Task 4 — Network Security & Vulnerability Assessment

Objective

To perform network scanning, service enumeration, and vulnerability assessment in a secure lab environment and analyze the results to identify potential risks, false positives, and appropriate mitigation steps.

Learning Outcomes

• Understand network topology and host discovery.

• Use Nmap, Zenmap, and OpenVAS/Nessus for vulnerability analysis.

• Interpret scan results, risk ratings, and CVSS scores.

• Verify findings manually using terminal tools like curl and nc.

• Propose security hardening recommendations.

Lab Setup

Component	Role	Example IP	Description
Kali Linux	Attacker / Scanner	192.168.56.101	Performs scans & analysis
Target VM	Victim	192.168.56.102	Exposed services for testing
Network Type	Host-Only	192.168.56.0/24	Isolated virtual network

Phase 1 — Network Discovery

Objective: Identify live hosts and reachable systems within the subnet.

Commands:

```
sudo netdiscover -r 192.168.56.0/24 -P -o scans/host_discovery.txt sudo nmap -sn
192.168.56.0/24 -oN scans/host_discovery_nmap.txt
```

Result: Discovered target IP (e.g., 192.168.56.102) as the active host for further scanning.

Phase 2 — Port Scanning & Service Enumeration

Objective: Identify open ports, services, and OS details.

Commands:

```
sudo nmap --top-ports 100 -T4 192.168.56.102 -oN scans/top100.txt sudo nmap -sS -sV -O -p-
-T4 192.168.56.102 -oA scans/full_combo
```

Findings Example:

Port | Service | Version | State | Observation 21/tcp | vsftpd | 2.3.4 | Open | Vulnerable to backdoor 22/tcp | ssh | OpenSSH 4.7p1 | Open | Secure but outdated 80/tcp | http | Apache 2.2.8 | Open | Potential misconfigurations

Tools Used: Nmap, Zenmap GUI. Purpose: Build a service map of the target.

Phase 3 — Vulnerability Scanning

Objective: Detect known vulnerabilities using automated tools.

Using Nmap NSE Scripts:

```
sudo nmap --script vuln 192.168.56.102 -oN scans/vuln_check.txt
```

Using OpenVAS (Greenbone):

```
sudo gvm-setup sudo gvm-start # Access via: https://127.0.0.1:9392/
```

Performed Steps: Added target host, created scan task, ran scan, analyzed report for critical/high vulnerabilities.

Findings Snapshot example: vsftpd 2.3.4 backdoor (Critical), Apache Directory Listing (High), SMB Null Session (High).

Phase 4 — Manual Verification

Objective: Validate automated findings manually.

Examples:

```
nc -v 192.168.56.102 21 curl -I http://192.168.56.102/ smbclient -L \\192.168.56.102
```

Purpose: Confirm true positives and discard false alarms.

Phase 5 — Packet Capture & Traffic Analysis

Tool: Wireshark. Steps: 1. Start capture on the host-only adapter. 2. Perform scans and access services. 3. Stop capture and analyze packets.

Useful Filters: ```ip.addr == 192.168.56.102 tcp.flags.syn==1 http ftp```

Outcome: Verified active TCP connections and service responses.

Phase 6 — Security Hardening Demonstration

Using iptables:

```
sudo iptables -A INPUT -p tcp --dport 21 -j DROP sudo iptables -L -n -v
```

Mitigation Recommendations: Disable unnecessary services, apply updates, enforce firewall policies, restrict admin access, use SSH keys.

Risk Analysis & Prioritization

Exploitability + Impact => Priority.

Critical: Exploitable remotely (RCE) — highest priority.

High: Auth bypass / data leakage.

Medium: Information disclosure.

Low: Minor misconfiguration.

Remediate high-impact items first (patch, disable service, firewall), then medium, then low.

Reporting Structure

Each finding should include Title, Affected Host, Evidence, Risk Rating, Impact, Recommendation, References.

Example Entry:

```
Title: vsftpd 2.3.4 Backdoor Vulnerability Affected Host: 192.168.56.102:21 Evidence: Found
in Nmap and OpenVAS scan reports Risk Rating: Critical Impact: Allows remote code execution
Recommendation: Disable FTP or update to latest secure version References: CVE-2011-2523
```

Deliverables

scans/full_combo.* — Nmap outputs (nmap, xml, gnmap, html).

scans/vuln_check.txt — NSE script output.

vuln_reports/openvas_report.html — exported OpenVAS/Nessus report.

pcaps/task4_capture.pcap — Wireshark capture (use Git LFS or external link if large).

notes/task4_analysis.md — Analysis & risk documentation.

scripts/helpers.sh — optional helper commands.

Ethics & Legal Disclaimer

All scanning and vulnerability testing were performed only on authorized lab machines within an isolated network.

Unauthorized scanning or exploitation of external systems is illegal and strictly prohibited.

Prepared by: [Your Name] — ApexPlanet Cybersecurity Internship — Task 4