1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **api.chenosis.io**. The analysis was initiated on April 16th at 21:45 and concluded after a duration of **00h:09m:08s**. The assessment, identified by tracking ID **175b330fca32**, was performed using a Basic scan methodology. The focus was on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, employing OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19 issues**, categorized as **0 High-risk**, **4 Medium-risk**, **2 Low-risk**, and **13 informational**. The most critical findings include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, significantly increasing the risk of injection-based attacks. Additionally, unusual port assignments and potentially insecure open ports were detected, which could be exploited for unauthorized access. The analysis also highlighted a Medium-risk subdomain naming issue, indicating potential exposure of sensitive endpoints. While SSL/TLS protocols are generally secure, the lack of TLS 1.3 support suggests room for improvement. Immediate actions should focus on implementing WAF protection and reviewing port configurations to mitigate these vulnerabilities.

1.3 Key Security Issues

Title	Risk
Absence of WAF	Medium
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assess…	Low
API Surface Analysis	Low

1.4 Detailed Findings

1.4.1 Absence of WAF

Description

The absence of a Web Application Firewall (WAF) was identified on the analyzed host, resulting in a 100% vulnerability rate. This significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks, which could lead to unauthorized data access and potential system compromise.

Affected Assets:

- Host: **api.chenosis.io**

Recommendations:

Implement a robust Web Application Firewall to provide an additional layer of security against injection attacks and other web-based threats. Regularly update and configure the WAF to ensure optimal protection.

1.4.2 Unusual Port Assignments Detected

Description:

Unusual port assignments were detected on the host, indicating potential misconfigurations or

attempts to evade detection. Services running on non-standard ports may expose the system to unauthorized access or proxy services.

Affected Assets:

- Host: **api.chenosis.io (35.241.155.125)** - Port: **80**

Recommendations:

Review and standardize port configurations to align with expected service assignments. Conduct regular audits to detect and rectify any unauthorized or unexpected port usage.

1.4.3 Nmap Port Scan Results Analysis

Description:

The Nmap port scan revealed open ports, including port **80**, which is associated with HTTP service lacking encryption. This poses a risk as it may allow interception of unencrypted data.

Affected Assets:

- IP: **35.241.155.125** - Ports: **80/tcp (http?)**, **443/tcp (ssl/https)**

Recommendations:

Ensure that HTTP traffic is redirected to HTTPS and that HSTS is enabled to enforce secure connections. Regularly review open ports and close any that are unnecessary or insecure.

1.4.4 Subdomain Naming Security Assessment

Description:

A Medium-risk subdomain naming issue was identified, with the subdomain potentially exposing sensitive endpoints or internal systems.

Affected Assets:

- Subdomain: **api.chenosis.io**

Recommendations:

Conduct a thorough review of subdomain configurations to ensure they do not expose sensitive information or systems. Implement access controls and monitoring to detect unauthorized access attempts.

1.5 General Recommendations

To enhance the security posture of the domain **api.chenosis.io**, it is recommended to implement a comprehensive security strategy that includes deploying a Web Application Firewall, standardizing port configurations, enforcing HTTPS with HSTS, and securing subdomains against exposure of sensitive information. Regular security audits and updates should be conducted to maintain robust defenses against evolving threats.