1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **newaccounts.southstarbank.com**. The analysis was executed using a Basic scan type, initiated on **May 13th at 06:45** and completed in **00h:10m:48s**. The evaluation focused on identifying vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies. This document highlights the critical and medium-risk issues discovered during the assessment.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High, **2** Medium, **2** Low, and **14** informational. Key findings include medium-risk vulnerabilities such as an open HTTP port **80**, which lacks encryption and poses a risk of data interception unless redirected to HTTPS, and an SSL certificate nearing expiration in **71** days, requiring timely renewal to maintain secure communications.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assess...	Low
Login Form Detection Analysis	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The assessment revealed that port **80/tcp** is open and associated with the HTTP service, which does not provide encryption. This poses a significant risk of data interception if not properly redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets:

- **IP:** 66.22.30.162
- **Ports:** 80/tcp (http), 443/tcp (ssl/https)

Recommendations:

- Implement a redirection from HTTP to HTTPS to ensure encrypted communication. - Enable HSTS to enforce secure connections and prevent protocol downgrade attacks.

1.3.2 SSL Certificate Expiration Analysis

Description:

The SSL certificate for the domain **newaccounts.southstarbank.com** is set to expire in **71** days, placing it in the warning category. Timely renewal is essential to maintain secure communications and avoid service disruptions.

Affected Assets:

- **Domain:** newaccounts.southstarbank.com

Recommendations:

- Initiate the renewal process for the SSL certificate well before the expiration date to ensure continuous secure operations. - Consider implementing automated reminders or monitoring tools to track certificate expiration dates.

1.4 General Recommendations

To enhance the security posture of the domain, it is recommended to prioritize addressing medium-risk vulnerabilities. Implementing HTTPS redirection and renewing SSL certificates are critical steps in mitigating potential security breaches. Additionally, consider upgrading to TLS 1.3 for improved security and performance, and regularly review security configurations to align with best practices.