NMAP (Network Mapping) Cheat Sheet

neverendingsecurity.wordpress.com/2015/05/10/nmap-network-mapping-cheat-sheet/amp/

Nmap (Network Mapping) Cheat Sheet. It is a very famous port scanner available for free. It is not just only a port scanner, it also do various jobs like banner grabbing, OS fingerprinting, Nmap script scanning, evading firewalls, etc. So we are gonna show you some important commands of Nmap.
Step 1: Open up the console and type nmap
It will give you the whole commands of Nmap. But we are here to understanding the commands so we should go ahead.

Here is the cheatsheet of NMAP.

BASIC SCANNING TECHNIQUES

Goal	Command	Example
Scan a Single Target	nmap [target]	nmap 192.168.0.1
Scan Multiple Targets	nmap [target1, target2, etc]	nmap 192.168.0.1 192.168.0.2
Scan a List of Targets	nmap -iL [list.txt]	nmap -iL targets.txt
Scan a Range of Hosts	nmap [range of ip addresses]	nmap 192.168.0.1-10
Scan an Entire Subnet	nmap [ip address/cdir]	nmap 192.168.0.1/24
Scan Random Hosts	nmap -iR [number]	nmap -iR 0
Excluding Targets from a Scan	nmap [targets] –exclude [targets]	nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200
Excluding Targets Using a List	nmap [targets] –excludefile [list.txt]	nmap 192.168.0.1/24 –excludefile notargets.txt
Perform an Aggressive Scan	nmap -A [target]	nmap -A 192.168.0.1
Scan an IPv6 Target	nmap -6 [target]	nmap -6 1aff:3c21:47b1:0000:0000:0000:0000:2afe

DISCOVERY OPTIONS

Goal	Command	Example
Perform a Ping Only Scan	nmap -sP [target]	nmap -sP 192.168.0.1
Don’t Ping	nmap -PN [target]	nmap -PN 192.168.0.1
TCP SYN Ping	nmap -PS [target]	nmap -PS 192.168.0.1
TCP ACK Ping	nmap -PA [target]	nmap -PA 192.168.0.1
UDP Ping	nmap -PU [target]	nmap -PU 192.168.0.1
SCTP INIT Ping	nmap -PY [target]	nmap -PY 192.168.0.1

ICMP Echo Ping	**nmap -PE [target]**	**nmap -PE 192.168.0.1**
ICMP Timestamp Ping	**nmap -PP [target]**	**nmap -PP 192.168.0.1**
ICMP Address Mask Ping	**nmap -PM [target]**	**nmap -PM 192.168.0.1**
IP Protocol Ping	**nmap -PO [target]**	**nmap -PO 192.168.0.1**
ARP Ping	**nmap -PR [target]**	**nmap -PR 192.168.0.1**
Traceroute	**nmap –traceroute [target]**	**nmap –traceroute 192.168.0.1**
Force Reverse DNS Resolution	**nmap -R [target]**	**nmap -R 192.168.0.1**
Disable Reverse DNS Resolution	**nmap -n [target]**	**nmap -n 192.168.0.1**
Alternative DNS Lookup	**nmap –system-dns [target]**	**nmap –system-dns 192.168.0.1**
Manually Specify DNS Server(s)	**nmap –dns-servers [servers] [target]**	**nmap –dns-servers 201.56.212.54 192.168.0.1**
Create a Host List	**nmap -sL [targets]**	**nmap -sL 192.168.0.1/24**

ADVANCED SCANNING OPTIONS

Goal	Command	Example
TCP SYN Scan	nmap -sS [target]	nmap -sS 192.168.0.1
TCP Connect Scan	nmap -sT [target]	nmap -sT 192.168.0.1
UDP Scan	nmap -sU [target]	nmap -sU 192.168.0.1
TCP NULL Scan	nmap -sN [target]	nmap -sN 192.168.0.1
TCP FIN Scan	nmap -sF [target]	nmap -sF 192.168.0.1
Xmas Scan	nmap -sX [target]	nmap -sX 192.168.0.1
TCP ACK Scan	nmap -sA [target]	nmap -sA 192.168.0.1
Custom TCP Scan	nmap –scanflags [flags] [target]	nmap –scanflags SYNFIN 192.168.0.1
IP Protocol Scan	nmap -sO [target]	nmap -sO 192.168.0.1
Send Raw Ethernet Packets	nmap –send-eth [target]	nmap –send-eth 192.168.0.1
Send IP Packets	nmap –send-ip [target]	nmap –send-ip 192.168.0.1

PORT SCANNING OPTIONS

Goal	Command	Example
Perform a Fast Scan	nmap -F [target]	nmap -F 192.168.0.1

Scan Specific Ports	nmap -p [port(s)] [target]	nmap -p 21-25,80,139,8080 192.168.1.1
Scan Ports by Name	nmap -p [port name(s)] [target]	nmap -p ftp,http* 192.168.0.1
Scan Ports by Protocol	nmap -sU -sT -p U:[ports],T: [ports] [target]	nmap -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.0.1
Scan All Ports	nmap -p '*' [target]	nmap -p '*' 192.168.0.1
Scan Top Ports	nmap –top-ports [number] [target]	nmap –top-ports 10 192.168.0.1
Perform a Sequential Port Scan	nmap -r [target]	nmap -r 192.168.0.1

VERSION DETECTION

Goal	Command	Example
Operating System Detection	nmap -O [target]	nmap -O 192.168.0.1
Submit TCP/IP Fingerprints	http://www.nmap.org/submit/	
Attempt to Guess an Unknown OS	nmap -O –osscan-guess [target]	nmap -O –osscan-guess 192.168.0.1
Service Version Detection	nmap -sV [target]	nmap -sV 192.168.0.1
Troubleshooting Version Scans	nmap -sV –version-trace [target]	nmap -sV –version-trace 192.168.0.1
Perform a RPC Scan	nmap -sR [target]	nmap -sR 192.168.0.1

TIMING OPTIONS

Goal	Command	Example
Timing Templates	nmap -T[0-5] [target]	nmap -T3 192.168.0.1
Set the Packet TTL	nmap –ttl [time] [target]	nmap –ttl 64 192.168.0.1
Minimum # of Parallel Operations	nmap –min-parallelism [number] [target]	nmap –min-parallelism 10 192.168.0.1
Maximum # of Parallel Operations	nmap –max-parallelism [number] [target]	nmap –max-parallelism 1 192.168.0.1
Minimum Host Group Size	nmap –min-hostgroup [number] [targets]	nmap –min-hostgroup 50 192.168.0.1
Maximum Host Group Size	nmap –max-hostgroup [number] [targets]	nmap –max-hostgroup 1 192.168.0.1
Maximum RTT Timeout	nmap –initial-rtt-timeout [time] [target]	nmap –initial-rtt-timeout 100ms 192.168.0.1
Initial RTT Timeout	nmap –max-rtt-timeout [TTL] [target]	nmap –max-rtt-timeout 100ms 192.168.0.1

Maximum Retries	nmap –max-retries [number] [target]	nmap –max-retries 10 192.168.0.1
Host Timeout	nmap –host-timeout [time] [target]	nmap –host-timeout 30m 192.168.0.1
Minimum Scan Delay	nmap –scan-delay [time] [target]	nmap –scan-delay 1s 192.168.0.1
Maximum Scan Delay	nmap –max-scan-delay [time] [target]	nmap –max-scan-delay 10s 192.168.0.1
Minimum Packet Rate	nmap –min-rate [number] [target]	nmap –min-rate 50 192.168.0.1
Maximum Packet Rate	nmap –max-rate [number] [target]	nmap –max-rate 100 192.168.0.1
Defeat Reset Rate Limits	nmap –defeat-rst-ratelimit [target]	nmap –defeat-rst-ratelimit 192.168.0.1

FIREWALL EVASION TECHNIQUES

Goal	Command	Example
Fragment Packets	nmap -f [target]	nmap -f 192.168.0.1
Specify a Specific MTU	nmap –mtu [MTU] [target]	nmap –mtu 32 192.168.0.1
Use a Decoy	nmap -D RND:[number] [target]	nmap -D RND:10 192.168.0.1
Idle Zombie Scan	nmap -sI [zombie] [target]	nmap -sI 192.168.0.38 192.168.0.1
Manually Specify a Source Port	nmap –source-port [port] [target]	nmap –source-port 1025 192.168.0.1
Append Random Data	nmap –data-length [size] [target]	nmap –data-length 20 192.168.0.1
Randomize Target Scan Order	nmap –randomize-hosts [target]	nmap –randomize-hosts 192.168.0.1-20
Spoof MAC Address	nmap –spoof-mac [MAC|0|vendor] [target]	nmap –spoof-mac Cisco 192.168.0.1
Send Bad Checksums	nmap –badsum [target]	nmap –badsum 192.168.0.1

OUTPUT OPTIONS

Goal	Command	Example
Save Output to a Text File	nmap -oN [scan.txt] [target]	nmap -oN scan.txt 192.168.0.1
Save Output to a XML File	nmap -oX [scan.xml] [target]	nmap -oX scan.xml 192.168.0.1
Grepable Output	nmap -oG [scan.txt] [targets]	nmap -oG scan.txt 192.168.0.1
Output All Supported File Types	nmap -oA [path/filename] [target]	nmap -oA ./scan 192.168.0.1
Periodically Display Statistics	nmap –stats-every [time] [target]	nmap –stats-every 10s 192.168.0.1
133t Output	nmap -oS [scan.txt] [target]	nmap -oS scan.txt 192.168.0.1

TROUBLESHOOTING AND DEBUGGING

Goal	Command	Example
Getting Help	nmap -h	nmap -h
Display Nmap Version	nmap -V	nmap -V
Verbose Output	nmap -v [target]	nmap -v 192.168.0.1
Debugging	nmap -d [target]	nmap -d 192.168.0.1
Display Port State Reason	nmap –reason [target]	nmap –reason 192.168.0.1
Only Display Open Ports	nmap –open [target]	nmap –open 192.168.0.1
Trace Packets	nmap –packet-trace [target]	nmap –packet-trace 192.168.0.1
Display Host Networking	nmap –iflist	nmap –iflist
Specify a Network Interface	nmap -e [interface] [target]	nmap -e eth0 192.168.0.1

NMAP SCRIPTING ENGINE

Goal	Command	Example
Execute Individual Scripts	nmap –script [script.nse] [target]	nmap –script banner.nse 192.168.0.1
Execute Multiple Scripts	nmap –script [expression] [target]	nmap –script ‘http-*’ 192.168.0.1
Script Categories	all, auth, default, discovery, external, intrusive, malware, safe, vuln	
Execute Scripts by Category	nmap –script [category] [target]	nmap –script ‘not intrusive’ 192.168.0.1
Execute Multiple Script Categories	nmap –script [category1,category2,etc]	nmap –script ‘default or safe’ 192.168.0.1
Troubleshoot Scripts	nmap –script [script] –script-trace [target]	nmap –script banner.nse –script trace 192.168.0.1
Update the Script Database	nmap –script-updatedb	nmap –script-updatedb