Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

Part 1: Reconnaissance (Advanced)

https://nmap.org/

GENERAL USAGE

```
nmap [Scan Type(s)] [Options] {target specification}
```

NOTES

Target specifications can be host names, IP addresses, ranges, networks, etc. (scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254)

Use these options to locate "alive machines" (sometimes only that, sometimes they also return some port / service information)

```
operario@kali:~$ sudo nmap --script targets-sniffer 192.168.20.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:47 CEST
Nmap scan report for 192.168.20.10
Host is up (0.000097s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:67:7A:EF (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.20.1
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.20.1 are closed

Nmap done: 256 IP addresses (2 hosts up) scanned in 29.35 seconds
```

TARGET SPECIFICATION

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

-iL <inputfilename>: Input from file a list of hosts/networks

-iR <num hosts>: Choose random targets

SCRIPT SCAN (https://nmap.org/book/man-nse.html)

-sC: equivalent to --script=default

--script=<NSE scripts>: <NSE scripts> is a comma separated list of directories, script-files or script-categories

--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts (see each script documentation to consult argument names, number, and valid value types)

--script-args-file=filename: provide NSE script args in a file

--script-trace: Show all data sent and received

HOST DISCOVERY OPTIONS (WAYS TO CHECK "ALIVE" MACHINES)

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-Pn: Treat all provided hosts as online -- skip host discovery

-PO[protocol list]: IP Protocol Ping

-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

-sL: List Scan - simply list targets to scan

-sn: Ping Scan - disable port scan

--system-dns: Use OS's DNS resolver

--traceroute: Trace hop path to each host

RECOMMENDED SCRIPT CATEGORIES FOR ADVANCED RECONNAISSANCE (https://nmap.org/nsedoc/)

broadcast: Scripts in this category typically do discovery of hosts not listed on the command line by broadcasting on the local network. Use the newtargets script argument to allow these scripts to automatically add the hosts they discover to the Nmap scanning queue.

https://nmap.org/nsedoc/categories/broadcast.html

RECONOISSANCE EXAMPLES

sudo nmap --script targets-sniffer 192.168.20.0/24

sudo nmap --script broadcast-dropbox-listener 192.168.20.0/24

sudo nmap --script mringo scanme.nmap.org

sudo nmap -iL ips_to_scan.txt

by José Manuel Redondo López