Nmap Security Scanning Lab

Target Specification

Switch	Example	Description
	nmap 192.168.1.1	Scan a single IP
	nmap 192.168.1.1 192.168.2.1	Scan specific IPs
	nmap 192.168.1.1-254	Scan a range
	nmap scanme.nmap.org	Scan a domain
	nmap 192.168.1.0/24	Scan using CIDR notation
-iL	nmap -iL targets.txt	Scan targets from a file
-iR	nmap -iR 100	Scan 100 random hosts
--exclude	nmap --exclude 192.168.1.1	Exclude listed hosts

Scan Techniques

Switch	Example	Description
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Host Discovery

Switch	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning. Host discovery only.
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only.
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x.

Switch	Example	Description
		Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Port Specification

Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-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-	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
--top-ports	nmap 192.168.1.1 --top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535

Service and Version Detection

Switch	Example	Description
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port
-sV --version-intensity	nmap 192.168.1.1 -sV --version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness
-sV --version-light	nmap 192.168.1.1 -sV --version-light	Enable light mode. Lower possibility of correctness. Faster
-sV --version-all	nmap 192.168.1.1 -sV --version-all	Enable intensity level 9. Higher possibility of correctness. Slower
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

OS Detection

Switch	Example	Description
-O	nmap 192.168.1.1 -O	Remote OS detection using TCP/IP stack fingerprinting
-O --osscan-limit	nmap 192.168.1.1 -O --osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O --osscan-guess	nmap 192.168.1.1 -O --osscan-guess	Makes Nmap guess more aggressively
-O --max-os-tries	nmap 192.168.1.1 -O --max-os-tries 1	Set the maximum number x of OS detection tries against a target
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

Timing and Performance

Switch	Example	Description
-T0	nmap 192.168.1.1 -T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 -T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 -T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources

Switch	Example	Description
-T3	nmap 192.168.1.1 -T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 -T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 -T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

Switch	Example input	Description
--host-timeout <time>	1s; 4m; 2h	Give up on target after this long
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	1s; 4m; 2h	Specifies probe round trip time
--min-hostgroup/max-hostgroup <size<size>	50; 1024	Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>	10; 1	Probe parallelization
--scan-delay/--max-scan-delay <time>	20ms; 2s; 4m; 5h	Adjust delay between probes
--max-retries <tries>	3	Specify the maximum number of port scan probe retransmissions
--min-rate <number>	100	Send packets no slower than <numberr> per second
--max-rate <number>	100	Send packets no faster than <number> per second

NSE Scripts

Switch	Example	Description
-sC	nmap 192.168.1.1 -sC	Scan with default NSE scripts. Considered useful for discovery and safe

Switch	Example	Description
--script default	nmap 192.168.1.1 --script default	Scan with default NSE scripts. Considered useful for discovery and safe
--script	nmap 192.168.1.1 --script=banner	Scan with a single script. Example banner
--script	nmap 192.168.1.1 --script=http*	Scan with a wildcard. Example http
--script	nmap 192.168.1.1 --script=http,banner	Scan with two scripts. Example http and banner
--script	nmap 192.168.1.1 --script "not intrusive"	Scan default, but remove intrusive scripts
--script-args	nmap --script snmp-sysdescr --script-args snmpcommunity=admin 192.168.1.1	NSE scri

Useful NSE Script Examples

Command	Description
nmap -Pn --script=http-sitemap-generator scanme.nmap.org	http site map generator
nmap -n -Pn -p 80 --open -sV -vvv --script banner,http-title -iR 1000	Fast search for random web servers
nmap -Pn --script=dns-brute domain.com	Brute forces DNS hostnames guessing subdomains
nmap -n -Pn -vv -O -sV --script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1	Safe SMB scripts to run
nmap --script whois* domain.com	Whois query
nmap -p80 --script http-unsafe-output-escaping scanme.nmap.org	Detect cross site scripting vulnerabilities
nmap -p80 --script http-sql-injection scanme.nmap.org	Check for SQL injections

Firewall / IDS Evasion and Spoofing

Switch	Example	Description
-f	nmap 192.168.1.1 -f	Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
--mtu	nmap 192.168.1.1 --mtu 32	Set your own offset size
-D	nmap -D 192.168.1.101,192.168.1.102, 192.168.1.103,192.168.1.23 192.168.1.1	Send scans from spoofed IPs
-D	nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	Above example explained
-S	nmap -S www.microsoft.com www.facebook.com	Scan Facebook from Microsoft (-e eth0 -Pn may be required)
-g	nmap -g 53 192.168.1.1	Use given source port number
--proxies	nmap --proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	Relay connections through HTTP/SOCKS4 proxies
--data-length	nmap --data-length 200 192.168.1.1	Appends random data to sent packets

Example IDS Evasion command

```
nmap -f -t 0 -n -Pn –data-length 200 -D
 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1
```

Output

Switch	Example	Description
-oN	nmap 192.168.1.1 -oN normal.file	Normal output to the file normal.file
-oX	nmap 192.168.1.1 -oX xml.file	XML output to the file xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Grepable output to the file grep.file
-oA	nmap 192.168.1.1 -oA results	Output in the three major formats at once

Switch	Example	Description
-oG -	nmap 192.168.1.1 -oG -	Grepable output to screen. -oN -, -oX - also usable
--append-output	nmap 192.168.1.1 -oN file.file --append-output	Append a scan to a previous scan file
-v	nmap 192.168.1.1 -v	Increase the verbosity level (use -vv or more for greater effect)
-d	nmap 192.168.1.1 -d	Increase debugging level (use -dd or more for greater effect)
--reason	nmap 192.168.1.1 --reason	Display the reason a port is in a particular state, same output as -vv
--open	nmap 192.168.1.1 --open	Only show open (or possibly open) ports
--packet-trace	nmap 192.168.1.1 -T4 --packet-trace	Show all packets sent and received
--iflist	nmap --iflist	Shows the host interfaces and routes
--resume	nmap --resume results.file	Resume a scan

Helpful Nmap Output examples

Command	Description
nmap -p80 -sV -oG - --open 192.168.1.1/24 | grep open	Scan for web servers and grep to show which IPs are running web servers
nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 > live-hosts.txt	Generate a list of the IPs of live hosts
nmap -iR 10 -n -oX out2.xml | grep "Nmap" | cut -d " " -f5 >> live-hosts.txt	Append IP to the list of live hosts

Command	Description
ndiff scanl.xml scan2.xml	Compare output from nmap using the ndif
xsltproc nmap.xml -o nmap.html	Convert nmap xml files to html files
grep " open " results.nmap | sed -r 's/ +/ /g' | sort | uniq -c | sort -rn | less	Reverse sorted list of how often ports turn up

Miscellaneous Options

Switch	Example	Description
-6	nmap -6 2607:f0d0:1002:51::4	Enable IPv6 scanning
-h	nmap -h	nmap help screen

Other Useful Nmap Commands

Command	Description
nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn	Discovery only on ports x, no port scan
nmap 192.168.1.1-1/24 -PR -sn -vv	Arp discovery only on local network, no port scan
nmap -iR 10 -sn -traceroute	Traceroute to random targets, no port scan
nmap 192.168.1.1-50 -sL --dns-server 192.168.1.1	Query the Internal DNS for hosts, list targets only

Source: https://www.stationx.net/nmap-cheat-sheet

Basic Scan:

```
┌──(mahedi㉿kali)-[~]
└─$ nmap  192.168.10.1-10
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:30 +06
Illegal character(s) in hostname -- replacing with '*'
Illegal character(s) in hostname -- replacing with '*'
Nmap scan report for dlinkrouter.*null* (192.168.10.1)
Host is up (0.015s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
2601/tcp  open  zebra
```

```
2602/tcp  open  ripd
5431/tcp  open  park-agent
49152/tcp open  unknown

Nmap done: 10 IP addresses (1 host up) scanned in 6.04 seconds
```

```
┌──(mahedi㉿kali)-[~]
└─$ nmap  192.168.10.1-255
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:30 +06
Illegal character(s) in hostname -- replacing with '*'
Illegal character(s) in hostname -- replacing with '*'
Nmap scan report for dlinkrouter.*null* (192.168.10.1)
Host is up (0.023s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
2601/tcp  open  zebra
2602/tcp  open  ripd
5431/tcp  open  park-agent
49152/tcp open  unknown

Nmap done: 255 IP addresses (1 host up) scanned in 61.12 seconds
```

```
┌──(mahedi㉿kali)-[~]
└─$ nmap  192.168.56.1-20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:32 +06
Nmap scan report for 192.168.56.5
Host is up (0.00055s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 20 IP addresses (1 host up) scanned in 1.82 seconds
```

TCP SYN Scan (-sS)

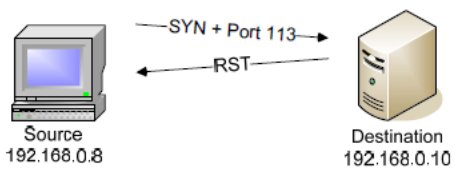
Requires Privileged Access: YES

Identifies TCP Ports: YES

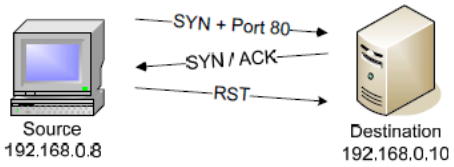
Identifies UDP Ports: NO

TCP SYN Scan Operation

Most of the ports queried during the TCP SYN scan will probably be closed. These closed port responses to the TCP SYN frame will be met with a RST frame from the destination station.



If nmap receives an acknowledgment to a SYN request, then the port is open. Nmap then sends an RST to reset the session, and the handshake is never completed.




```
┌──(mahedi㉿kali)-[~]
└─$ nmap -sS -v scan.nmap.org
You requested a scan type which requires root privileges.
QUITTING!
```

```
┌──(mahedi㉿kali)-[~]
└─$ sudo nmap -sS scan.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:26 +06
Nmap scan report for scan.nmap.org (45.33.49.119)
Host is up (0.043s latency).
Other addresses for scan.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
Not shown: 993 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
25/tcp    open   smtp
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 49.94 seconds
```

TCP connect() Scan (-sT)

Requires Privileged Access: NO

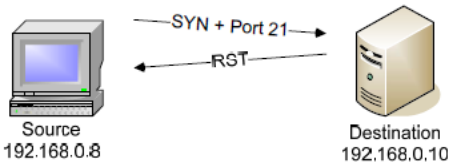
Identifies TCP Ports: YES

Identifies UDP Ports: NO

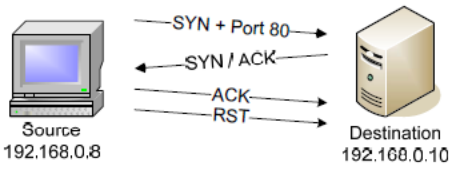
The TCP connect() scan is named after the connect() call that's used by the operating system to initiate a TCP connection to a remote device. Unlike the TCP SYN scan (-sS), the TCP connect() scan uses a normal TCP connection to determine if a port is available. This scan method uses the same TCP handshake connection that every other TCP-based application uses on the network.

TCP connect() Scan Operation

The TCP connect() scan to a closed port looks exactly like the TCP SYN scan:



A scan to an open port results in a different traffic pattern than the TCP SYN scan:




```
┌──(mahedi㉿kali)-[~]
└─$ nmap -sT -v scan.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:39 +06
Initiating Ping Scan at 01:39
Scanning scan.nmap.org (45.33.49.119) [2 ports]
Completed Ping Scan at 01:39, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:39
Completed Parallel DNS resolution of 1 host. at 01:39, 0.01s elapsed
Initiating Connect Scan at 01:39
Scanning scan.nmap.org (45.33.49.119) [1000 ports]
Discovered open port 25/tcp on 45.33.49.119
Discovered open port 22/tcp on 45.33.49.119
Discovered open port 443/tcp on 45.33.49.119
Discovered open port 80/tcp on 45.33.49.119
Completed Connect Scan at 01:40, 13.92s elapsed (1000 total ports)
Nmap scan report for scan.nmap.org (45.33.49.119)
Host is up (0.26s latency).
Other addresses for scan.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
Not shown: 996 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.67 seconds
```

When to use the TCP connect() Scan

Because this scan is so obvious when browsing through the application event logs, it might be considered the TCP scan of last resort. If privileged access isn't available and determination of open TCP ports is absolutely necessary, however, this scan may be the only method available.

Stealth Scanning – The FIN Scan (-sF), Xmas Tree Scan (-sX), and Null Scan (-sN)

Requires Privileged Access: YES

Identifies TCP Ports: YES

Identifies UDP Ports: NO

These three scans are grouped together because their individual functionality is very similar. These are called "stealth" scans because they send a single frame to a TCP port without any TCP handshaking or additional packet transfers. This is a scan type that sends a single frame with the expectation of a single response.

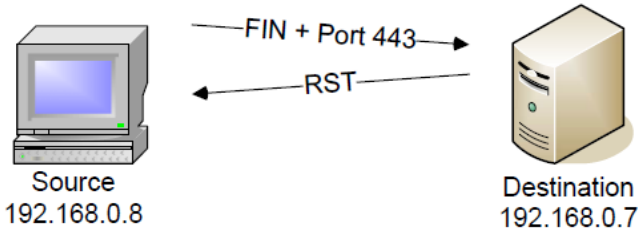
FIN, Xmas Tree, and Null Scan Operation

In the following examples, the graphical descriptions and trace files for the open and closed ports will look functionally identical, except that the bits in the TCP flags will be different in each scan type.

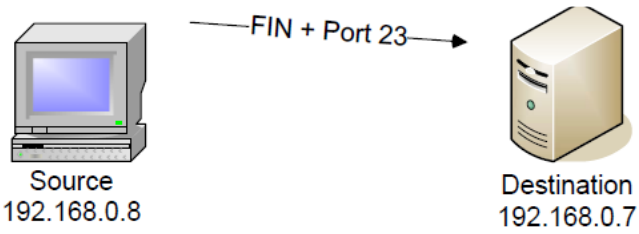
The FIN Scan (-sF)

The FIN scan's "they stealth" frames are unusual because are sent to a device without first going through the normal TCP handshaking. If a TCP session isn't active, the session certainly can't be formally closed!

In this FIN scan, TCP port 443 is closed so the remote station sends a RST frame response to the FIN packet:



If a port is open on a remote device, no response is received to the FIN scan:



The nmap output shows the open ports located with the FIN scan:

```
┌──(mahedi㉿kali)-[~]
└─$ sudo nmap -sF -v scan.nmap.org
[sudo] password for mahedi:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:52 +06
Initiating Ping Scan at 01:52
Scanning scan.nmap.org (45.33.49.119) [4 ports]
Completed Ping Scan at 01:52, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:52
Completed Parallel DNS resolution of 1 host. at 01:52, 0.01s elapsed
Initiating FIN Scan at 01:52
Scanning scan.nmap.org (45.33.49.119) [1000 ports]
Completed FIN Scan at 01:52, 0.19s elapsed (1000 total ports)
Nmap scan report for scan.nmap.org (45.33.49.119)
Host is up (0.0019s latency).
Other addresses for scan.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
rDNS record for 45.33.49.119: nmap.org
All 1000 scanned ports on scan.nmap.org (45.33.49.119) are closed
```

```
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
           Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
```

```
┌──(mahedi㉿kali)-[~]
└─$ sudo nmap -sF 192.168.56.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:54 +06
Nmap scan report for 192.168.56.5
Host is up (0.000018s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```