Cheatography

Enumeration Cheat Sheet

by djf via cheatography.com/68878/cs/17349/

Alive Hosts

NMAP

```
nmap -sn -n 172.16.0.1\24 | grep " Nma p" | cut -d " " -f 5 > alives
```

NIX

bash/sh

```
for x in {1..25 4..1 };do ping -c 1 172.16.0.$x | grep "64 b" | cut -d" " -f4 >> alive.h osts; done
```

WIN

cmd.exe

```
for /L %i in (10,1,254) do @ (for /L %x in (10,1,254) do @ ping -n 1 -w 172.16.%i.%x 2>nul | find " Rep ly"
s)
```

powershell.exe

```
Foreach($x in 1..255 ){T est -Co nne ction 172.16.0.$x}
```

NMAP

Alives Generation

```
nmap -sn -n | grep " Nma p" | awk $6 > alives.hosts
nmap -sn -n -oN scan.nmap && awk $6 scan.nmap > alives.hosts
```

Very Minimal Footprint with Fragmentation & Decoys

```
nmap -sS --max- retries 0 --scan -delay 3 --os-limit --max- os- tries 1 -T0 -n -Pn -iL target s.txt -vv -f -
 32
```

Conscious Footprint

```
nmap -sS -sN -p1,2-9,39 -Pn -n -T2 -f 192.16 8.0.1\24
```

Aggressive Everything

```
nmap -A -p- 0.0.0.0\0
```

XML Web Presentation

```
nmap -sT -p- 192.16 8.1.5 -oX webpre sen tat ion.xml --webxml
```

By **djf**
cheatography.com/djf/

Published 11th September, 2020.
Last updated 11th September, 2020.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

NMAP Flags/Args

-sn	Alive hosts discovery[1A]	-sU	UDP Scan
-Pn	Assume host is alive	-sT	Full TCP Handshake Sc
-n	Don't resolve IP addresses	-sS	TCP SYN Scan
-R	Always resolve IP addresses	-sA	TCP ACK Scan
-F	Fast amount of ports Scan	-sC	Nmap Scripts
-p-	All ports 1-65355	-sN	TCP NULL Scan
-T[1-5]	Timing speed very slow (1) to very fast (5)	-sF	TCP FIN Scan
--scan -delay [int]	Time between probes	-sV	Service Enumer ation
-f	Fragment Packets (IDS/FW evasion)	-O	OS Type Enumer ation
-D	Decoy hosts traffic	RND:10	10 Random source host
-PS	TCP SYN Ping[2A]	-PA	TCP ACK Ping[2A]
-PU	UDP Ping[3A]	-PE	ICMP Echo Request
-PP	ICMP Timestamp Query[4A]	-PM	ICMP Address Mask Que
-A	Aggressive Scan[6A]	--ttl	Set Time-T o-Live for
--vers ion -light	Versioning intensity: 2	--vers ion-all	Version intensity: 9
--iflist	List interfaces (ifconfig)	--trac eroute	Trace route to destir
--stats every [int]	Time between writing to stdout	--scri pt- upd ate db	Update script db
--data -length [int]	Use with -sU, size of UDP payload	--open	Return only open port
--syst em-dns	Resolve hostnames with localhost	--dns- servers	Specify name server a s
--resume [file]	Scan to resume from output file	--appe nd- output	Append to output file
--ip-o ptions	Specify raw IP frame hex options	Example	--ip-o ptions \x01\x
-sW	TCP Window Scan	-sM	TCP Maimon Scan
-sX	TCP Xmas Scan (all flags)	--scan flags URGAC K	Set TCP Flags

1A. Sends ICMP Echo Req, SYN:443, ACK:80, ICMP Timestamp Req
2A. Destin ation port 80, may specify alternate port with the '-p' flag.
3A. Destin ation port 40125, may specify alternate port with the '-p' flag.
4A. Expects ICMP Code 14 reply, indicates host is available.
5A. Expects ICMP Code 18 reply, indicates host is available.
6A. Includes, OS detection, version scans, script scans, and tracer oute.

By **djf**
cheatography.com/djf/

Published 11th September, 2020.
Last updated 11th September, 2020.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com