1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **pop.hfl3.com**. The analysis commenced on **May 26th** at **18:00** and concluded in a duration of **00h:10m:34s**. The assessment was identified with the tracking ID **04f8928ba7eb** and was categorized as a **Basic** type scan. The evaluation focused on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19 issues**, categorized as **1 High-risk**, **3 Medium-risk**, **3 Low-risk**, and **12 informational**. The most critical finding is a Denial of Service (DoS) vulnerability with a **97.33% timeout rate** across HTTP and HTTPS services, posing a significant risk of service disruption. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, and insecure open ports (**110 and 143**) that could lead to unauthorized access. Additionally, sensitive subdomains were detected, increasing the risk of exposure to critical systems. Immediate actions include implementing DoS protection, enhancing WAF coverage, and securing vulnerable ports to mitigate potential threats.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS) Assessment	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
Shared Hosting Environment Analysis	Low
SSL/TLS Protocols Security Assessment	Low
Services Vulnerable to Brute Force Attacks	Low

1.3.1 Denial of Service (DoS) Assessment

Description:
A high severity DoS vulnerability was identified, characterized by a significant percentage of timeouts (**97.33%**) on HTTP and HTTPS services. This indicates a substantial risk of service disruption, potentially affecting business continuity and customer satisfaction.

Affected Assets:

- Hostname: **pop.hfl3.com** - Ports: **80 (HTTP)**, **443 (HTTPS)**

Recommendations:
Immediate implementation of DoS protection mechanisms is advised. This includes configuring rate limiting, deploying anti-DoS technologies, and optimizing server performance to handle high traffic loads effectively.

1.3.2 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was detected on the analyzed host, resulting in a high vulnerability rate (**100%**). This lack of protection increases the risk of successful cyberattacks, particularly those involving injection-based techniques.

Affected Assets:
- Hostname: **pop.hfl3.com**

Recommendations:
Deploy a robust WAF solution to protect against common web application attacks. Regularly update WAF rulesets to ensure comprehensive coverage against emerging threats.

1.3.3 Nmap Port Scan Results Analysis

Description:
Open ports **110 (POP3)** and **143 (IMAP)** were identified as potentially insecure due to clear text authentication, posing risks of email interception and unauthorized access.

Affected Assets:
- IP Address: **216.69.141.90** - Ports: **110/tcp**, **143/tcp**

Recommendations:
Secure these services by enforcing encrypted communication protocols such as SSL/TLS. Implement strong authentication mechanisms and regularly audit access logs for suspicious activity.

1.3.4 Subdomain Naming Security Assessment

Description:
A sensitive subdomain, **pop.hfl3.com**, was detected, which may provide access to critical systems and sensitive data. This increases the risk of exposure to unauthorized entities.

Affected Assets:
- Subdomain: **pop.hfl3.com**

Recommendations:
Review subdomain configurations for potential security weaknesses. Implement access controls and monitor for unauthorized access attempts.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, continuous monitoring, and incident response planning. Prioritize the deployment of security controls such as firewalls, intrusion detection systems, and encryption protocols to safeguard critical assets against evolving threats.