

Nmap Basics Cheat Sheet

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

Nmap Fundamentals	
Listing open ports on a remote host	nmap <target></target>
Exclude a host from scan	nmapexclude <excluded ip=""> <target></target></excluded>
Use custom DNS Server	nmapdns-servers [DNS1],[DNS2] <target></target>
Scan - no ping targets	nmap -PN <target></target>
Scan - no DNS resolve	nmap -n <target></target>
Scan specific port	nmap -p80 <target></target>

Scanning Port Ranges	
Scan specific port list	nmap - p80,443,23 <target></target>
Scan specific port range	nmap -p1-100 <target></target>
Scan all ports	nmap -p- <target></target>
Scan specific ports by protocol	nmap - pT:25,U:53 <target></target>
Scan by Service name	nmap -p smtp <target></target>
Scan Service name wildcards	nmap -p smtp* <target></target>
Scan only port registered in Nmap services	nmap -p[1- 65535] <target></target>

Scanning Large Networks	
Skipping tests to speed up long scans	nmap -T4 -n -Pn - p- <target></target>
Arguments:	
No Ping	-Pn
No reverse resolution	-n
No port scanning	-sn
Timing Templates Arguments	

By RomelSan (RomelSan)
cheatography.com/romelsan
www.betasetup.com

-T2
-T4
-T3
-T5 or T1 or T0

Nmap Specifics	
Select Interface to make scans	nmap -e <interface> <target></target></interface>
Save Normal method	nmap -oN <filename> <target></target></filename>
Save as xml (export)	nmap -oX <filename> <target></target></filename>

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

Fingerprinting services of a remote host	
Display service version	nmap -sV <target></target>
Set probes	nmap -sVversion- intensity 9 <target></target>
Aggressive detection	nmap -A <target></target>

Fingerprinting the operation	ng system of a
Detect Operating System	nmap -O <target></target>
Guess Operating System	nmap -O -p osscan-guess <target></target>
Detect Operating System (Verbose)	nmap -O -v <target></target>
Listing protocols supported by a remote host	nmap -sO <target></target>
Discovering stateful firewalls by using a TCP ACK scan	nmap -sA <target></target>

Nmap Examples	
Detect Service versions and OS	nmap -sV -O <target></target>
Detect Web Servers	nmap -sVscript http-title <target></target>
Discover host using Broadcast pings	nmapscript broadcast-ping
Brute force DNS records	nmapscript dns- brute <target></target>

Sponsored by Readability-Score.com Measure your website readability! https://readability-score.com



Published 9th February, 2013. Last updated 9th February, 2013. Page 1 of 1.