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>

Scanning Port Ranges

Scan specific port list	nmap -p80,443,23 <target>
Scan specific port range	nmap -p1-100 <target>
Scan all ports	nmap -p- <target>
Scan specific ports by protocol	nmap -pT: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 Normal method	nmap -oN <filename> <target>
Save as xml (export)	nmap -oX <filename> <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>

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 Examples

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

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

Published 9th February, 2013.
Last updated 9th February, 2013.