1 Executive Security Assessment Report

1.1 Assessment Overview

The security assessment was conducted on the domain **hastingsfcu-dn.financial-net.com**. The analysis commenced on **March 16th** at **16:00** and concluded in **00h:08m:15s**. The assessment type was categorized as "Basic". The evaluation focused on identifying High and Medium-risk security issues using OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, with **0** High-risk, **1** Medium-risk, **1** Low-risk, and **16** informational findings. The primary concern is the Medium-risk issue related to open port **80**, which lacks encryption and could expose sensitive data if not redirected to HTTPS. Additionally, the SSL/TLS assessment revealed that TLS **1.2** is in use, which is acceptable, but there is no support for the more secure TLS **1.3**.

1.3 Issue Table

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:

The assessment identified **2** open ports on the IP address **66.22.23.51**, specifically port **80/tcp** running HTTP without encryption and port **443/tcp** running SSL/HTTPS. The lack of encryption on port **80** poses a risk of data exposure unless it is redirected to HTTPS or protected by HTTP Strict Transport Security (HSTS).

Affected Assets:

- IP: **66.22.23.51**
- Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

It is recommended to implement a redirection from HTTP to HTTPS for all traffic on port **80**. Additionally, enabling HSTS can further enhance security by ensuring that browsers only connect to the server over HTTPS.

1.4.2 SSL/TLS Protocols Security Assessment

Description:

The SSL/TLS assessment revealed that the endpoint is using TLS **1.2**, which is currently an acceptable minimum standard. However, there is no support for TLS **1.3**, which offers improved security and performance.

Affected Assets:

- Endpoint using TLS **1.2**

Recommendations:

Consider upgrading to TLS **1.3** to align with current best practices for enhanced security and performance. This upgrade will provide better cryptographic strength and reduce the risk of protocol-based attacks.

1.5 General Recommendation

To maintain a robust security posture, it is crucial to address the Medium-risk issue promptly by enforcing HTTPS across all communications and considering the upgrade to TLS **1.3** for improved security standards. Regular security assessments should be conducted to ensure compliance with evolving security protocols and standards.