Conducting Vulnerability Assessment and Penetration Testing on a Simulated Web Application Environment

1. Executive Summary

Objective:

Conduct a controlled vulnerability assessment and penetration test on a simulated FinTech web application to identify security weaknesses, recover planted flags as proof-of-concept, and provide prioritized remediation guidance.

Top findings:

- Open SSH service detected on 10.0.2.2 (OpenSSH 8.9p1 Ubuntu) — medium risk.
- Additional TCP ports on 10.0.2.2 (2289, 35768, 51078) found closed but initially exposed.
- DNS server at 10.0.2.1 (port 53) available, other ports mostly closed.
- No HTTP services detected on 10.0.2.15 (ports 80/443), limiting web-based tests.

Flags recovered:

- flag_hits.txt contains 1 flag (15 bytes) from malware_extracted repository.

2. Problem Statement & Motivation

FinTech applications handle sensitive financial and personal data. Ensuring these applications are free from exploitable vulnerabilities before production is critical. This lab simulates a realistic pre-release environment with intentionally vulnerable services to train penetration testing skills and safely recover planted flags.

3. Scope & Limitations

Scope:

- Target VM network (10.0.2.1, 10.0.2.2, 10.0.2.6, 10.0.2.15).
- Services: HTTP/HTTPS, SSH, DNS, and other TCP ports discovered.
- Local malware_extracted files and flag recovery.

Limitations:

- No destructive actions were performed; HTTP tests failed due to closed ports on 10.0.2.15.

- Only accessible services were scanned; no external network interaction.

4. Environment & Tools

AttackerV M: Kali Linux
Target VMs: 10.0.2.1, 10.0.2.2, 10.0.2.15
Tools Used: Nmap, Netcat, dig, curl, Python3 HTTP server, zip/unzip, bash scripting

5. Methodology

1. Prepared pentest_outputs folder structure for organized scanning results.
2. Conducted Nmap scans for HTTP ports (80/443) and full TCP port ranges.
3. Used curl to probe HTTP services.
4. Extracted flags from malware_extracted directory using file search scripts.
5. Documented findings in VAPT_Report_Sanjana.txt.
6. Packaged all outputs, flags, and reports into submission_project_final.zip.

6. Reconnaissance Summary

Nmap TCP Scan Findings:

10.0.2.1:

53/tcp open domain

10.0.2.2:

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.13

2289/tcp closed dict-lookup

35768/tcp closed unknown

51078/tcp closed unknown

10.0.2.15:

- No HTTP or other TCP services detected on ports 80/443.

DNS Check (dig @10.0.2.1):

- No DNS answer returned.

SSH Banner (10.0.2.2):

SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13

7. Findings

Finding 1 — SSH Service

- **IP/Port:** 10.0.2.2 / 22
- **Service:** OpenSSH 8.9p1 Ubuntu
- **Impact:** Medium — standard SSH; ensure strong passwords/key authentication.
- **Remediation:** Use key-based authentication, disable root login, monitor for brute force attempts.

Finding 2 — Closed Additional Ports

- **IP/Ports:** 10.0.2.2 / 2289, 35768, 51078
- **Service:** Initially detected, all closed after banner scan.
- **Impact:** Low — confirm no rogue services running.
- **Remediation:** Ensure firewall rules restrict unexpected ports.

Finding 3 — No HTTP Service on Target VM

- **IP/Port:** 10.0.2.15 / 80,443
- **Result:** Connection failed
- **Impact:** Testing web-based vulnerabilities not possible; HTTP service not running.
- **Remediation:** Enable service if testing web vulnerabilities, or document as unavailable.

Finding 4 — Flags Recovery

- **Source:** malware_extracted folder on attacker VM.
- **Command:** find ~/malware_extracted -type f -name '*.txt' -exec grep -i 'flag{' {} \; > ~/flag_hits.txt
- **Flag:** Stored in flag_hits.txt (15 bytes).

8. Recommendations

1. Harden SSH: disable password login, use keys.
2. Verify no unnecessary services listening on unexpected ports.
3. Maintain proper network segmentation and firewall rules.
4. Document service availability (HTTP not running) for completeness.
5. Secure storage of flags and sensitive test data.

9. Appendix — Key Commands Used

TCP port scanning

nmap -Pn -p 80,443 --script=http-title,http-headers,http-enum -oN ~/pentest_outputs/10.0.2.15/nmap_http.txt 10.0.2.15

nmap -Pn -sT -p- -T4 -oN ~/pentest_outputs/10.0.2.1/full_tcp_10.0.2.1.txt 10.0.2.1

nmap -Pn -sV --script=banner -p 22,2289,35768,51078 -oN ~/pentest_outputs/10.0.2.2/ports_22_others.txt 10.0.2.2

SSH Banner Retrieval

timeout 3 bash -c 'echo | nc -w 3 10.0.2.2 22' > ~/pentest_outputs/10.0.2.2/ssh_banner.txt

DNS check

dig @10.0.2.1 any +noall +answer > ~/pentest_outputs/10.0.2.1/dig_any.txt 2>/dev/null

Flag recovery

find ~/malware_extracted -type f -name '*.txt' -exec grep -i 'flag{' {} \; > ~/flag_hits.txt

10. Conclusion

The assessment successfully identified available services, open and closed ports, and recovered the planted flag. HTTP testing was not possible due to unavailable web service on 10.0.2.15. Recommended hardening focuses on SSH, port management, and network documentation. All outputs and evidence have been packaged in submission_project_final.zip for submission.