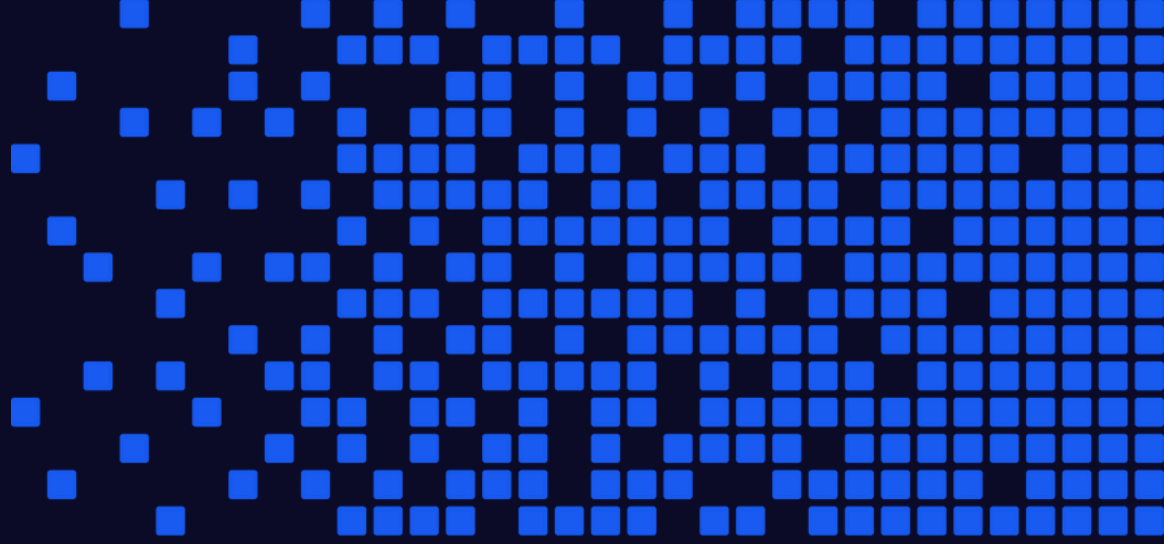


</CODE4>

Cybersecurity Analysis



**NMAP**



**CHEAT SHEET**

[WWW.CODE4CYBERSECURITY.COM](http://WWW.CODE4CYBERSECURITY.COM)

## TARGET SPECIFICATION

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

## SCAN TECHNIQUES

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

## HOST DISCOVERY

Switch	Example	Description
<code>-sL</code>	<code>nmap 192.168.1.1-3 -sL</code>	No Scan. List targets only
<code>-sn</code>	<code>nmap 192.168.1.1/24 -sn</code>	Disable port scanning
<code>-Pn</code>	<code>nmap 192.168.1.1-5 -Pn</code>	Disable host discovery. Port scan only
<code>-PS</code>	<code>nmap 192.168.1.1-5 -PS22-25,80</code>	TCP SYN discovery on port x. Port 80 by default
<code>-PA</code>	<code>nmap 192.168.1.1-5 -PA22-25,80</code>	TCP ACK discovery on port x. Port 80 by default
<code>-PU</code>	<code>nmap 192.168.1.1-5 -PU53</code>	UDP discovery on port x. Port 40125 by default
<code>-PR</code>	<code>nmap 192.168.1.1-1/24 -PR</code>	ARP discovery on local network
<code>-n</code>	<code>nmap 192.168.1.1 -n</code>	Never do DNS resolution

## PORT SPECIFICATION

Switch	Example	Description
<code>-p</code>	<code>nmap 192.168.1.1 -p 21</code>	Port scan for port x
<code>-p</code>	<code>nmap 192.168.1.1 -p 21-100</code>	Port range
<code>-p</code>	<code>nmap 192.168.1.1 -p U:53,T:21-25,80</code>	Port scan multiple TCP and UDP ports
<code>-p-</code>	<code>nmap 192.168.1.1 -p-</code>	Port scan all ports
<code>-p</code>	<code>nmap 192.168.1.1 -p http,https</code>	Port scan from service name
<code>-F</code>	<code>nmap 192.168.1.1 -F</code>	Fast port scan (100 ports)
<code>--top-ports</code>	<code>nmap 192.168.1.1 --top-ports 2000</code>	Port scan the top x ports
<code>-p-65535</code>	<code>nmap 192.168.1.1 -p-65535</code>	Leaving off initial port in range makes the scan start at port 1
<code>-p0-</code>	<code>nmap 192.168.1.1 -p0-</code>	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

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
-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>	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 <number> 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
--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 script with arguments

### 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
-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
ndiff scan1.xml scan2.xml	Compare output from nmap using the ndiff
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