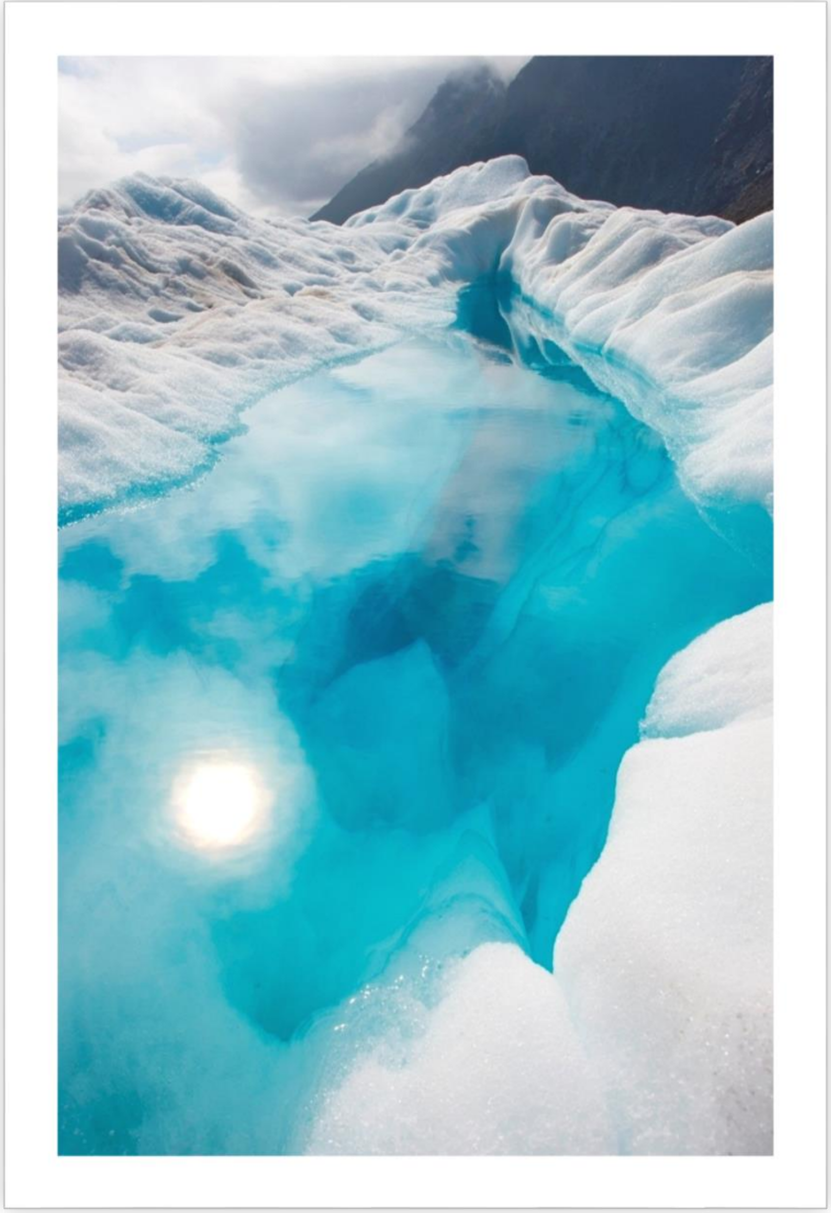

VULNERABILITY ASSESSMENT REPORT FOR ABC SecureBank

ASSESSOR: ALIYU EGWA USMAN COMPANY: EXTION INFOTECH

Position | Cyber security intern | December 1, 2024

Vulnerability Assessment Report Client: ABC Securebank

EXECUTIVE SUMMARY

This report provides the results of a network vulnerability assessment for ABC SecureBank, conducting using Nmap. The objective was to identify potential security vulnerability that could be exploited by malicious entities.

METHODOLOGY

1. **Nmap scanning:**
    - A comprehensive network scan was performed using Nmap to identify open ports, services running on those ports, and potential vulnerabilities.
    - Specific Nmap commands used: nmap -sS -sV -O –script vuln {41.80.37.16}

      ABCSecureBank_vulnassessment.txt
    -
2. **Vulnerability analysis:**
    - Analyzed the scan result to identify known vulnerabilities associated with detect services and software versions.

FINDINGS

high-Risk Vulnerabilities

1. **Open port 80 (HTTP)**
    - **Description:** Web server running Apache httpd 2.2.15
    - **Vulnerability:** Outdated software version with known vulnerabilities.
    - **Recommendation:** upgrade to the latest version of Apache.
    -

Medium-Risk Vulnerabilities

1. **Open port 25 (SMTP)**
    - **Description:** Mail server detected.
    - **Vulnerability:** possible open relay configuration.
    - **Recommendation:** configure the mail server to prevent open relay.
2. **Open port 110 (POP3)**
    - **Description:** Mail server detected.
    - **Vulnerability:** unauthorized access and data interception.

- **Recommendation:** secure POP3 service properly and software update with latest security patches.

3. **Open port 143 (IMAP)**
    - **Description:** Dovecot IMAP server detected
    - **Vulnerability:** unencrypted communication.
    - **Recommendation:** use IMAP over SSL/TLS (port 993) for secure communication.
4. **Open port 443 (SSL/HTTP)**
    - **Description:** SSL/TLS service detected.
    - **Vulnerability:** weak SSL/TLS configuration
    - **Recommendation:** Update SSL/TLS configuration to use strong ciphers and protocols.
5. **Open port 465 (SSL/SMTP)**
    - **Description:** Mail server detected.
    - **Vulnerability:** possible open relay configuration.
    - **Recommendation:** configure the mail server to prevent open relay.
6. **Open port 587 (SMTP)**
    - **Description:** Mail server detected.
    - **Vulnerability:** possible open relay configuration.
    - **Recommendation:** configure the mail server to prevent open relay.

Low-Risk Vulnerability

1. **Open port 993 (IMAPS)**
    - **Description:** IMAPS server detected.
    - **Vulnerability:** weak SS/TLS configuration.
    - **Recommendation:** use strong ciphers and protocols.
2. **Open port 995 (POP3s)**
    - **Description:** secure Mail server detected.
    - **Vulnerability:** possible outdated protocols.
    - **Recommendation:** disable week ciphers and outdated protocols.

CONCLUSION

The vulnerability assessment revealed several areas of concern that need to be addressed to improve the security posture ABC SecureBank. Implementing the recommended actions will help mitigate identified risks.