nmap cheat sheet v1.0 by Jimmy Larsson, https://nat0.net

Target specification
Single host by ip: 192.168.1.10
Single host by dns name: scanme.nmap.org
Range: 192.168.1.10-20
Range in any octet: 192.168-169.1-240.20
CIDR/prefix notation: 192.168.1.0/24
Any combination of the above can be stacked as parameters
Targets specified in file: -iL <filename>
Random targets: -iR <number of targets> (use with caution!)
List the specified targets enumerated: -sL (does not scan at all)

Nmap phases
- Target enumeration
- Host discovery (arp/ping)
- Reverse DNS (-n to disable)
- Port scanning
- Version detection (enable with -SV)
- OS Detection (enable with -O)
- trace-route (enable with --trace-route)
- Script scanning (enable with --script)
- Output

Specifying ports to scan
nmap defaults scan the 1000 most common TCP ports
-p <ports>
where <ports> can be a range of ports: 80-85
or multiple ports or ranges separated by commas: 80-85,89,91-99
-F <number> scans only the <number> most common ports

Output during scan
-v for verbosity
-vv for more verbosity
-d for debug

press “v” during scan to increase verbosity level
press “V” during scan to decrease verbosity level

Press Enter during scan to get current status

Output after scan
--open to only list open ports
-oG <filename> to write result to grepable file
-oX <filename> to write result to XML file

tcp scanning techniques

Connect scan: -sT (default)
SYN scan: -sS

Version scanning
-sV to enable version scanning

OS Detection
-O to enable OS detection

Script scanning
--script to enable default set of scripts
--script=<scriptname> to run a specific script