nmap cheatsheet Cheat Sheet

by Abhisek (netwrkspider) via cheatography.com/23282/cs/5099/

Basic Scanning with Nmap

Scan a single target	nmap [target]
Scan multiple targets	nmap [target1,target2,etc]
Scan a list of targets	nmap -iL [hacklist.txt]
Scan a range of hosts	nmap [range of IP addresses]
Scan an entire subnet	nmap [IP address/cdir]
Scan random hosts	nmap -iR [number]
Excluding targets from a scan	nmap [targets] –exclude [targets]
Excluding targets using a list	nmap [targets] –excludefile [list.txt]
Perform an aggressive scan	nmap -A [target]
Scan an IPv6 target	nmap -6 [target]

Output Options

Save output to a text file	nmap -oN [scan.txt] [target]
Save output to a xml file	nmap -oX [scan.xml] [target]
Grepable output	nmap -oG [scan.txt] [target]
Output all supported file types	nmap -oA [path/filename] [target]
Periodically display statistics	nmap –stats-every [time] [target]

Output Options (cont)

133t output	nmap -oS [scan.txt] [target]

Nmap Scripting Engine

Execute individual scripts

nmap –script [script.nse] [target]

Execute multiple scripts

nmap –script [expression] [target]

Execute scripts by category

nmap –script [cat] [target]

Execute multiple scripts categories

nmap –script [cat1,cat2, etc]

Troubleshoot scripts

nmap –script [script] –script-trace [target]

Update the script database

nmap –script-updatedb

Script categories

a

auth

default

discovery

external

intrusive

malware

safe

vuln

Version Detection with Nmap

Operating system detection	nmap -O [target]
Attempt to guess an unknown	nmap -O –osscan-guess [target]
Service version detection	nmap -sV [target]
Troubleshooting version scans	nmap -sV –version-trace [target]
Perform a RPC scan	nmap -sR [target]

Firewall Evasion Techniques with Nmap

Fragment packets	nmap -f [target]
Specify a specific MTU	nm ap –mtu [MTU] [target]
Use a decoy	nmap -D RND: [number] [target]
Idle zombie scan	nmap -sI [zombie] [target]
Manually specify a source port	nmap –source-port [port] [target]
Append random data	nmap –data-length [size] [target]
Randomize target scan order	nmap –randomize-hosts [target]
Spoof MAC Address	nmap –spoof-mac [MAC|0|vendor] [target]
Send bad checksums	nmap –badsum [target]

Ndiff

Comparison using Ndiff	ndiff [scan1.xml] [scan2.xml]
Ndiff verbose mode	ndiff -v [scan1.xml] [scan2.xml]
XML output mode	ndiff –xml [scan1.xm] [scan2.xml]

About me

Name	netwrkspider
website	http://www.netwrkspider.org
Job Profile	Security Researcher & Developers

Nmap Discovery Options

Perform a ping scan only	nmap -sP [target]
Don't ping	nmap -PN [target]
TCP SYN Ping	nmap -PS [target]
TCP ACK ping	nmap -PA [target]
UDP ping	nmap -PU [target]
SCTP Init Ping	nmap -PY [target]
ICMP echo ping	nmap -PE [target]
ICMP Timestamp ping	nmap -PP [target]
ICMP address mask ping	nmap -PM [target]
IP protocol ping	nmap -PO [target]
ARP ping	nmap -PR [target]

Nmap Discovery Options (cont)

Traceroute	nmap –traceroute [target]
Force reverse DNS resolution	nmap -R [target]
Disable reverse DNS resolution	nmap -n [target]
Alternative DNS lookup	nmap –system-dns [target]
Manually specify DNS servers	nmap –dns-servers [servers] [target]
Create a host list	nmap -sL [targets]