**Vulnerability Assessment Report**

**Client Name**: Al NAEES Corporation  
**Prepared by**: Sheharyar Security Solutions  
**Date**: September 11, 2024

**Table of Contents**

1. Executive Summary
2. Scope of Assessment
3. Vulnerability Summary
4. Detailed Findings
5. Tools and Methodologies Used
6. Risk Assessment
7. Recommendations
8. Conclusion
9. Appendices

**1. Executive Summary**

The vulnerability assessment conducted for AL NAFEES Corporation focused on identifying potential security gaps within the corporate network and associated systems. The assessment identified 10 critical vulnerabilities, 5 high-severity issues, and several medium and low-risk weaknesses. These vulnerabilities, if exploited, could lead to unauthorized access, data breaches, and system compromise. Immediate attention is required for the most severe vulnerabilities to mitigate potential risk.

**2. Scope of Assessment**

* **Assets Assessed**: Corporate network, internal servers, firewall configurations, and external-facing web applications.
* **Timeframe**: September 1–5, 2024.
* **Methodology**: Automated scans (Nmap, OpenVAS) and manual analysis for validation of results.

**3. Vulnerability Summary**

| **Severity** | **Number of Vulnerabilities** |
| --- | --- |
| Critical | 10 |
| High | 5 |
| Medium | 8 |
| Low | 3 |

**4. Detailed Findings**

**Vulnerability 1: SQL Injection on Web Application Login (Critical)**

* **Severity**: Critical
* **Description**: The login page of the corporate web application is vulnerable to SQL injection. An attacker can manipulate SQL queries by entering crafted input into form fields, which could result in unauthorized access to the application database.
* **Impacted Assets**: Web Application (IP: 192.168.1.10)
* **Evidence**: During the assessment, a manual SQL injection attack was performed, confirming the vulnerability. See the attached screenshot (Appendix A) for the output of the injection attack.
* **Risk Impact**: Unauthorized access to sensitive data, including usernames and passwords, leading to potential data breaches and compromised business operations.
* **Likelihood**: High
* **Remediation Recommendation**: Implement parameterized queries or use prepared statements in the login form to sanitize user input. Review all input fields for potential injection points.

**Vulnerability 2: Outdated OpenSSL Version (High)**

* **Severity**: High
* **Description**: The OpenSSL library installed on internal servers (version 1.1.0) is outdated and vulnerable to known attacks, such as Heartbleed.
* **Impacted Assets**: Internal Servers (IP: 192.168.1.20, 192.168.1.21)
* **Evidence**: Scan results show that OpenSSL 1.1.0 is installed on multiple servers. See Appendix B for the full scan report.
* **Risk Impact**: Attackers could exploit this vulnerability to eavesdrop on communications, steal data, or conduct man-in-the-middle attacks.
* **Likelihood**: Medium
* **Remediation Recommendation**: Update OpenSSL to the latest stable version (1.1.1 or higher) across all servers.

**Vulnerability 3: Unencrypted FTP Traffic (Medium)**

* **Severity**: Medium
* **Description**: The corporate network is using FTP for file transfers without encryption, exposing file data to potential interception.
* **Impacted Assets**: FTP Server (IP: 192.168.1.30)
* **Evidence**: Network scans reveal traffic over port 21 without encryption (See Appendix C).
* **Risk Impact**: Unencrypted FTP traffic could allow attackers to capture sensitive files, usernames, and passwords over the network.
* **Likelihood**: Medium
* **Remediation Recommendation**: Replace FTP with secure protocols such as SFTP or FTPS to ensure data is encrypted during transfer.

**Vulnerability 4: Weak Password Policy (Low)**

* **Severity**: Low
* **Description**: The current password policy allows users to create weak passwords, with a minimum of 6 characters and no enforced complexity requirements.
* **Impacted Assets**: Entire corporate network (Domain Controllers)
* **Evidence**: During the assessment, password complexity was tested using a brute-force attack on low-privileged accounts. Multiple weak passwords were successfully cracked (See Appendix D).
* **Risk Impact**: Weak passwords could allow unauthorized access to network resources.
* **Likelihood**: Low
* **Remediation Recommendation**: Implement stronger password policies with a minimum length of 12 characters, requiring a mix of uppercase letters, numbers, and special characters.

**5. Tools and Methodologies Used**

* **Nmap**: Used to scan the network and identify open ports and services.
* **OpenVAS**: Used for vulnerability scanning to detect known weaknesses in the system.
* **Manual Testing**: Performed for SQL injection and password policy validation.

**6. Risk Assessment**

A risk matrix was developed to prioritize vulnerabilities based on their impact and likelihood. The most critical issues involve the SQL injection vulnerability and outdated OpenSSL versions, which present a significant risk to the business.

| **Vulnerability** | **Impact** | **Likelihood** | **Risk Level** |
| --- | --- | --- | --- |
| SQL Injection on Web Application | High | High | Critical |
| Outdated OpenSSL Version | High | Medium | High |
| Unencrypted FTP Traffic | Medium | Medium | Medium |
| Weak Password Policy | Low | Low | Low |

**7. Recommendations**

1. **SQL Injection Fix**: Implement parameterized queries and input validation across all user input fields. This should be addressed immediately.
2. **OpenSSL Update**: Patch and update all servers running outdated OpenSSL libraries to prevent potential data theft.
3. **Secure File Transfers**: Implement SFTP or FTPS protocols to ensure secure data transfer within the network.
4. **Strengthen Password Policies**: Enforce a strong password policy with more stringent complexity requirements across all systems.

**8. Conclusion**

The vulnerability assessment uncovered several critical security flaws in AL NAFEES Corporation's network, notably the SQL injection vulnerability and outdated OpenSSL libraries. Addressing these vulnerabilities promptly will significantly enhance the organization's security posture. Additional improvements, such as stronger password policies and encrypted communications, will further reduce the likelihood of security breaches.

**9. Appendices**

* **Appendix A**: SQL Injection Test Results
* **Appendix B**: OpenSSL Vulnerability Scan Report
* **Appendix C**: Network Scan Results for FTP Traffic
* **Appendix D**: Password Brute Force Test Results