📌 Nmap Cheat Sheet for Red Teaming

1. Basic Scanning

Command	Description
nmap <IP>	Top 1000 ports scan karega (default).
nmap -p- <IP>	All 65535 ports scan karega.
nmap -p 21,22,80 <IP>	Specific ports scan karega.

2. Service & Version Detection

Command	Description
nmap -sV <IP>	Service name + version detect karega.
nmap -sV --version-intensity 9 <IP>	Deep version detection (more accurate).

3. OS Detection

Command	Description
nmap -O <IP>	Operating System guess karega.
nmap -A <IP>	Aggressive mode (OS + services + NSE scripts).

4. Timing & Speed

Command	Description
nmap -T4 <IP>	Fast scan (good for LAN).
nmap -T1 <IP>	Slow scan (stealthy).

5. Output Saving

Command	Description
nmap -oN output.txt <IP>	Normal output save karega.
nmap -oX output.xml <IP>	XML output save karega.
nmap -oG output.gnmap <IP>	Grepable output.

6. NSE Scripts (Nmap Scripting Engine)

Command	Description
nmap --script vuln <IP>	Common vulnerability check karega.
nmap --script http-enum <IP>	HTTP directories enumerate karega.
nmap --script ftp-anon <IP>	FTP anonymous login check karega.
nmap --script smb-os-discovery <IP>	SMB service se OS info lega.

7. Stealth Scans

Command	Description
nmap -sS <IP>	SYN scan (stealthy, fast).
nmap -sF <IP>	FIN scan (firewall bypass try).
nmap -Pn <IP>	Host discovery skip (even if ICMP blocked).

8. UDP Scanning

Command	Description
nmap -sU <IP>	UDP scan (slow).
nmap -sU -p 53,161 <IP>	Specific UDP ports.