Task-2 — Network Security & Scanning

TimeLine: Days 13–24

Objective:

Perform passive & active reconnaissance, host discovery, port/service enumeration, vulnerability scanning, and packet capture in an isolated lab (Kali → Metasploitable/DVWA). Produce scan outputs, vuln reports, pcaps, notes, and prioritized remediation recommendations.

Steps (high level):

• Set up/verify lab network (Host-Only): confirm Kali and target IPs.
• Passive recon: whois, nslookup, dig, basic OSINT.
• Active discovery: netdiscover / nmap -sn to find live hosts.
• Port & service scanning: nmap -sS -p- -T4, then -sV and -O.
• Run NSE vulnerability scripts: nmap --script vuln.
• Vulnerability assessment: run OpenVAS / Nessus and export report.
• Packet capture: run Wireshark on host-only interface while generating HTTP/FTP traffic.
• Firewall demo: simple iptables rules to block/allow ports.
• Save & convert results (Nmap XML → HTML), write findings & mitigations.
• Prepare deliverables: scans, vuln report, pcaps, notes; push to GitHub.

Key commands (copy / paste):

```
# discovery sudo netdiscover -r 192.168.56.0/24 sudo nmap -sn 192.168.56.0/24 -oN scans/host_discovery.txt # full scan + service + OS sudo nmap -sS -sV -O -p- -T4 192.168.56.102 -oA scans/full_combo # NSE vuln scripts sudo nmap --script vuln 192.168.56.102 -oN scans/vuln_check.txt # convert xml to html xsltproc scans/full_combo.xml -o scans/full_combo.html # start OpenVAS (example) sudo gvm-start # capture with Wireshark (GUI) and save as: # pcaps/task2_capture.pcap # iptables demo sudo iptables -A INPUT -p tcp --dport 21 -j DROP sudo iptables -L -n -v
```

Tools used:

Kali Linux (attacker); Metasploitable2 / DVWA (target); Nmap, Wireshark, OpenVAS / Nessus, netdiscover, nc, curl, iptables

Theory (concise):

OSI & TCP/IP — why it matters
OSI model is a conceptual map for networking. For scanning and packet analysis, focus on Layer 3 (Network/IP) for addressing & discovery, Layer 4 (Transport/TCP/UDP) for ports & flags used in scans, and Layer 7 (Application) for service behavior inspected with Wireshark.

Reconnaissance: passive vs active
Passive recon gathers public info (DNS, WHOIS) without touching the target (stealthy). Active recon (ping sweeps, port scans) sends packets and reveals hosts & services (accurate but noisy).

Scanning techniques & Nmap basics
SYN scan (-sS) is a stealth TCP scan; UDP scan (-sU) checks UDP services; service/version detection (-sV) probes banners; OS detection (-O) fingerprints the system; -p- scans all ports; -T4 sets timing.

Nmap Scripting Engine (NSE)
NSE provides scripts for discovery & vuln checks (e.g., --script vuln). Use scripts as leads; always verify manually.

Vulnerability scanning principles
Scanners (OpenVAS/Nessus) map services to known CVEs and prioritize findings. They can have false positives—manual verification required.

Packet capture & analysis (Wireshark)

Capture on the attacker-target interface. Use filters (ip.addr==, http). Follow TCP/HTTP streams to view request/response. Save PCAPs as evidence.

Firewalls & basic hardening
iptables rules can block or allow ports. Hardening includes removing unused services, patching, enforcing least privilege, and secure configurations (e.g., SSH over Telnet).

Risk triage & reporting
Prioritize by Exploitability and Impact. For each issue include evidence, risk, recommendation, and references.

Ethics & legal
Test only systems you own or have written permission to test. Unauthorized scanning is illegal.

Deliverables:

- scans/full_combo.nmap / scans/full_combo.html
- scans/vuln_check.txt (NSE output)
- vuln_reports/openvas_report.html (export)
- pcaps/task2_capture.pcap (Wireshark) — track with Git LFS or provide external link
- notes/task2_analysis.md (findings, risk ratings, mitigations)
- GitHub repo link (with all artifacts)

Prepared for ApexPlanet Internship — Task 2