Nmap Cheat Sheet — Quick Reference (2025)

Basic Syntax

```
nmap [Scan Type] [Options] [Target]
```

Example: `nmap -sS -p 80,443 192.168.1.1`

Quick Flags

`-sS`	TCP SYN scan (stealth)
`-sU`	UDP scan
`-sV`	Version detection
`-O`	OS detection
`-A`	Aggressive (OS, version, scripts)
`-T[0-5]`	Timing (0=slow, 5=fast)
`-p`	Port specification
`-oA`	Output all formats

Common Commands

Command	Description
`nmap -sn 192.168.1.0/24`	Ping scan (host discovery, no port scan)
`nmap --top-ports 100 target.com`	Scan the 100 most common ports
`nmap -p- target.com`	Scan all 65535 ports
`nmap -sV -p 22,80,443 target.com`	Version detection on specific ports
`nmap -oA scan_results target.com`	Save output in all formats (XML, grepable, normal)
`nmap -T4 -A target.com`	Fast aggressive scan with OS/version detection

NSE Scripts (Nmap Scripting Engine)

`--script safe`
Run all safe scripts

`--script discovery`
Network discovery scripts

`--script vuln`
Vulnerability detection scripts

`--script http-enum`
Enumerate web directories

`--script ssl-cert`
Retrieve SSL certificate info

Pro Tips

- Use `-Pn` to skip host discovery if firewall blocks pings
- Combine `-sV --version-intensity 5` for thorough version detection
- Use `-v` or `-vv` for verbose output during scans
- Save time with `-F` (fast mode, scans fewer ports)
- Use `--reason` to see why ports are marked open/closed

⚠ **ALWAYS GET PERMISSION BEFORE SCANNING**