Nmap

Options:

```
nmap -sC -sV -oA nmap 10.10.10.29
nmap -sS -sU -T4 -A -oA nmapscan 10.10.10.20
```

sC --> default scripts
sV --> enumerate version
-sT —> TCP connect scan : very effective but detectable
-sN —> Null scan
-sF --> Fin scan
--> xmas scan ?
--> Idle scan (zombie scan) ?
-Pn --> don’t ping before connect ,default sends ping then connect (can be blocked after the ping)

Port specification:

--top-ports <number> --> scan the first <number> most famous ports
nmap -p 1-65535 --> scan all ports
nmap -p 80,443,100- --> scan 80,443 and from 100 till the end 65535

Responses:

open = syn-ack
closed = reset
filtered = firewall dropped the packet (probably)

To get the categories of all nmap scripts

```
locate -r '\.nse$' | xargs grep categories | grep 'default\|versiom' | grep smb
```

Default scripts location

```
/usr/share/nmap/scripts
```

add --script to use , for example
nmap --script safe -p 445 10.10.10.100 --> safe scripts on port 445 (smb)
nmap -p 80 <host> --script=http* --> this will apply all scripts that has http in them

nmap cheat sheet

https://www.stationx.net/nmap-cheat-sheet/

Get os info from TTL : https://subinsb.com/default-device-ttl-values/