Nmap Commands Cheat Sheet

■ *Scan with Decoys (Hide Your IP)*

```
nmap -D RND:10 192.168.1.1
```

Purpose: Makes your scan appear as if it’s coming from multiple IPs instead of just yours.

■ *Scan for Vulnerable Services*

```
nmap --script=vuln 192.168.1.1
```

Purpose: Automatically detects known vulnerabilities in services running on a target.

■ *Timing Template for Speed*

```
nmap -T4 192.168.1.1
```

Purpose: Increases scan speed while keeping accuracy.

■ *UDP Scan (Often Overlooked)*

```
nmap -sU 192.168.1.1
```

Purpose: Finds open UDP ports (services that don’t use TCP).

■ *Detect Heartbleed Vulnerability*

```
nmap -p 443 --script=ssl-heartbleed 192.168.1.1
```

Purpose: Checks if a system is vulnerable to the Heartbleed bug (CVE-2014-0160).

■ *Aggressive Scan (All-in-One Recon)*

```
nmap -A 192.168.1.1
```

Purpose: Enables OS detection, version detection, script scanning, and traceroute in one command.

■ *Scan All Ports*

```
nmap -p- 192.168.1.1
```

Purpose: Covers all 65,535 ports instead of just the top 1,000.

■ *Service Version Detection*

```
nmap -sV 192.168.1.1
```

Purpose: Identifies versions of services running on open ports.

■ *Save Scan Results*

```
nmap -oN scan.txt 192.168.1.1
```

Purpose: Saves output in a readable format for later review.

■ *Top 100 Common Ports*

```
nmap --top-ports=100 192.168.1.1
```

Purpose: Focuses on the 100 most commonly used ports for faster reconnaissance.