Enumeration Cheat Sheet

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

Alive Hosts

NMAP

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

NIX

bash/sh

```
for x in {1..254..1};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 "Reply" && echo 172.16.%i.%x >> alive.hosts)
```

powershell.exe

```
Foreach($x in 1..255){Test-Connection 172.16.0.$x}
```

NMAP

Alives Generation

```
nmap -sn -n | grep "Nmap" | 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 targets.txt -vv -f -D RND:10 --ttl 32
```

Conscious Footprint

```
nmap -sS -sN -p1,2-9,39 -Pn -n -T2 -f 192.168.0.1\24
```

Aggressive Everything

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

XML Web Presentation

```
nmap -sT -p- 192.168.1.5 -oX webpresentation.xml --webxml
```

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 hosts for '-D'
-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[5A]
-A	Aggressive Scan[6A]	--ttl	Set Time-To-Live for packets
--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-updatedb	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 for resolutions
--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\x07\x04\x00*36\x01
-sW	TCP Window Scan	-sM	TCP Maimon Scan
-sX	TCP Xmas Scan (all flags)	--scanflags 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.