1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **api.arkane.network** using a Basic scan type. The analysis commenced on **April 21st** at **04:45** and concluded in **00h:10m:15s**. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** High, **3** Medium, **3** Low, and **12** informational. Notably, medium-risk findings include the presence of potentially insecure open ports (HTTP on port **80** and **8080**) and sensitive subdomain endpoints, which could expose critical systems to unauthorized access. Additionally, an SSL certificate is nearing expiration in **77** days, requiring prompt renewal to maintain secure communications. The analysis revealed that all servers are located in the United States, with no high-risk geographic locations detected. While no high-density services or brute-force vulnerable services were found, the focus should be on addressing medium-risk vulnerabilities to enhance security posture.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
API Surface Analysis	Low
Login Form Detection Analysis	Low

1.4 Nmap Port Scan Results Analysis

Description:

The analysis revealed **4** open ports on the IP address **104.22.14.156**, with ports **80** and **8080** being potentially insecure due to lack of encryption and possible web service vulnerabilities. Port **80** is associated with HTTP services without encryption, necessitating verification for HTTPS redirection or HSTS implementation. Port **8080** is linked to web service vulnerabilities and proxy services.

Affected Assets:

- IP Address: **104.22.14.156** - Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**

Recommendations:

- Implement HTTPS with strong encryption protocols on all HTTP services. - Ensure HSTS is enabled to enforce secure connections. - Regularly update and patch web services to mitigate vulnerabilities.

1.5 Subdomain Naming Security Assessment

Description:

A sensitive subdomain, **api.arkane.network**, was identified, which could provide access to critical systems and sensitive data. This subdomain may expose development and staging environments with unpatched vulnerabilities or debug information.

Affected Assets:
- Subdomain: **api.arkane.network**

Recommendations:
- Conduct regular audits of subdomains to ensure they do not expose sensitive information. - Implement access controls and monitoring on sensitive subdomains. - Ensure development and staging environments are secured and isolated from production systems.

1.6 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for **api.arkane.network** is set to expire in **77** days, categorized under the “Warning” risk level. Timely renewal is essential to maintain secure communications.

Affected Assets:
- Domain: **api.arkane.network**

Recommendations:
- Plan for the renewal of the SSL certificate well before the expiration date. - Consider implementing automated alerts for certificate expiration. - Evaluate the use of certificate management tools to streamline renewals.

1.7 General Recommendation

To enhance the overall security posture, it is recommended that the organization prioritize addressing medium-risk vulnerabilities identified in this assessment. Implementing robust encryption practices, securing sensitive subdomains, and ensuring timely SSL certificate renewals are critical steps toward mitigating potential threats. Regular security assessments and adherence to best practices will further strengthen the organization’s defenses against evolving cyber threats.