1 Executive-Level Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **raisingcanesme.com**. The analysis commenced on **3rd October** at **22:45** and concluded in a duration of **00h:08m:49s**. The scope of work involved a basic security scan focusing on identifying High and Medium-risk vulnerabilities within the domain's infrastructure, employing methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Key Issues

The security assessment identified a total of **17 issues**, categorized as **1 High-risk**, **2 Medium-risk**, **1 Low-risk**, and **13 informational**. The most critical finding is the High-risk shared hosting environment, with **1 host** sharing infrastructure with over **1500 domains**, posing significant security risks due to potential cross-domain vulnerabilities. Medium-risk issues include an SSL certificate nearing expiration with only **37 days** remaining, and insecure HTTP port exposure, which could lead to data interception if not redirected to HTTPS.

1.3 Issue Table

Title	Risk
Shared Hosting Environment Analysis	High
SSL Certificate Expiration Analysis	Medium
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
No Resolvable Domains Found	Info

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description

A shared hosting environment was detected where the domain **raisingcanesme.com** shares infrastructure with over **1500 domains**. This configuration significantly increases the risk of cross-domain vulnerabilities, where a compromise in one domain could potentially affect all others sharing the same environment.

Affected Assets

- Hostname: raisingcanesme.com

Recommendations

To mitigate risks associated with shared hosting, it is recommended to migrate to a dedicated hosting environment or implement strict isolation measures between hosted domains. Regular security audits should be conducted to identify and address potential vulnerabilities arising from shared resources.

1.4.2 SSL Certificate Expiration Analysis

Description

The SSL/TLS certificate for **raisingcanesme.com** is set to expire in **37 days**, placing it in the "Warning" category. This poses a risk of service disruption and potential trust issues if not renewed promptly.

Affected Assets

- Domain: raisingcanesme.com

Recommendations

Immediate steps should be taken to renew the SSL certificate before expiration to maintain secure communications and avoid service interruptions. Implementing automated certificate renewal processes can prevent similar issues in the future.

1.4.3 Nmap Port Scan Results Analysis

Description

The domain has an open HTTP port (**80/tcp**) running Varnish, which lacks encryption, posing a risk of data interception. The presence of an HTTPS port (**443/tcp**) suggests potential for secure communication, but verification of HTTPS redirection or HSTS implementation is necessary.

Affected Assets

- IP: 151.101.65.124 - Ports: 80/tcp (http), 443/tcp (ssl/https)

Recommendations

Ensure all HTTP traffic is redirected to HTTPS and consider implementing HTTP Strict Transport Security (HSTS) to enforce secure connections. Regularly audit open ports and services for compliance with security best practices.

1.4.4 SSL/TLS Protocols Security Assessment

Description

All endpoints support modern TLS 1.2 and 1.3 standards, ensuring secure communications. No deprecated protocols like SSLv3, TLS 1.0, or TLS 1.1 were found, indicating a strong security posture regarding protocol support.

Affected Assets

- **4** endpoints support TLS 1.3 - **4** endpoints use TLS 1.2

Recommendations

Continue monitoring for any protocol updates and ensure all systems remain configured to use the latest cryptographic standards. Regular audits should be performed to maintain compliance with evolving security requirements.

1.4.5 No Resolvable Domains Found - Verify Domain Names

Description

The analysis could not resolve domain names, indicating a potential issue with domain name configuration or input errors during the setup of the assessment.

1.5 General Recommendations

It is crucial to address the High-risk shared hosting environment promptly by considering migration to dedicated hosting or enhancing isolation measures. Additionally, ensure timely renewal of SSL certificates and enforce HTTPS across all web services to uphold data security and integrity. Regular security assessments should be scheduled to continuously monitor and improve the security posture of the domain.