1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **showmecu-dn.financial-net.com**. The scan was initiated on **05-06** at **14:45** and completed in **00h:12m:02s**. The assessment type was classified as “Basic” with the tracking ID **0998b4aaa2a3**. The scope of the work included a comprehensive analysis of open ports and SSL/TLS protocols to identify potential vulnerabilities and assess the security posture of the infrastructure.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** High, **1** Medium, **1** Low, and **16** informational. The most significant finding is a Medium-risk issue related to an open HTTP port (**80**) that lacks encryption, posing potential security risks if not redirected to HTTPS. This vulnerability could expose sensitive data to interception, impacting data confidentiality. Additionally, the SSL/TLS assessment revealed that while TLS **1.2** is in use, there is no support for the more secure TLS **1.3**, suggesting an opportunity for protocol enhancement. The analysis also confirmed that all services are running on standard ports, and no shared hosting environments were detected, indicating a well-segmented infrastructure. It is recommended to address the HTTP port issue promptly and consider upgrading to TLS **1.3** to enhance security posture.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description:

The analysis identified an open HTTP port (**80**) on IP **107.162.237.204** that lacks encryption. This poses a Medium risk as it could allow attackers to intercept unencrypted traffic, potentially exposing sensitive information.

Affected Assets:

- IP: **107.162.237.204** - Ports: **80/tcp (http)**, **443/tcp (ssl/https)**

Recommendations:

It is recommended to ensure that HTTP traffic is redirected to HTTPS or that HTTP Strict Transport Security (HSTS) is enabled to mitigate risks associated with unencrypted data transmission.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The SSL/TLS assessment revealed that TLS **1.2** is currently in use, which is acceptable but does not include support for TLS **1.3**, the current best practice for enhanced security and performance.

Affected Assets:

- **1** endpoint using TLS **1.2**

Recommendations:

Consider upgrading to TLS **1.3** to improve security and performance, ensuring compliance with modern cryptographic standards.

1.4 General Recommendation

To enhance the overall security posture, it is crucial to address the Medium-risk issue by implementing HTTPS redirection or enabling HSTS on the affected HTTP port. Additionally, upgrading to TLS **1.3** should be prioritized to align with current best practices and improve both security and performance across all endpoints. Regular security assessments should be conducted to ensure ongoing protection against emerging threats and vulnerabilities.