered ports
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
389/udp open  ldap
```

```
Nmap done: 1 IP address (1 host up) scanned in 17.27 seconds
```

If the firewall is disabled then they will be no response back.

Inverse Scans

Description	Command	Example
Xmas scan	nmap -sX [Target]	nmap -sX 192.168.100.11
FIN scan	nmap -sF [Target]	nmap -sF 192.168.100.11
TCP Null scan	nmap -sN [Target]	nmap -sN 192.168.100.11
ACK scan	nmap -sA [Target]	nmap -sA 192.168.100.11

The **-sX** switch is called a Xmas Scan, when you scan a network or a target host with Xmax scan, the xmas scan sends a packet that contains multiple flags, the packet contains the URG, PSH & FIN flags. If the host have closed ports, it will respond with a single RST packet. If the ports are open on the host, then the host will respond as an open ports. Modern operating systems, firewalls and IDS drops this kind of packets if they are properly configured.

We will run the xmax scan against a windows server with firewall enabled.

```
nmap -sX 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 17:07 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.100.11 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 27.62 seconds
```

Observe the line “All 1000 scanned ports on 192.168.100.11 are open|filtered” the output is showing that all scanned ports are “open|filtered”. This means that the firewall are enabled on the target host.

Lets try the same scan but this time we will disable the firewall on our target host.

```
nmap -sX 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 17:13 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.100.11 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
```

Now we get “All 1000 scanned ports on 192.168.100.11 are closed” this indicates that the firewall disabled.

The **-sF** switch scans the the host with a FIN scan, a FIN scan sends a packet with only the FIN flag set, this allows the packet to pass the firewall. If the port is open you will not get any respond, if the port is closed the target will respond with a RST packet.

When the firewall is enabled on the target the output will have a “open|filtered” response.

```
nmap -sF 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 17:51 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.100.11 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 27.19 seconds
```

If the firewall is disabled on the target the output will have a “are closed” response.

```
nmap -sF 192.168.100.11
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 18:06 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.100.11 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.29 seconds
```

The **-sN** switch will scan the target with a NULL scan, the scan sends a packet without any flags set. if the NULL packet is sent to an open port, the will be no response back. If the NULL packet is sent to a close port, it will respond with a RST packet. This type of scan is easy to detect due that there are no reason to send a TCP packet without a flag.

When using the NULL scan the target will respond similar to the FIN and Xmaz scans.

The **-sA** switch send a packet with the ACK flag set when scanning a host, when the target receive the ACK packet it will replay with a RST packet. if the port is closed and the firewall is enabled the firewall will block the target host response and there will be no response back.

Observe the output in namp when the firewall is enabled.

```
nmap -sA 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 19:36 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.100.11 are filtered

Nmap done: 1 IP address (1 host up) scanned in 27.58 seconds
```

If the firewall is enabled the “All 1000 scanned ports on 192.168.100.11 are filtered” line will comeback with the “**filtered**” value. The “filtered” response shows that a firewall is enabled in the system.

Running the same command against a target with a disabled firewall, the output will have a different value.

```
nmap -sA 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 19:39 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.100.11 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 7.23 seconds
```

The response back on the “All 1000 scanned ports on 192.168.100.11 are unfiltered” is coming back with the “unfiltered” value. The response back means that there are no firewall enabled on the target.

Firewall Evasion

Description	Command
Idle zombie scan	nmap -sI [zombie] [target]
Use a decoy	nmap -D RND: [number] [target]
Fragment packets	nmap -f [target]
Specify MTU	nmap –mtu [MTU] [target]
Randomize scan order	nmap –randomize-hosts [target]
Send bad checksums	nmap –badsum [target]
Specify source port	nmap –source-port [port] [target]
Spoof MAC Address	nmap –spoof-mac [MAC|0|vendor] [target]

The **-sI** is called a Idle scan or a zombie scan is a stealth technique, when using the a zombie scan packets revised on the scanned host cant be traced back the sender, all network traffic to the target host are going trough a second host on the network called “zombie”.

For a more detail explanation on how the idle scan work i recommend to read the official nmap documentation at https://nmap.org/book/idlescan.html

The **-f** switch is used to fragment probes into 8-byte packets, the scan will split the TCP header up to several packet, it is a very effective way to hide thee and make it harder for intrusion detection systems to the detect the scans.

The **-D** switch is used to hide port scans by using one or more decoys IP address,the network traffic on the scanned host will appear coming from the decoys IP address.

The **—source-port** switch is used to manually specify the source port number of a probe.

The **—-randomize-hosts** switch is used to randomize the scanning order of the specified ping sweep or a range scan.

Script Engines

Description	Command
Run script	nmap —script [script.nse] [target]
Run scripts	nmap —script [expression] [target
Run scripts by category	nmap —script [cat] [target]
Run multiple scripts categories	nmap —script [cat1,cat2,cat3] [target]
Update script database	nmap —script-updatedb
Script categories	all
	discovery
	default
	auth
	external
	malware

Description	Command
	vuln intrusive safe

Useful scans

Find Information about IP address

```
nmap --script=asn-query,whois,ip-geolocation-maxmind [target]
```

Detect Heart bleed SSL vulnerability

```
nmap -sV -p 443 --script=ssl-heartbleed [target]
```

Scan for DDOS reflection UDP services

```
nmap –sU –A –PN –n –pU:19,53,123,161 –script=ntp-monlist,dns-recursion,snmp-sysdescr [target]
```

Scan HTTP Service

Get page titles

```
nmap --script=http-title [target]
```

Get HTTP headers

```
nmap --script=http-headers [target]
```

Recommended sites

https://highon.coffee/blog/nmap-cheat-sheet/

Conclusion

We have looked into some of the scanning techniques we can use with nmap.

Check out the Ethical Hacking notes for more Kali Linux quick guides.