Capstone Project 3 Penetration Test Report Template

[Acme Corp] Security Assessment Report
Date: [08/06/2025]
Prepared By: [Alexander Focsha]

---

1. Confidentiality Statement

This document contains proprietary and confidential information. Unauthorized duplication or distribution is prohibited. Access is restricted to authorized personnel only.

2. Disclaimer

This penetration test represents a snapshot in time and reflects findings based on the assessment period. The results do not account for changes made after the engagement.

3. Contact Information

- **Name**: Alexander Focsha
- **Title**: Junior Penetration Tester
- **Contact Information**:
    - Email: pitbee04@gmail.com
    - Phone: (267) 701-6539

---

4. Scope

In-Scope Assets:

- Metasploitable 3 VM (IP: 192.168.1.100)
- Services: SSH (Port 22), FTP (Port 21), HTTP (Port 80), PostgreSQL (Port 5432), and other outdated services.

Scope Exclusions:

- No external services or production systems were tested.
- Internal documentation systems were not included in the assessment.

Client Allowances:

- Test accounts provided:
    - Username: msfadmin
    - Password: msfadmin

---

5. Executive Summary

- **Total vulnerabilities identified**: 5
- **Key risks**: Exploitable services could allow unauthorized access and data leakage.
- **Overall recommendation**: Immediate patching of known vulnerabilities, implementation of strong password policies, and regular security audits.

---

6. Methodology

- **Reconnaissance**: Conducted network scanning using Nmap to identify active services and open ports on the Metasploitable 3 VM.
- **Scanning**: Utilized OpenVAS for vulnerability scanning to identify weaknesses across the services.
- **Exploitation**: Leveraged Metasploit Framework to exploit the identified vulnerabilities.
- **Post-exploitation**: Evaluated the level of access gained and assessed potential lateral movement opportunities within the environment.

---

7. Findings Summary

Vulnerability	Severity	Impact	Affected Systems	Recommendation
Outdated SSH	High	Remote access	192.168.1.100	Patch to the latest version of OpenSSH.
Unsecured FTP	Medium	Unauthorized access	192.168.1.100	Configure FTP with secure authentication.
SQL Injection	High	Data leakage	Web App (Port 80)	Implement input validation and sanitization.
Default Credentials	High	Unauthorized access	SSH, FTP	Enforce password policy; change defaults.
Open Ports	Medium	Increased attack surface	192.168.1.100	Close unused ports and services.

---

8. Exploitation Details

- **Vulnerability**: Outdated SSH
  - **What was found**: SSH version 6.6p1, known vulnerabilities (CVE-2014-1473).
  - **How it was exploited**: Used Metasploit's `exploit/unix/ssh/sshd` module to gain remote access.

---

9. Security Strengths

- The firewall is configured to restrict access to sensitive services.
- Regular updates to firewall rules are maintained.

---

10. Security Weaknesses

- Critical vulnerabilities in outdated services expose the system to remote attacks.
- Use of default credentials across multiple services significantly increases risk.

---

11. Remediation Recommendations

- **Outdated SSH**: Upgrade OpenSSH to the latest stable version. (High Priority)
- **Unsecured FTP**: Configure FTP to require secure authentication methods like FTPS. (Medium Priority)
- **SQL Injection**: Sanitize all user inputs to prevent injection attacks. (High Priority)
- **Default Credentials**: Change all default passwords to complex passwords. (High Priority)
- **Open Ports**: Conduct a review of active services and disable those that are unnecessary. (Medium Priority)

---

12. Conclusion & Reflection

- **What went well**: Effective use of tools led to quick identification of multiple vulnerabilities.
- **What was challenging**: Difficulty in exploiting certain vulnerabilities due to environmental constraints.
- **What you'd do differently next time**: Plan for more extensive reconnaissance to identify potential attack vectors earlier.

Change Log

- Updated Findings Table based on peer suggestion to clarify CVSS score explanation.