Nmap Mastery Guide (Day 1–10)

Day 4: Advanced Basics

■ *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.

Day 4

■ *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).

Day 5: Firewall & IDS Evasion

■ *Fragment Packets*

```
nmap -f target.com
```

Purpose: Splits packets into tiny fragments to bypass firewalls and IDS.

Day 5

■ *Custom MTU*

```
nmap -mtu 24 target.com
```
Purpose: Uses custom packet sizes to evade detection systems.

■ *ACK Scan*

```
nmap -sA target.com
```
Purpose: Maps out firewall rules by sending ACK packets.

Day 6: OS & Version Fingerprinting

■ *Detect OS*

```
nmap -O target.com
```

Purpose: Identifies the operating system running on a host.

Day 6

■ *Aggressive Version Detection*

```
nmap -sV --version-all target.com
```

Purpose: Performs deep service version detection on open ports.

Day 7: Stealth Scanning

■ *SYN Scan*

```
nmap -sS target.com
```

Purpose: Half-open scan that avoids full TCP connections, stealthier against firewalls.

Day 7

■ *Skip Host Discovery*

```
nmap -Pn target.com
```

Purpose: Scans targets even if ICMP echo requests are blocked.

Day 8: NSE Power Moves

■ *HTTP Enumeration*

```
nmap --script=http-enum target.com
```
Purpose: Enumerates common web applications and directories.

Day 8

■ *Anonymous FTP Login*

```
nmap --script=ftp-anon target.com
```
Purpose: Checks if anonymous login is enabled on FTP servers.

■ *SMB OS Discovery*

```
nmap --script=smb-os-discovery target.com
```
Purpose: Retrieves Windows OS information via SMB.

Day 9: Bypassing Rate Limits

■ *Scan Delay*

```
nmap --scan-delay 1s target.com
```
Purpose: Slows scan timing to avoid triggering intrusion detection systems.

Day 9

■ *Limit Retries*

```
nmap --max-retries 2 target.com
```
Purpose: Reduces retries for faster, stealthier scans.

Day 10: Advanced Recon & Hybrid Scans

■ *Full TCP & UDP Scan*

```
nmap -sS -sU -p- -A -T4 target.com
```

Purpose: Comprehensive scan of all ports with version detection, OS detection, and traceroute.

Day 10

■ *Default Scripts + Versions*

```
nmap -sC -sV target.com
```
Purpose: Runs default NSE scripts and version detection for quick recon.

■ *Scan Multiple Targets*

```
nmap -iL targets.txt
```
Purpose: Scans a list of hosts provided in a text file.