# 1 Executive Security Assessment Report

## 1.1 Introduction

The security assessment was conducted on the domain **imap.thewatergarden-la.com**. The analysis began on **April 8th** at **12:45** and concluded in a duration of **10 minutes and 11 seconds**. The assessment was categorized as a **Basic** type scan. The primary objective was to evaluate the security posture of the domain using OWASP and OSCP methodologies, focusing on identifying High and Medium-risk vulnerabilities.

## 1.2 Summary of Findings

The assessment identified a total of **19 issues**, with **0 High-risk**, **4 Medium-risk**, **2 Low-risk**, and **13 informational** findings. Key Medium-risk issues include the absence of a Web Application Firewall (WAF), a Denial of Service (DoS) vulnerability, insecure open ports, and exposure of a sensitive subdomain.

## 1.3 Issues Table

| Title | Risk |
|---|---|
| Absence of WAF | Medium |
| Nmap Port Scan Results Analysis | Medium |
| Subdomain Naming Security Assessment | Medium |
| Denial of Service (DoS) Vulnerability | Medium |
| SSL/TLS Protocols Security Assessment | Low |
| Services Vulnerable to Brute Force | Low |

### 1.3.1 Absence of WAF

**Description:**
The assessment revealed that the host lacks a Web Application Firewall (WAF), resulting in a **100% vulnerability rate**. This absence significantly increases the risk of injection attacks and unauthorized access, potentially leading to data breaches and system compromise.

**Affected Asset:**

- Host: **imap.thewatergarden-la.com**

**Recommendations:**
Implement a robust WAF solution to filter and monitor HTTP traffic between the web application and the Internet. This will help mitigate injection attacks and protect against unauthorized access attempts.

### 1.3.2 Nmap Port Scan Results Analysis

**Description:**
The Nmap scan identified port **110/tcp** open for the POP3 service, which is vulnerable to clear text authentication risks. This poses a threat of email interception and unauthorized access.

**Affected Asset:**

- IP: **216.69.141.90** - Port: **110/tcp** - Service: **pop3**

**Recommendations:**
Secure the POP3 service by implementing encrypted communication protocols such as TLS. Consider disabling unnecessary services or ports to reduce exposure.

### 1.3.3 Subdomain Naming Security Assessment

**Description:**
A sensitive subdomain, **imap.thewatergarden-la.com**, was identified, which could expose critical systems and sensitive data. This subdomain is categorized under "Sensitive Services" with a High risk level.

**Affected Asset:**

- Subdomain: **imap.thewatergarden-la.com**

**Recommendations:**

Review and secure sensitive subdomains by implementing strict access controls and monitoring for unauthorized access attempts. Ensure that development and staging environments are not exposed to the public.

### 1.3.4 Denial of Service (DoS) Vulnerability Assessment

**Description:**
The assessment detected indications of a Medium severity DoS vulnerability with a timeout rate of **0.31%** on the HTTP service. This could lead to potential service disruptions.

**Affected Asset:**

- Endpoint: **imap.thewatergarden-la.com:80**

**Recommendations:**

Enhance server resilience against DoS attacks by implementing request rate limiting and monitoring server performance during peak times. Optimize server configurations to handle high traffic loads efficiently.

## 1.4 General Recommendations

To improve the overall security posture, it is recommended to implement comprehensive security measures such as deploying a Web Application Firewall (WAF), securing open ports with encryption, monitoring sensitive subdomains, and enhancing DoS protection mechanisms. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.