Task-2 — Network Security & Scanning: Command Reference

Cheat sheet with ready-to-run commands, short explanations, and suggested screenshot filenames. Use this inside your Kali + Metasploitable lab.

Lab Overview

Machine	Role	Typical IP	Notes
Kali Linux	Attacker	192.168.56.101	Tools: nmap, wireshark, OpenVAS
Metasploitable2	Target	192.168.56.102	Common vulnerable services for practice

1. Passive Reconnaissance

whois — Get domain registration info *Screenshot: s21_passive_recon.png*
nslookup — DNS lookup
dig ANY — Advanced DNS query
theHarvester -d -l 100 -b google — Gather emails & subdomains
Google dork example: — site:example.com filetype:pdf password

2. Active Reconnaissance — Network Discovery

ping -c 4 192.168.56.102 — Check connectivity *Screenshot: s22_netdiscover.png*
arp -a — List discovered hosts
sudo netdiscover -r 192.168.56.0/24 — Scan local subnet for active hosts

3. Port & Service Scanning (Nmap)

Common flags: -sS (SYN), -sU (UDP), -sV (service/version), -O (OS), -p- (all ports), -Pn (skip discovery), -T4 (timing), -oN/-oX (output).

sudo nmap -sS -T4 192.168.56.102 Quick TCP scan - *s23_nmap_full.png*

sudo nmap -sS -p- -T4 192.168.56.102 -oN scans/tcp_full.txt Full port scan (all ports)

sudo nmap -sS -sV 192.168.56.102 -oN scans/svc_detect.txt Service/version detection

sudo nmap -O 192.168.56.102 -oN scans/os_detect.txt OS detection

sudo nmap -sS -sV -O -p- -T4 192.168.56.102 -oA scans/full_combo Combined full scan (TCP/service/OS)

4. Vulnerability Scanning (OpenVAS / Nessus)

gvm-setup / gvm-start — OpenVAS / Greenbone setup on Kali; then open https://127.0.0.1:9392/ to access the dashboard. *Screenshot: s24_openvas_dashboard.png*
Nessus — Install Nessus Essentials, access at https://localhost:8834, create scan, run against target.

5. Packet Capture with Wireshark

Steps: Open Wireshark → select host-only interface (e.g., enp0s8) → Start capture. Generate traffic (curl or browser). Apply filters: ip.addr==192.168.56.102, http, ftp, dns, tcp.flags.syn==1. Save as pcaps/task2_capture.pcap.
Screenshot: s25_wireshark_http.png

6. Firewall Basics (iptables)

sudo iptables -L — View current rules
sudo iptables -A INPUT -p tcp --dport 21 -j DROP — Block incoming FTP (port 21)
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT — Allow HTTP (port 80)
sudo iptables-save > /etc/iptables.rules — Save rules to file
Screenshot: s26_iptables_rules.png

7. Analyzing & Reporting

Create a short findings table in your report mapping Port → Service → Version → Risk → Recommendation. Example row: Port: 21/tcp | Service: vsftpd 2.3.4 | Risk: HIGH | Recommendation: Disable FTP / patch service. Include Nmap outputs, vulnerability report (OpenVAS/Nessus), and Wireshark capture as evidence. Save outputs in a structured repo.
Suggested screenshot: s27_scan_table.png

8. Useful One-Liners

`sudo nmap --top-ports 10 192.168.56.102 -oN scans/top10.txt` — `Save top 10 open ports`

`sudo nmap -sn 192.168.56.0/24 -oN scans/host_discovery.txt` — `Find hosts up in subnet`

`xsltproc scans/full_combo.xml -o scans/full_combo.html` — `Convert XML output to HTML using xsltproc`

`sudo nmap --script vuln 192.168.56.102 -oN scans/vuln_check.txt` — `Run NSE vulnerability scripts`

9. Optional Add-ons (extra tools)

masscan — Ultra-fast port scanner
`sudo masscan 192.168.56.102 -p1-65535 --rate=1000` *s29_masscan.png*

hping3 — Packet crafting & SYN flood simulation
`sudo hping3 -S 192.168.56.102 -p 80 -i u1000`

netcat — Manual port check
`nc -vz 192.168.56.102 80`

curl -I — Header check
`curl -I http://192.168.56.102`

End of Task-2 Command Reference