1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **peoplesenergycu-dn.financial-net.com**. The analysis was performed using a Basic scan type, initiated on **March 27th at 05:45** and completed in **00h:09m:26s**. The evaluation focused on identifying High and Medium-risk security issues, utilizing methodologies aligned with OWASP and OSCP standards.

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 an open HTTP port 80, which lacks encryption and poses a potential security risk if not redirected to HTTPS. This could expose sensitive data to interception, impacting data confidentiality. Additionally, SSL/TLS analysis revealed that while TLS 1.2 is in use, there is no support for the more secure TLS 1.3, and SSL certificates are set to expire in **158 days**, requiring monitoring. The assessment found no evidence of shared hosting environments or brute-force vulnerable services, indicating a generally secure infrastructure. Immediate actions include addressing the HTTP port vulnerability and planning for SSL certificate renewal.

1.3 Issues Table

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

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:

The scan identified an open HTTP port (port 80) on IP address **66.22.21.108**. This port is running without encryption, which poses a security risk unless there is a redirection to HTTPS or HSTS is enabled. The lack of encryption on HTTP can lead to potential interception of sensitive data.

Affected Assets:

- IP Address: **66.22.21.108** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

Implement a redirection from HTTP to HTTPS to ensure all traffic is encrypted. Enable HTTP Strict Transport Security (HSTS) to enforce secure connections and prevent downgrade attacks.

1.4.2 SSL/TLS Protocols Security Assessment

Description:

The analysis revealed that TLS 1.2 is currently in use, which is acceptable as a minimum standard. However, there is no support for TLS 1.3, which offers improved security and performance. No deprecated or vulnerable protocols such as SSLv3, TLS 1.0, or TLS 1.1 were detected.

Affected Assets:

- **1** endpoint using TLS 1.2

Recommendations:
Upgrade to support TLS 1.3 to enhance security and performance. Regularly review protocol configurations to ensure compliance with current best practices.

1.4.3 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for the domain “peoplesenergycu-dn.financial-net.com” is set to expire in **158 days**, placing it in the “Monitor” category. This indicates that the certificate should be monitored for timely renewal to avoid service disruptions.

Affected Assets:
- Domain: peoplesenergycu-dn.financial-net.com

Recommendations:
Establish a monitoring process for SSL certificate expiration dates and plan for renewal at least **30** days before expiration to maintain uninterrupted secure communications.

1.5 General Recommendation

To enhance the overall security posture, it is recommended to address the Medium-risk issue by enforcing HTTPS across all services and upgrading to TLS 1.3 where possible. Additionally, implement a robust monitoring system for SSL certificate management to ensure timely renewals and avoid potential service disruptions. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.