

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..254};do ping -c 1 172.16.0.$x | grep "64 b" | cut -d" " -f4 >> alive.hosts; 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 webpresentation.xml --webxml
```



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

Published 11th September, 2020.
Last updated 11th September, 2020.
Page 1 of 2.

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 Scan
-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 Enumeration
-f	Fragment Packets (IDS/FW evasion)	-O	OS Type Enumeration
-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 Query
-A	Aggressive Scan ^{6A}	--ttl	Set Time-To-Live for
--version-light	Versioning intensity: 2	--version-all	Version intensity: 9
--iflist	List interfaces (ifconfig)	--traceroute	Trace route to destination
--stats-every [int]	Time between writing to stdout	--script-update	Update script db
--data-length [int]	Use with -sU, size of UDP payload	--open	Return only open ports
--system-dns	Resolve hostnames with localhost	--dns-servers	Specify name server addresses
--resume [file]	Scan to resume from output file	--append-output	Append to output file
--ip-options	Specify raw IP frame hex options	Example	--ip-options '\x01\x00'
-sW	TCP Window Scan	-sM	TCP Maimon Scan
-sX	TCP Xmas Scan (all flags)	--scan-flags URGACK	Set TCP Flags

1A. Sends ICMP Echo Req, SYN:443, ACK:80, ICMP Timestamp Req

2A. Destination port 80, may specify alternate port with the '-p' flag.

3A. Destination 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 traceroute.



By djf
cheatography.com/djf/

Published 11th September, 2020.
Last updated 11th September, 2020.
Page 2 of 2.

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