

Download ZeNMAP

<https://nmap.org/download.html>

Host Notation

IP	152.120.2.200
Hostname	IDNS3.dot.gov
Subnet	152.120.2.0/24
IP Range	152.120.2.5-20

Common Options

-T3	Normal Speed
-T4	Fast Speed
-A	OS and Version detection
-O	OS detection
-v	Verbose
-sV	Probe open ports to determine service/version info
-sn	Ping Scan
-p <port range>	Only scan specified ports
--script=	Run a specified script
-iL [filename]	Input file of hosts/IPs
-oN [filename]	Save as text file
-oX [filename]	Save as XML file

Common Scripts

ssl-enum-ciphers	Display SSL cipher
smb-protocols	Display SMB protocol
ssl-heartbleed	Display heartbleed

Preset Profiles

Intense	<code>nmap -T4 -A -v</code>
Quick Scan Plus	<code>nmap -sV -T4 -O -F --version-light</code>
Ping Scan	<code>nmap -sn</code>

References

<https://nmap.org/book/man.html>
<https://www.cyberciti.biz/security/nmap-command-examples-tutorials/>
<https://www.linux.com/learn/beginners-guide-nmap>

FAQ

How do tell who at DOT runs a server?

Run `nmap -sV -T4 -O -A` and look for a hostname
 Check the hostname for a mode
 Check Solarwinds for the Support t_M anager property
 Check the patch list to see if ITSS manages it

Is a host running SMB v1?

Run `nmap --script= smb -pr otocols`
 Check for anything below version 2.0

Is a host using low security SSL?

Run `nmap --script= ssl -en um- ciphers`
 Check for any warnings about SWEET32/RC4/ low Diffie-Helman key exchanges

Example #1

NCATS report for a server comes in

Summary:

NCCIC NCATS Cyber Hygiene reported a system vulnerability

Source IP: 204.68.195.16

Host Name: docket sin fo.d ot.gov

- 1) Run `nmap -sV -T4 -A -v docket sin fo.d ot.gov`
- 2) Note the hostname in the 3389 and 10000 port results, and the `smb-os -di scovery script`
- 3) determine that this is an OST server that is not on the ITSS patch list
- 4) most likely an OST (Non-ITSS) managed server

Example #2

NCATS report for a server comes in

Summary:

NCCIC NCATS Cyber Hygiene reported a system vulnerability

Source IP: 204.68.194.45

Destination IP: 64.69.57.0 /24

Host Name: 204.68.194.45 DOTDMZ WAS 018 VG.e xt.do t.gov

- 1) Run `nmap -sV -T4 -A -v DOTDMZ WAS 018 VG.e xt.do t.gov`
- 2) Note the hostname in the 443 port scan
- 3) Find this server in the ITSS patch list
- 4) Determine that this is an ITSS manager server.



By **Brent Miller** (squigit)
cheatography.com/squigit/
www.dot.gov

Not published yet.
 Last updated 6th March, 2018.
 Page 1 of 1.

Sponsored by **CrosswordCheats.com**
 Learn to solve cryptic crosswords!
<http://crosswordcheats.com>