1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **ftp.2000avenueofthestars.com**. The analysis commenced on **March 31st at 15:00** and concluded in **00h:09m:02s**. The assessment was identified with tracking ID **06037195a129** and employed a basic scan type. The evaluation focused on identifying High and Medium-risk vulnerabilities within the domain's infrastructure.

1.2 Summary of Key Issues

The security assessment identified a total of **18 issues**, categorized as **1 High-risk**, **2 Medium-risk**, **1 Low-risk**, and **14 informational**. The most critical finding is the High-risk shared hosting environment, with one host sharing its IP with over **500,000 domains**, posing significant security risks due to potential cross-domain vulnerabilities. Medium-risk issues include insecure open ports, such as HTTP on port **80**, which lacks encryption, and sensitive subdomain exposure, which could lead to unauthorized access. Notably, **100%** of servers are located in the USA, with no High-risk geographic locations detected. Immediate actions should focus on mitigating the High-risk shared hosting and securing open ports to prevent potential breaches.

1.3 Issues Table

Title	Risk
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low

1.4 Shared Hosting Environment Analysis

Description:

The analysis revealed that the host **ftp.2000avenueofthestars.com** is part of a High-risk shared hosting environment, sharing its IP address with over **500,000 domains**. This configuration significantly increases the risk of cross-domain vulnerabilities, where a security issue in one domain could potentially affect others sharing the same infrastructure.

Affected Assets:

- Hostname: **ftp.2000avenueofthestars.com**

Recommendations:

It is recommended to migrate critical services to a dedicated hosting environment to minimize the risk of cross-domain vulnerabilities. Additionally, continuous monitoring and regular security audits should be implemented to detect and mitigate any emerging threats promptly.

1.5 Nmap Port Scan Results Analysis

Description:

The port scan identified **2 open ports** on IP address **15.197.225.128**, including port **80** running HTTP without encryption. This lack of encryption poses a risk of data interception and unauthorized access.

Affected Assets:

- IP Address: **15.197.225.128**

Recommendations:

Immediate action should be taken to secure port **80** by implementing HTTPS with a valid SSL certificate. Ensure that HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections.

1.6 Subdomain Naming Security Assessment

Description:

The assessment detected a sensitive subdomain, **ftp.2000avenueofthestars.com**, which may expose critical systems or sensitive data. Such exposure can lead to unauthorized access if not properly secured.

Affected Assets:

- Subdomain: **ftp.2000avenueofthestars.com**

Recommendations:

Review and restrict access to sensitive subdomains, ensuring that they are protected by strong authentication mechanisms. Regularly audit subdomains for exposure of sensitive information and apply necessary security controls.

1.7 SSL/TLS Protocols Security Assessment

Description:

The analysis confirmed that all endpoints support TLS 1.3, which is currently the best practice for secure communications. No deprecated protocols such as SSLv3 or TLS 1.0 were detected.

Affected Assets:

- No vulnerable hosts detected

Recommendations:

Continue to maintain TLS 1.3 support across all systems and ensure that deprecated protocols remain disabled to protect against known vulnerabilities.

1.8 General Recommendations

To enhance overall security posture, it is crucial to prioritize the mitigation of High and Medium-risk issues identified in this assessment. Implementing dedicated hosting environments, securing open ports with encryption, and protecting sensitive subdomains are immediate actions that should be taken. Regular security audits and continuous monitoring will further safeguard against potential threats and ensure compliance with best practices.