NMAP Cheat sheet:

Command	Description
`nmap <ip> -A -T5nam`	- T0: “Paranoid (0) Intrusion Detection System evasion” - Gets OS, running services, etc *somewhat* quickly
`sudo nmap -T5 -O -p 1-65353 <ip>`	- Most TCP ports - Pretty basic OS detect
`nmap -F <ip>`	- Scans the 100 most common ports - Very fast
`sudo nmap -sT -T5 <ip>`	- Very quick - Gets most ports
`nmap -Pn -A -T5 <ip>`	- Pretty in depth scan
Service and OS Detection	**Description**
`nmap -A <ip>`	Detect OS and Services
`nmap -sV --version-intensity 5 192.168.1.1`	More aggressive Service Detection
`nmap --dns-servers <server-1> <server-2>`	Specifies custom DNS server

https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
https://www.stationx.net/nmap-cheat-sheet/

Could print this:
https://s3-us-west-2.amazonaws.com/stationx-public-download/nmap_cheet_sheet_0.6.pdf