nikto -h example.com – Scans for common vulns.

nikto -h example.com -p 80,443 – Targets HTTP and HTTPS.

nikto -h https://example.com (https://example.com) -ssl – Scans secure sites.

nikto -h example.com -nossl – For non-SSL only. nikto -update – Keeps scans current.

nikto -h example.com -maxtime 600 – Limits to 10 minutes.

nikto -h example.com -timeout 10 – Avoids hanging on slow responses.

nikto -h 192.168.1.1 -vhost example.com – For name-based hosting

nikto -h example.com -Tuning 49 – XSS and SQL injection only.

nikto -h example.com -useragent "Mozilla/5.0"

nmap -sn 192.168.1.0/24 – Discovers hosts on the subnet.

nmap -Pn example.com – Scans even if ping fails.

nmap -PS80,443 192.168.1.1-255 – Probes common ports for responses

nmap -PA 192.168.1.0/24 – Bypasses some firewalls

nmap -PU53 10.0.0.1 – Checks DNS port for live hosts

nmap 192.168.1.1 – Scans top 1000 ports.

nmap -sS example.com – Fast and less detectable.

nmap -sT 10.0.0.1 – When SYN isn't possible (non-root).

nmap -sU 192.168.1.1 – Checks UDP ports like DNS/NT

nmap -p 1-1024,8080 192.168.1.0/24 – Targets common and custom ports

nmap -F example.com – Quick recon.

nmap -sC 10.0.0.1 – Basic scripting engine use

nmap -sV 192.168.1.1 versions

nmap -A example.com – All-in-one for detailed info.

nmap --version-intensity 5 10.0.0.1 – Balances speed and accuracy.

nmap -O 192.168.1.1 – Detects Windows/Linux/etc.

nmap -O --osscan-guess example.com – When fingerprint isn't exact.

nmap -f 192.168.1.1 – Evades some packet filters.

nmap -D RND:10 example.com – Sends from random fake IPs

nmap --source-port 53 10.0.0.1 – Uses trusted port like DNS

nmap -g 80 192.168.1.0/24 – Web port spoof.

nmap -MTU 24 example.com – Small packets to slip through.

nmap -oN scan.txt 192.168.1.1 – Human-readable log.

nmap -oX scan.xml example.com – For tools like Metasploit.

nmap -oG scan.grep 10.0.0.1 – Easy to parse with grep.

nmap -vv 192.168.1.0/24 – More details during scan.

nmap --script http-enum 192.168.1.1 – Enumerates web dirs.

nmap --script=vuln 10.0.0.1 – Looks for known vulnerabilities