1 Executive-Level Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain `ftp.100williamstreetny.com` using a Basic scan type. The analysis commenced on October 3rd at 17:00 and concluded in **00h:11m:33s**. The tracking ID for this assessment is **08fbe8d7f3f6**. The scope of work included identifying vulnerabilities within the web application and infrastructure, focusing on critical and medium-risk issues to enhance the security posture of the client's digital assets.

1.2 Summary of Key Findings

The security assessment identified **2** High-risk, **3** Medium-risk, and **13** informational issues. Critical findings include unusual port assignments and shared hosting environments, both categorized as High-risk. The unusual port assignments suggest potential evasion of security controls, while the shared hosting environment, with over **393** shared domains, increases the risk of cross-domain vulnerabilities. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, exposing them to injection attacks, and potentially sensitive subdomains that could be exploited. Immediate actions should focus on implementing WAF protection, securing port configurations, and evaluating shared hosting risks to mitigate potential data breaches and unauthorized access.

1.3 Issues Table

Title	Risk
Unusual Port Assignments Detected	High
Shared Hosting Environment Analysis	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium

1.4 Detailed Findings

1.4.1 Unusual Port Assignments Detected

Description:
Unusual port assignments have been detected on `ftp.100williamstreetny.com`, specifically on IP **208.68.246.151**. The service running on port **443** is flagged as High risk due to its non-standard assignment, which could indicate attempts to evade detection or misconfigured applications.

Affected Assets:
- Host: `ftp.100williamstreetny.com` with IP **208.68.246.151**

Recommendations:
- Review and standardize port configurations to ensure compliance with security policies. - Implement network monitoring tools to detect and alert on unusual port activity. - Conduct a thorough review of firewall rules to prevent unauthorized access through non-standard ports.

1.4.2 Shared Hosting Environment Analysis

Description:
The domain `ftp.100williamstreetny.com` is hosted in a shared environment with over **393**

domains sharing the same IP address, which poses a High risk for cross-domain vulnerabilities and potential data leaks.

Affected Assets:

- Hostname: `ftp.100williamstreetny.com`

Recommendations:

- Consider migrating to a dedicated hosting environment to isolate critical assets. - Regularly audit shared hosting configurations to identify and mitigate risks associated with co-hosted domains. - Implement strict access controls and monitoring for shared resources.

1.4.3 Absence of WAF

Description:

The absence of a Web Application Firewall (WAF) was noted across all analyzed hosts, resulting in a **100%** vulnerability rate. This significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks.

Affected Assets:

- Host: `ftp.100williamstreetny.com`

Recommendations:

- Deploy a Web Application Firewall to protect against common web threats such as SQL injection and cross-site scripting. - Regularly update WAF rulesets to address emerging threats. - Conduct periodic security assessments to ensure WAF effectiveness.

1.4.4 Nmap Port Scan Results Analysis

Description:

The Nmap port scan detected open ports **80/tcp** and **443/tcp** on IP **208.68.246.151**. Port **80**, running HTTP without encryption, poses a risk unless redirected to HTTPS or if HSTS is enabled.

Affected Assets:

- IP Address: **208.68.246.151** - Ports: **80/tcp** and **443/tcp**

Recommendations:

- Implement HTTPS with strong encryption for all web traffic. - Enable HSTS to enforce secure connections. - Regularly review and update SSL/TLS configurations.

1.4.5 Subdomain Naming Security Assessment

Description:

The subdomain `ftp.100williamstreetny.com` is categorized as High risk due to its potential access to sensitive services and data.

Affected Assets:

- Subdomain: `ftp.100williamstreetny.com`

Recommendations:

- Conduct regular audits of subdomains to identify and secure sensitive services. - Implement access controls and monitoring for critical subdomains. - Ensure development and staging environments are adequately secured.

1.5 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 adherence to best practices in cybersecurity hygiene. Prioritize addressing High and Medium-risk issues identified in this report to mitigate potential threats effectively.