Ethical Hacking and Countermeasures
Nmap Cheat Sheet

EC-Council
Building A Culture Of Security

Nmap
Source: https://nmap.org

Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their specific needs.

Syntax

```
nmap [Scan Type...]
[Options] {Target
specification}
```

1.Nmap Options
2.Nmap Port Scan types
3.Nmap Commands

Nmap Options

Option (Switch/ Syntax)	Description
Target Specification	
`-iL <inputfilename>`	Input from list of hosts/networks
`-iR <num hosts>`	Choose random targets/ Scan random hosts nmap -iR [number]
`--exclude <host1[,host2][,host3],...>`	Exclude single or multiple hosts/networks
`--excludefile <exclude_file>`	Exclude list from file

Host Discovery

`-sL`	List Scan - simply lists targets nmap <Target IP>-3 -sL
`-sn`	Ping Scan - disable port scan for discovering hostnmap <Target IP>/24 -sn
`-Pn`	Treat all hosts as online -- skip host discovery nmap <Target IP>-5 -Pn
`-PS/PA/PU/PY[portlist]`	TCP SYN/ACK, UDP or SCTP INIT discovery to given ports
`-PE/PP/PM`	ICMP echo, timestamp, and netmask request discovery probes
`-PP`	Use ICMP timestamp request
`-PO[protocol list]`	IP Protocol Ping
`-n/-R`	Never do DNS resolution/Always resolve [default: sometimes] nmap –n <Target IP> nmap –R <Target IP>
`--dns-servers <serv1[,serv2],...>`	Immediate mode, display things as we find them
`--system-dns`	A string representing the intended sequence ignorance level
`--traceroute`	Path to a file where flat text will be dumped that normally would go to the users terminal
`-PR`	Numeric value representing the number of seconds to wait before declaring the scan over

Scan Techniques

`-sS/sT/sA/sW/sM`	TCP SYN/Connect()/ACK/Window/Maimon scans
`-sU`	UDP Scan nmap -sU -v <Target IP>
	UDP port scan nmap <Target IP> -sU
`-sN/sF/sX`	TCP Null, FIN, and Xmas scans
`scanflags=value –sA`	TCP ACK scan nmap –scanflags=value –sA <Target IP>
`–scanflags`	TCP scan flags nmap –-scanflags <Target IP>
`-Sp`	Ping scan nmap -Sp <Target IP>
`--scanflags <flags>`	Customize TCP scan flags
`-sI <zombie host[:probeport]>`	Idle zombie scan nmap –sI zombie <Target IP>
`-sY/sZ`	SCTP INIT scan nmap -sY -v <Target IP> SCTP COOKIE-ECHO scan nmap -sZ -v <Target IP>
`-sO`	IP protocol scan nmap –sO <Target IP>
`-b <FTP relay host>`	FTP bounce scan
`–send-eth`	Send raw ethernet packets nmap –send-eth <Target IP>
`–send-ip`	Send IP packets nmap –send-ip <Target IP>

Port Specification and Scan Order

`-p <port ranges>`	Only scan specified range ports nmap -p 1-100 <Target IP> e.g. -p80,443 or -p1–65535
`-p-`	Port scans all 1-65535 ports nmap <Target IP> -p-
`-p <protocol>`	Port scan from specified protocols nmap -smtp,https <Target IP>
`-F`	Fast mode - Scan less ports than the default scan (scan 100 most common ports) nmap <Target IP> -F
`-r`	Scan ports consecutively – do not randomize
`–randomize-hosts`	Randomize target host order nmap –randomize-hosts <Target IP>
`-p<port1>,<port2>,...`	Port list

`-p<port1>-<port2>`	Port range
`-P "*"`	Scan port using name nmap -p "*" ftp <Target IP>
`-pU:53,U:110,T20-445`	Mix TCP and UDP
`--top-ports <number>`	Scan <number> most common ports
`--port-ratio <ratio>`	Scan ports more common than <ratio>
`-p-65535`	Leaving off initial port in range makes Nmap scan start at port 1 nmap <Target IP> -p-65535 Leaving off initial port in range makes the scan start at port 1 nmap -p-65535 <Target IP>
`-p0-`	Leaving off end port in range makes Nmap scan through port 65535 nmap <Target IP> -p0- nmap -p0- <Target IP>

Service/Version Detection

`sV`	Probe open ports to determine service/version info nmap <Target IP> -sV
`--version-intensity <level>`	Set from 0 (light) to 9 (try all probes)
`--version-light`	Limit to most likely probes (intensity 2)
`--version-all`	Try every single probe (intensity 9)
`--version-trace`	Show detailed version scan activity (for debugging)

Script Scan

`--script=<ScriptName>|<ScriptCategory>|<ScriptDir>...`	Run individual or group of scripts
`--script=<Lua scripts>`	<Lua scripts> is a comma separated list of directories, script-files or script-categories
`--script-trace`	Show all data sent and received
`--script-updatedb`	Update the script database. nmap –script-updatedb
`--script-help`	“Lua scripts” = Show help about scripts

C|EH Certified Ethical Hacker

Ethical Hacking and Countermeasures
Nmap Cheat Sheet

EC-Council
Building A Culture Of Security

Nmap
Source: https://nmap.org

Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their specific needs.

Syntax

```
nmap [Scan Type...]
[Options] {Target
specification}
```

```
1.Nmap Options
2.Nmap Port Scan types
3.Nmap Commands
```

Nmap Options

Option (Switch/ Syntax)	Description
OS Detection	
`-O`	Enable OS detection/ OS Discovery using Nmap and Unicornscan/ Remote OS Detection using TCP/IP stack fingerprinting nmap -O <Target IP>
`--osscan-limit`	Limit OS detection to promising targets
`--osscan-guess`	Guess OS more aggressively
`--max-os-tries`	Set the maximum number x of OS detection tries against a target

Timing and Performance

`-T<0-5>`	Set timing template (higher is faster)
`-ttl [time]`	Set the packet TTL nmap –ttl [time] <Target IP> nmap <Target IP>/24 -sn
`--min-hostgroup/max-hostgroup <size>`	Parallel host scan group sizes
`--min-parallelism/max-parallelism <numprobes>`	Probe parallelization
`--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>`	Specifies probe round trip time
`--max-retries <tries>`	Caps number of port scan probe retransmissions
`--host-timeout <time>`	Give up on target after this long
`--scan-delay/--max-scan-delay <time>`	Adjust delay between probes
`--min-rate <number>`	Send packets no slower than <number> per second
`--max-rate <number>`	Send packets no faster than <number> per second
`-defeat-rst-ratelimit`	Defeat reset rate limits nmap –defeat-rst-ratelimit <Target IP>

Firewall/IDS Evasion and Spoofing

`-f; --mtu <val>`	Fragment packets (optionally w/given MTU)
`-D <decoy1,decoy2[,ME],...>`	Cloak a scan with decoys
`-S <IP_Address>`	Spoof source address
`-e <iface>`	Use given port number
`-g/--source-port <portnum>`	Append random data to send packets nmap –data-length [size] <Target IP>
`--data-length <num>`	Send packets with specified IP options
`--ip-options <options>`	Set IP time-to-live field
`--ttl <val>`	Spoof your MAC address nmap –spoof-mac [MAC|0|vendor] <Target IP>
`--spoof-mac <mac address/prefix/vendor name>`	Idle zombie scan nmap –sI zombie <Target IP>
`--badsum`	Send packets with a bogus TCP/UDP/SCTP checksum
`--proxies url1,[url2],...`	Relay connections through HTTP/SOCKS4 proxies

OUTPUT

`-oN/-oX/-oS/-oG <file>`	Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename
`-oA <basename>`	Output in the three major formats at once
`-v`	Increase verbosity level (use -vv or more for greater effect) nmap -v <Target IP>
`-d`	Increase debugging level (use -dd or more for greater effect) nmap -d <Target IPs>
`--reason`	Display the reason a port is in a particular state
`--open`	Only show open (or possibly open) ports nmap –open <Target IP>
`--packet-trace`	Show all packets sent and received nmap –packet-trace <Target IP>
`--iflist`	Print host interfaces and routes (for debugging) nmap –iflist
`--log-errors`	Log errors/warnings to the normal-format output file
`--append-output`	Append to rather than clobber specified output files
`--resume <filename>`	Resume an aborted scan

`--stylesheet <path/URL>`	XSL stylesheet to transform XML output to HTML
`--webxml`	Reference stylesheet from Nmap.Org for more portable XML
`--no-stylesheet`	revent associating of XSL stylesheet w/XML output
`-stats-every [time]`	Periodically display statistics nmap –stats-every [time] <Target IP>

Miscellaneous Options

`-h`	Nmap help screen nmap -h
`-6`	IPv6 Scanning by using -6 option in Zenmap nmap -6 scanme.nmap.org Enable IPv6 scanning
	nmap -6 2607:f0d0:1002:51::4 OS discovery using IPv6 fingerprinting method nmap -6 -O <Target IP>
`-A`	Enables OS detection, version detection, script scanning, and traceroute, also known as Aggressive scan
`-n`	Disable reverse IP address lookups
`--datadir <dirname>`	Specify custom Nmap data file location
`--send-eth/--send-ip`	Send using raw ethernet frames or IP packets
`--privileged`	Assume that the user is fully privileged
`-V`	Display Nmap version nmap -V
`--unprivileged`	Assume the user lacks raw socket privileges

Nmap

Source: https://nmap.org

Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their specific needs.

Syntax	
`nmap [Scan Type...] [Options] {Target specification}`	1.Nmap Options 2.Nmap Port Scan types 3.Nmap Commands

2.Nmap Port Scan types

Command	Description
`nmap -sT <Target IP>`	Connect Scan (Default without root privileges)/ Scan using TCP connect
`nmap -sS <Target IP>`	Scan using TCP SYN scan (default)
`nmap -Su <Target IP>`	UDP Scan
`nmap -sA <Target IP>`	ACK Scan
`nmap -Sw <Target IP>`	Window Scan
`nmap -sM <Target IP>`	Maimon Scan
`nmap -sL <Target IP>`	No Scan, list targets only
`nmap -sL -v <Target IP>`	List scan
`nmap -Pn <Target IP>`	Disable host discovery, port scanning
`nmap -PSx <Target IP>`	SYN Discovery on port x, port 80 by default
`nmap -PUx <Target IP>`	UDP discovery on port x, port 40125 by default
`nmap -PAx <Target IP>`	ACK discovery on port x, port 80 by default
`nmap -PR <Target IP>/24`	ARP discovery on local network
`--mnmap -n <Target IP>`	Never do DNS resolution
`nmap -p x <Target IP>`	Scan for port x
`nmap -p 21-50 <Target IP>`	Port Range
`nmap -p U:53,T:21-25,80`	Scan multiple TCP and UDP ports

Command	Description
`nmap -p- <Target IP>`	Scan all ports
`nmap -p http,ftp <Target IP>`	Port scan from service name
`nmap -F <Target IP>`	Fast port scan (100 ports)
`nmap -f <Target IP>`	Scan fragmented IP packets
`nmap --mtu x <Target IP>`	Set own offset size x
`nmap --top-ports x <Target IP>`	Scan the top x ports
`nmap -sV--version-intensity 5 <Target IP>`	Aggressive service discovery
`nmap -sV --version-intensity 0 <Target IP>`	Light banner grabbing
`nmap -sV--version-light <Target IP>`	Enable light mode, lower possibility of correctness
`nmap -sV--version-all <Target IP>`	Enable intensity level 9. Higher possibility of correctness
`nmap -O--osscan-limit <Target IP>`	Limit OS detection to promising targets
`nmap -O--osscan-guess <Target IP>`	Guess OS detection results
`nmap -O --max-os-tries x <Target IP>`	Set maximum number of OS detection tries against a target
`nmap -sU -p 123,161,162 <Target IP>`	Scan UDP ports
`nmap -Pn -F <Target IP>`	Scan selected ports - ignore discovery
`nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p <Port List> <Target IP>`	Identify open ports and services
`nmap -Pn -sT -p 46824 <Target IP>`	Identify HMI systems
`nmap -Pn -sT -p 102 --script s7-info <Target IP>`	Scan Siemens SIMATIC S7 PLCs
`nmap -Pn -sT -p 502 --script modbus-discover <Target IP>`	Scan Modbus Devices
`nmap -sU -p 500 <Target IP>`	Check the status of isakmp over port 500
`nmap -Pn -sU -p 47808 --script bacnet-info <Target IP>`	ScanBACnet Devices
`nmap -Pn -sU -p 44818 --script enip-info <Target IP>`	Scan Ethernet/IP Devices

Command	Description
`nmap -Pn -sT -p 1911,4911 --script fox-info <Target IP>`	Scan Niagara Fox Devices
`nmap -Pn -sT -p 20547 --script proconos-info <Target IP>`	Scan ProConOS Devices
`nmap -Pn -sT -p 9600 --script omron-info <Target IP>`	Scan Omron PLC Devices
`nmap -Pn -sU -p 9600 --script omron-info <Target IP>`	Scan Omron PLC Devices
`nmap -Pn -sT -p 1962 --script pcworx-info <Target IP>`	Scan PCWorx Devices

C|EH

Ethical Hacking and Countermeasures
Nmap Cheat Sheet

EC-Council
Building A Culture Of Security

Nmap
Source: https://nmap.org

Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their specific needs.

Syntax

```
nmap [Scan Type...]
[Options] {Target
specification}
```

```
1.Nmap Options
2.Nmap Port Scan types
3.Nmap Commands
```

3. Nmap Commands

Command	Description
`nmap -p 1-65535 -T4 -A -v <Target IP>`	Perform intense scan on all TCP ports
`nmap -p ports <Target IP>`	Run Nmap to identify IoT devices using insecure HTTP ports for transmitting data
`nmap -T4 -A -v -Pn <Target IP>`	Perform Intense scan with no ping
`nmap -T4-A-v-PE-PS-PA Ports URL`	Footprint Web Infrastructure: Service Discovery
`nmap -sn <Target IP>`	Perform ping scan
`nmap -sn <Target IP/Subnet>`	Disable port scanning, host discovery only
`nmap -sn -PR <Target IP>`	ARP Ping Scan
`nmap -sn -PU <Target IP>`	UDP Ping Scan
`nmap -sn -PE <Target IP>`	ICMP ECHO Ping Scan
`nmap -sn -PE <IP range>`	ICMP ECHO Ping Sweep
`nnmap –sn –PP <Target IP>`	ICMP Timestamp Ping Scan
`nmap –sn –PM <Target IP>`	ICMP Address Mask Ping Scan
`nmap –sn –PS <Target IP>`	TCP SYN Ping Scan
`nmap –sn –PA <Target IP>`	TCP ACK Ping Scan
`nmap –sn –PO <Target IP>`	IP Protocol Ping Scan
`nmap -St -v <Target IP>`	TCP Connect/ Full Open Scan
`namp -sS -v <Target IP>`	Stealth Scan (Half-open Scan)

Command	Description
`nmap -sX -v <Target IP>`	Xmas Scan
`nmap -sM -v <Target IP>`	TCP Maimon Scan
`nmap -sA -v <Target IP>`	TCP Connect/ Full Open Scan
`nmap –badsum <Target IP>`	Sending Bad Checksums

`nmap --script`
`smb-os-discovery.nse <Target IP>`
	OS Discovery using Nmap Script Engine

`nmap -sV -T4 -O -F`
`–version-light <Target IP>`
	Perform quick scan plus

`nmap -sV -T4 -O -F`
`–version-light scanme.nmap.org`
	Wi-Fi vulnerability scanning on wireless networks

`nmap -sV –O –p <Target IP>`
`nmap -sV --script http-enum`
`<Target IP>`
	NSE scripts to enumerate information about the target website/ web servers

`nmap target IP address -p 80`
`--script = http-frontpage-login`
`nmap --script http-passwd`
`--script-args http-passwd.root`	

`nmap -sV --script http-enum`
`<Target domain>`
	Analyze Web Applications: Identify exposed Files and Directories of the target webserver

`nmap -iL list-of-ips.txt`	Scan targets from a text file

`nmap --script=sniffer-detect`
`[Target IP Address/Range of IP`
`addresses]`
	Command to detect NIC in promiscuous mode

`nmap <Target IP> --data`
`Oxdeadbeef`
	Create Custom Packets by Appending Custom Binary Data

`nmap <Target IP> --data-string`
`“ph34r my |33t skills”`
	Create Custom Packets by Appending Custom String

`nmap <Target IP> --data-string 5`	Create Custom Packets by Appending Random Data
`nmap –sU –p 500 <Target IP>`	Perform a check on the status of ISAKMP over port 500
`nmap -sR <Target IP/network>`	Identify the RPC service running on the network
`nmap --script hostmap <host>`	Discover virtual domains with hostmap

`nmap --script http-trace -p80`
`localhost`
	Detect a vulnerable server that uses the TRACE method

`nmap --script http-google-email`
`<host>`
	Harvest email accounts with http-google-email

`nmap -p80 --script http-userdir`
`-enum localhost`
	Enumerate users with http-userdir-enum

`nmap -p80 --script http-trace`
`<host>`
	Detect HTTP TRACE

Command	Description

`nmap -p80 --script`
`http-waf-detect`
`--script-args=”http-wafdetect.`
`uri=/testphp.vulnweb.com/artists.`
`php,http-wafdetect.`
`detectBodyChanges”`
`www.modsecurity.org`
	Check if web server is protected by WAF/IPS

`nmap --script http-enum -p80`
`<host>`
	Enumerate common web applications

`nmap -p80 --script`
`http-robots.txt <host>`
	Obtain robots.txt

`nmap -p80 --script http-test.txt`
`<host>`
	Obtain test.txt

`nmap`
`--script=asn-query,whois,ip-geolo`
`cation-maxmind <Target IP/`
	IP address Information

`nmap --script=http-title`
`<Target IP/ Subnet>`
	Gather page titles from HTTP services

`nmap --script=http-headers`
`<Target IP/ Subnet>`
	Get HTTP headers of web services

`nmap --script=http-enum <Target`
`IP/ Subnet>`
	Find web apps from known paths

`nmap -n -Pn -sSU`
`-pT:0-65535,U:0-65535 -v -A -oX`
`<Name><Target IP>`
	Perform complete scan of the IoT device that checks for both TCP and UDP services and ports

`nmap -sS -T4 -A -f -v <Target`
`IP>`
	Packet Fragmentation/ SYN/FIN scan using Nmap

`nmap -g 80 <Target IP>`	Source Port Manipulation/ Use given source port number

`nmap –sU –A –PN –n`
`–pU:19,53,123,161`
`–script=ntp-monlist,dns-recursi`
`on,snmp-sysdescr <Target IP/`
`network>`
	Scan for UDP DDOS reflectors

`nmap -6 -n -Pn -sSU`
`-pT:0-65535,U:0-65535 -v -A -oX`
`<Name><Target IP>`
	Identify the IPv6 capabilities of a device

`nmap -T4 -A -v <Target IP>`	Perform intense scan
`nmap -T4 -A <Target IP/Subnet>`	Identify vulnerable services on service port by attackers by using RPC Enumeration
`nmap -p 23 <Target Domain>`	Telnet Enumeration

`nmap -p 23 --script`
`telnet-ntlm-info <Target IP>`
	Enumerate information from remote Microsoft Telnet services with NTLM authentication enabled

`nmap -p 23 -script`
`telnet-brute.nse –script-args`
	Perform brute-force attack against telnet server

`nmap -p 445 -A <Target IP>`	Enumerate SMB service running on the target IP address/ SMB Enumeration
`nmap -p 21 <Target Domain>`	FTP Enumeration

95% Chose C|EH for Career Growth

Ethical Hacking and Countermeasures
Nmap Cheat Sheet

Nmap
Source: https://nmap.org

Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their specific needs.

Syntax

```
nmap [Scan Type...]
[Options] {Target
specification}
```

```
1.Nmap Options
2.Nmap Port Scan types
3.Nmap Commands
```

3. Nmap Commands

Command	Description
`nmap -p 69 <Target Domain>`	Enumerate TFTP service running on the target domain
`nmap -p 179 <Target IP>`	BGP Enumeration
`nmap -sS -sU -T4 -A -v <Target IP>`	Perform intense scan and scanning for UDP
`nmap -sV -v -p 139,445 <Target IP/Subnet>`	Detect all exposed Netbios servers on the subnet
`nmap -sV -v --script nbstat.nse <Target IP>`	map's nbstat NSE script allow attackers to retrieve target's NetBIOS names and MAC addresses
`nmap -sU --script nbstat.nse -p 137 <Target IP address>`	Find target Netbios name
`nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p 445 <Target IP address>`	Check if Netbios servers are vulnerable to MS08-067
`nmap -sV --version-intensity 0 <Target IP>`	Lighter banner grabbing detection
`nmap -sV --version-intensity 5 <Target IP>`	More aggressive Service Detection
`nmap -sV <Target IP>`	Attempts to determine the version of service running/ Standard service detection/ Service Version Discovery in Zenmap
`nmap --script-help=ssl-heartbleed`	Get help for a script
`nmap --script dns-zonetransfer.nse --script-args dns-zonetransfer.domain=<domain> -p53 <hosts>`	Attempts to pull a zone file (AXFR) from a DNS server
`nmap --script http-robots.txt <hosts>`	Harvests robots.txt files from discovered web servers
`nmap --script smb-brute.nse -p445 <hosts>`	Attempts to determine valid username and password combinations via automated guessing
`nmap --script smb-psexec.nse –script-args=smbuser=<username>, smbpass=<password>[,config=<config>] -p445 <hosts>`	Attempts to run a series of programs on the target machine, using credentials provided as scriptargs
`nmap -sV -p 443 --script=ssl-heartbleed <Target IP/Subnet>`	Detect Heartbleed SSL Vulnerability
`nmap <Target IP>-50 -sL --dns-server <Target IP>`	Query the Internal DNS for hosts, list targets only

Command	Description
`nmap -iR 10 -sn -traceroute`	Traceroute to random targets, no port scan
`nmap <Target IP>-1/24 -PR -sn -vv`	Arp discovery only on local network, no port scan
`nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn`	Discovery only on ports x, no port scan
`nmap -sP <Target IP/Subnet>`	Ping scans the network, listing machines that respond to ping
`nmap -v -sS -A -T4 <Target IP>`	Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection, traceroute and scripts against target services
`nmap -v -sV -O -sS -T5 <Target IP>`	Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection
`nmap -iL ip-addresses.txt`	Scans a list of IP addresses
`nmap — script-args=unsafe=1 — script smb-check-vulns.nse -p 445 <Target IP>`	Check if Netbios servers are vulnerable to MS08–067
`nmap –Pn –p- -sI zombie target`	Attack
`nmap –b ftp rely host`	FTP Bounce Scan <username>:<password>@<server>:<port>. <Server> is the name or IP address of a vulnerable FTP server
`nmap -T0 <Target IP>`	Paranoid (0) Intrusion Detection System evasion
`nmap -T1 <Target IP>`	Sneaky (1) Intrusion Detection System evasion
`nmap -T2 <Target IP>`	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
`nmap -T3 <Target IP>`	Normal (3) default speed
`nmap -T4 <Target IP>`	Aggressive (4) speeds scan; assumes you are on a reasonably fast and reliable network
`nmap -T5 <Target IP>`	Insane (5) speeds scan; assumes you are on extraordinarily fast network
`nmap --script=ftp <Target IP>`	Scan with a single script
`nmap --script=http* <Target IP>`	Scan with a wildcard script
`nmap --script=banner,http <Target IP>`	Scan with two scripts
`nmap --script "not intrusive" <Target IP>`	Scan default, but remove intrusive scripts
`nmap -Pn --script=http-sitemap-generator xyz.com`	HTTP site map generator

Command	Description
`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 xyz.com`	Brute forces DNS hostnames guessing subdomain
`nmap -n -Pn -vv -O -sV --script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv <Target IP>`	Safe SMB scripts to run
`nmap --script whois*<Target Domain>`	Whois query
`nmap -p80 --script http-unsafe-output-escaping <Target Website>`	Detect cross site scripting vulnerabilities
`nmap -p80 --script http-sql-injection <Target`	Check for SQL injections
`nmap --data-length x <Target IP>`	Appends random data to sent packets
`nmap -oN file.file --append-output <Target IP>`	Append a scan to a previous scan file
`nmap --iflist`	Shows the host interface and routes
`nmap -6 2607:f0d2:5664:51::5`	Enable IPV6 scanning
`nmap -T0 -b username:password@ftpserver.tld :21 victim.tld`	Uses the username "username", the password "password", the FTP server "ftpserver.tld" and port 21 on said server to scan victim.tld.
`nmap -sU -sT -p U:[ports],T:[ports] <Target IP>`	Scan ports by protocol
`nmap -sV –version-trace <Target IP>`	Troubleshooting version scans
`nmap –script [script.nse] <Target IP>`	Execute individual scripts
`nmap –script [expression] <Target IP>`	Execute multiple scripts
`nmap –script [category] <Target IP>`	Execute scripts by category
`nmap –script [category1,category2, etc]`	Execute multiple scripts categories
`nmap –script [script] –script-trace <Target IP>`	Troubleshoot scripts
`$ docker -H <docker host> run --network=host --rm marsmensch/nmap -ox <IP Range>`	Use Nmap to scan the host's internal network to identify running services
`ndiff [scan1.xml] [scan2.xml]`	Comparison using Ndiff
`ndiff -v [scan1.xml] [scan2.xml]`	Ndiff verbose mode
`ndiff –xml [scan1.xm]`	XML output mode

Nmap

Source: https://nmap.org

Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their specific needs.

Syntax

```
nmap [Scan Type...]
[Options] {Target
specification}
```

1.Nmap Options
2.Nmap Port Scan types
3.Nmap Commands

Port Selection

Command	Description
nmap <Target IP>	Scan single IP
nmap <Target IP> <Target IP>	Scan specific IPs
nmap <Target IP range>	Scan a range of IPs
nmap <Target Website>	Scan a host
nmap <Target Domain>	Scan a domain
nmap <Target IP/Subnet>	Scan using CIDR notation
nmap -iL file.txt	Scan targets using given file
nmap --exclude <Target IP>	Exclude listed host/ specified IP s exclude from scan
nmap -iR 50	Scan 50 random hosts

NSE Scripts

Command	Description
nmap -sC <Target IP>	Scan with default NSE scripts.
nmap --script-default <Target IP>	Scan with default NSE scripts.
nmap --script snmp-sysdescr --script-args snmpcommunity=admin <Target IP>	NSE script with arguments
nmap -script-args-file=filename	Provide NSE script args in a file
nmap -sV -sC <Target IP>	Scan using default safe scripts
nmap -sV --script=smb* <Target IP>	Scan with a set of scripts
nmap -sV -p 443 -script=ssl-heartbleed.nse <Target IP>	Scan using a specific NSE script