



## 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 troubleshoot, 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 while 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	<code>nmap -oN [file.txt] [Target]</code>	<code>nmap -oN file.txt 192.168.100.11</code>
Save output as XML	<code>nmap -oX [file.xml] [Target]</code>	<code>nmap -oX file.xml 192.168.100.11</code>
Save in all formats	<code>nmap -oA [file] [Target]</code>	<code>nmap -oA file 192.168.100.11</code>

### Basic Scanning

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

## Quick Scans

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

**-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	<code>nmap -O [Target]</code>	<code>nmap -O 192.168.100.11</code>
Detect OS & Services	<code>nmap -A [Target]</code>	<code>nmap -A 192.168.100.11</code>
Detect Services	<code>nmap -sV [Target]</code>	<code>nmap -sV 192.168.100.11</code>

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

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 easily 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	Length	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	Length	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 SACK_PERM=1
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 SACK_PERM=1
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 responds 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 the 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 with a SYN+ACK packet and we respond back with a RST packet.

No.	Time	Source	Destination	Protocol	Length	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 then we will get a RST+ACK back.

No.	Time	Source	Destination	Protocol	Length	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 do not have any ACK flag set, the UDP protocol doesn't require the receiver to confirm that he received a UDP packet.

If 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	<code>nmap -sX [Target]</code>	<code>nmap -sX 192.168.100.11</code>
FIN scan	<code>nmap -sF [Target]</code>	<code>nmap -sF 192.168.100.11</code>
TCP Null scan	<code>nmap -sN [Target]</code>	<code>nmap -sN 192.168.100.11</code>
ACK scan	<code>nmap -sA [Target]</code>	<code>nmap -sA 192.168.100.11</code>

The `-sX` switch is called a Xmas Scan, when you scan a network or a target host with Xmas 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 xmas 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, there will be no response back. If the NULL packet is sent to a closed port, it will respond with a RST packet. This type of scan is easy to detect due to the fact that there is no reason to send a TCP packet without a flag.

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

The **-sA** switch sends a packet with the ACK flag set when scanning a host, when the target receives the ACK packet it will reply 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 nmap 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 come back 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	<code>nmap -sI [zombie] [target]</code>
Use a decoy	<code>nmap -D RND: [number] [target]</code>
Fragment packets	<code>nmap -f [target]</code>
Specify MTU	<code>nmap -mtu [MTU] [target]</code>
Randomize scan order	<code>nmap --randomize-hosts [target]</code>
Send bad checksums	<code>nmap --badsum [target]</code>
Specify source port	<code>nmap --source-port [port] [target]</code>
Spoof MAC Address	<code>nmap --spooof-mac [MAC 0 vendor] [target]</code>

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	<code>nmap --script [script.nse] [target]</code>
Run scripts	<code>nmap --script [expression] [target]</code>
Run scripts by category	<code>nmap --script [cat] [target]</code>
Run multiple scripts categories	<code>nmap --script [cat1,cat2,cat3] [target]</code>
Update script database	<code>nmap --script-updatedb</code>
<b>Script categories</b>	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.