1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **newaccount-admin.bankfsb.com**. The analysis was initiated on **March 27th** at **14:45** and completed in **00h:09m:50s**. The assessment was identified with the tracking ID **196a9001cd1e** and employed a basic scanning methodology. The primary objective was to identify potential security vulnerabilities within the web application and infrastructure, focusing on High and Medium-risk issues.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High-risk, **2** Medium-risk, **3** Low-risk, and **13** informational. The most critical findings include the presence of potentially insecure HTTP ports (Medium-risk) and sensitive subdomain naming conventions that could expose administrative interfaces (Medium-risk). These vulnerabilities could lead to unauthorized access and data exposure if not addressed. Notably, **100%** of servers are located in the USA, with no High-risk geographic locations detected. Additionally, SSL/TLS protocols are mostly compliant, with TLS 1.2 being the minimum standard used. Immediate actions should focus on securing HTTP ports and reviewing subdomain configurations to mitigate potential threats.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low
SSL Certificate Expiration Analysis	Low
Login Form Detection Analysis	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The scan revealed that port **80/tcp** is open and associated with an HTTP service lacking encryption. This poses a risk if there is no redirection to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets:

- IP address: **66.22.30.39** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

- Ensure that HTTP traffic is redirected to HTTPS. - Implement HSTS to enforce secure connections. - Regularly review open ports and services for unnecessary exposure.

1.3.2 Subdomain Naming Security Assessment

Description:

A sensitive subdomain, **newaccount-admin.bankfsb.com**, was identified, indicating potential access to administrative interfaces and management panels. These are critical systems that could expose sensitive data if accessed by unauthorized users.

Affected Assets:

- Subdomain: **newaccount-admin.bankfsb.com**

Recommendations:
- Review and rename sensitive subdomains to non-descriptive names. - Implement access controls and monitoring for administrative interfaces. - Regularly audit subdomains for exposure risks.

1.4 General Recommendations

To enhance the security posture of the domain, it is recommended to conduct regular security assessments to identify new vulnerabilities. Implement a robust patch management process to address identified vulnerabilities promptly. Enhance monitoring and logging mechanisms to detect and respond to potential security incidents swiftly. Educate staff on security best practices to minimize human-related risks. By addressing these recommendations, the organization can significantly reduce its risk exposure and improve its overall security resilience.