Cheatography

Nmap Basics Cheat Sheet

by RomelSan (RomelSan) via cheatography.com/3953/cs/830/

Nmap Fundamentals

Listing open ports on a remote host	nmap [target]
Exclude a host from scan	nmap --exclude [excluded ip] [target]
Use custom DNS Server	nmap --dns-servers [DNS1],[DNS2] [target]
Scan - no ping targets	nmap -PN [target]
Scan - no DNS resolve	nmap -n [target]
Scan specific port	nmap -p80 [target]
Scan an IPv6 target	nmap -6 [target]

Scanning Port Ranges

Scan specific port list	nmap -p 80,443,23 [target]
Scan specific port range	nmap -p 1-100 [target]
Scan all ports	nmap -p- [target]
Scan specific ports by protocol	nmap -p T:25,U:53 [target]
Scan by Service name	nmap -p smtp [target]
Scan Service name wildcards	nmap -p smtp* [target]
Scan only port registered in Nmap services	nmap -p [1-65535] [target]

Scanning Large Networks

Skipping tests to speed up long scans	nmap -T4 -n -Pn -p- [target]
Arguments:	
No Ping	-Pn
No reverse resolution	-n
No port scanning	-sn
Timing Templates Arguments	

Scanning Large Networks (cont)

Scanning is not supposed to interfere with the target system	-T2
Recommended for broadband and Ethernet connections	-T4
Normal Scan Template	-T3
Not Recommended	-T5 or T1 or T0

Nmap Specifics

Select Interface to make scans	nmap -e [INTERFACE] [target]
Save as text file (export)	nmap -oN [filename] [target]
Save as xml (export)	nmap -oX [filename] [target]
Save as all supported file types	nmap -oA [filename] [target]
Periodically display statistics	nmap –stats-every [time] [target]

Finding alive hosts

Default ping scan mode	nmap -sP [target]
Discovering hosts with TCP SYN ping scans	nmap -sP -PS [target]
Specific Port using TCP SYN ping scans	nmap -sP -PS80 [target]
Ping No arp	nmap -sP --send-ip [target]
IP Protocol ping scan (IGMP, IP-in-IP, ICMP)	nmap -sP -PO [target]
ARP Scan	nmap -sP -PR [target]

Fingerprinting services of a remote host

Display service version	nmap -sV [target]
Set probes	nmap -sV --version-intensity 9 [target]
Aggressive detection	nmap -A [target]
Troubleshooting version scans	nmap -sV –version-trace [target]
Perform a RPC scan	nmap -sR [target]

Fingerprinting the operating system of a host

Detect Operating System	nmap -O [target]
Guess Operating System	nmap -O -p- --osscan-guess [target]
Detect Operating System (Verbose)	nmap -O -v [target]
Listing protocols supported by a remote host	nmap -sO [target]
Discovering stateful firewalls by using a TCP ACK scan	nmap -sA [target]

Nmap Scripting Engine

Execute individual scripts	nmap –script [script.nse] [target]
Execute scripts by category	nmap –script [category] [target]
Troubleshoot scripts	nmap –script [script] –script-trace [target]
Update the script database	nmap –script-updatedb
Script categories	auth broadcast dos default discovery external intrusive malware safe version vuln

By **RomelSan** (RomelSan)
cheatography.com/romelsan/
keybase.io/romel

Published 9th February, 2013.
Last updated 13th March, 2017.

Cheatography

Nmap Basics Cheat Sheet

by RomelSan (RomelSan) via cheatography.com/3953/cs/830/

Nmap Examples	
Detect Service versions and OS	nmap -sV -O [target]
Detect Web Servers	nmap -sV --script http-title [target]
Scan top common ports	nmap --top-ports 10 [target]
Discover host using Broadcast pings	nmap --script broadcast-ping
Getting information from whois records	nmap --script whois [target]
Brute force DNS records	nmap --script dns-brute [target]
Scan a firewall for MAC address spoofing	nmap -v -sT -PN --spoof-mac [Mac Address] [target]
Run all scripts in the vuln category	nmap -sV --script vuln [target]
Run the scripts in the categories version or discovery	nmap -sV --script="version,discovery" [target]
Sniffer Detect	nmap -sP --script sniffer-detect [target]

By **RomelSan** (RomelSan)
cheatography.com/romelsan/
keybase.io/romel

Published 9th February, 2013.
Last updated 13th March, 2017.