1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **m-ofcu-dn.financial-net.com**. The evaluation was performed using a Basic scan methodology, adhering to OWASP and OSCP standards. The analysis was initiated on **06-10** at **02:00** and completed in **00h:10m:38s**. The primary focus was to identify High and Medium-risk vulnerabilities that could potentially impact the security posture of the domain.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **1 Medium-risk**, **2 Low-risk**, and **15 informational**. The most significant finding is a Medium-risk issue related to open port **80**, which lacks encryption and could expose sensitive data if not redirected to HTTPS or secured with HSTS. This vulnerability could lead to data breaches, impacting business reputation and customer trust. Additionally, SSL/TLS analysis revealed that all endpoints support modern protocols, with **1 endpoint** using TLS 1.3, ensuring robust encryption. The SSL certificate for the domain is set to expire in **151 days**, requiring monitoring to prevent service disruptions. Overall, the assessment highlights the need for immediate action on the Medium-risk issue and ongoing monitoring of SSL certificates to maintain security posture.

1.3 Issues Table

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

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:

The assessment identified an open port **80** running HTTP without encryption on IP **107.162.254.116**. This lack of encryption poses a risk of data interception and unauthorized access, as HTTP traffic can be easily captured and analyzed by malicious actors.

Affected Assets:

- IP: **107.162.254.116** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

It is recommended to implement a redirection from HTTP to HTTPS to ensure all traffic is encrypted. Additionally, enabling HTTP Strict Transport Security (HSTS) will enforce secure connections and prevent protocol downgrade attacks.

1.4.2 SSL/TLS Protocols Security Assessment

Description:

The domain supports modern TLS protocols, with **1 endpoint** using TLS 1.3 and another using TLS 1.2. No deprecated or vulnerable protocols such as SSLv3, TLS 1.0, or TLS 1.1 were detected, indicating a strong encryption posture.

Affected Assets:

- **1 endpoint** with modern TLS 1.3 support - **1 endpoint** using TLS 1.2

Recommendations:
Continue to monitor and maintain the use of modern TLS protocols. Regularly update configurations to adhere to the latest security standards and best practices.

1.4.3 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain is set to expire in **151 days**, placing it in the "Monitor" category. While no immediate action is required, it is crucial to plan for renewal to avoid service disruptions.

Affected Assets:
- HTTPS-enabled subdomains

Recommendations:
Implement a certificate management process to ensure timely renewals. Consider automating certificate renewal processes to minimize the risk of expiration-related service outages.

1.5 General Recommendations

To enhance the overall security posture, it is advised to address the Medium-risk issue promptly by securing open ports and ensuring all communications are encrypted. Regular monitoring of SSL certificates and adherence to modern encryption standards will further safeguard against potential threats. Implementing a robust incident response plan will also prepare the organization for any unforeseen security events.