Task	Nmap command	What it does	Flags description
TCP Full-Open scan (single host) — your example	`nmap -Pn -sT -v 150.1.7.102`	TCP connect (full) scan; no host discovery; verbose.	`-sT` — TCP connect; `-Pn` — skip ping; `-v` — verbose
TCP Half-Open (SYN) scan (single host) — your example	`nmap -Pn -sS -v 150.1.7.102`	SYN (half-open) scan; no host discovery; verbose.	`-sS` — SYN scan; `-Pn` — skip ping; `-v` — verbose
UDP scan (single host) — your example	`nmap -Pn -sU -v 150.1.7.102`	UDP port scan; no host discovery; verbose.	`-sU` — UDP scan; `-Pn` — skip ping; `-v` — verbose
XMAS Tree scan (single host) — your example	`nmap -Pn -sX -v 150.1.7.102`	XMAS (FIN/PSH/URG) probe; no host discovery; verbose.	`-sX` — XMAS flags; `-Pn` — skip ping; `-v` — verbose
TCP Full-Open across subnet — detailed, save output	`nmap -sT -Pn -p- -A -vv 150.1.7.0/24 -oA nmap_fullopen_150.1.7.0_24`	Full connect scan all ports + svc/version/OS; very verbose; save outputs.	`-p-` — all ports; `-A` — svc/vers/OS; `-oA` — save all
TCP SYN across subnet — detailed, save output	`nmap -sS -Pn -p- -A -vv 150.1.7.0/24 -oA nmap_syn_150.1.7.0_24`	SYN scan all ports + svc/version/OS; save outputs.	`-sS` — SYN scan; `-p-` — all ports; `-A` — svc/vers/OS
XMAS across subnet — verbose, save	`nmap -sX -Pn -p- -vv 150.1.7.0/24 -oA nmap_xmas_150.1.7.0_24`	XMAS scan all ports; verbose; save outputs.	`-sX` — XMAS flags; `-p-` — all ports; `-vv` — extra verbose
Comprehensive single host (svc/version + OS)	`nmap -sS -Pn -p- -A -vv 150.1.7.102 -oA nmap_scan_150.1.7.102`	Wide SYN scan with service/version and OS detection; saved outputs.	`-A` — svc/vers/OS; `-oA` — save
Service/version exhaustive probe (single host)	`nmap -sV -Pn -p 1-65535 --version-all -vv 150.1.7.102 -oN nmap_sV_150.1.7.102.txt`	Exhaustive version detection across all ports; normal output file.	`-sV` — svc/version detect; `--version-all` — extensive probes; `-oN` — normal file

Task	Nmap command	What it does	Flags description
Quick top-ports scan across subnet	`nmap -sS -T4 --top-ports 1000 150.1.7.0/24 -oN nmap_quick_150.1.7.0_24`	Faster scan of the 1000 most common ports; quicker results.	`-T4` — faster timing; `--top-ports` — common ports
Fragmentation Scan	`nmap -f 150.1.7.102`	Sends fragmented packets to evade firewalls and IDS by splitting TCP headers.	`-f` Fragments the packets
Decoy Scan	`nmap -D RND:10 150.1.7.102`	Uses decoy IP addresses to obscure the source of the scan, making it harder to trace.	`-D` Decoy `-RND:10` 10 Decoy ips rounds
Source IP Manipulation	`nmap --source-port 80 150.1.7.102`	Sets a specific source port to bypass firewalls that allow traffic from trusted ports.	`--source-port` Fixed Ports (Because Servers use them) easily bypasses the Firewall
IDLE-Zombie Scan	`nmap -sI <Zombie ip> 150.1.7.102`	Uses a third-party host (zombie) to send packets, hiding the attacker's IP.	`-sI` Acts like we are the legit. By probing using insider's IP
ACK scan	`nmap -sA 150.1.7.102`	Firewall detection	`-sA` Determines if a firewall is present
TCP Null scan	`nmap -sN 150.1.7.102`	Bypasses some firewalls/IDS	`-sN` Sends packets with no flags set
TCP FIN scan	`nmap -sF 150.1.7.102`	Bypasses some firewalls/IDS	`-sF` Sends packets with FIN flag set
Scan Delay	`nmap --scan-delay <time> 150.1.7.102`	Adjust scan delay	Slows down scan to avoid detection by IDS/IPS.
Data Length	`nmap --data-length <num> 150.1.7.102`	Append random data to packets	Alters packet size to evade detection.