1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **web-bff.smartfm.cbre.com**. The analysis commenced on **April 13th** at **05:00** and concluded in **18 minutes and 16 seconds**. The scope of the work involved a basic security scan focusing on identifying High and Medium-risk vulnerabilities within the infrastructure.

1.2 Summary of Key Issues

The security assessment identified **1** High-risk, **3** Medium-risk, **3** Low-risk, and **11** informational issues. The most critical finding is the High-risk shared hosting environment, with one host sharing its IP with over **100** domains, increasing the risk of cross-domain vulnerabilities. Medium-risk issues include unusual port assignments and high service density, with **100%** of hosts having more than four services, expanding the attack surface. Additionally, **4** services are vulnerable to brute force attacks due to lack of proper authentication controls. While SSL/TLS protocols are generally secure, with **5** endpoints supporting TLS 1.3, monitoring is advised for certificate expiration in **129** days. Immediate actions should focus on mitigating shared hosting risks and securing exposed services to prevent unauthorized access.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment Analysis	High
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Services Vulnerable to Brute Force Attacks	Low
SSL Certificate Expiration Analysis	Low

1.4 Shared Hosting Environment Analysis

1.4.1 Description

The analysis identified a High-risk shared hosting environment where the host **web-bff.smartfm.cbre.com** shares its IP address with over **100** domains. This configuration significantly increases the risk of cross-domain vulnerabilities, potentially allowing attackers to exploit weaknesses in one domain to affect others.

1.4.2 Affected Assets

- Hostname: **web-bff.smartfm.cbre.com**

1.4.3 Recommendations

It is recommended to evaluate the necessity of shared hosting for critical applications and consider migrating to a dedicated hosting environment. Implement strict access controls and continuous monitoring to detect and respond to potential threats promptly.

1.5 Unusual Port Assignments Detected

1.5.1 Description

The scan detected **5** unusual port assignments on the host **web-bff.smartfm.cbre.com (45.223.163.4)**. Services are running on non-standard ports or ports running unexpected services, which may indicate attempts to evade detection or misconfigured applications.

1.5.2 Affected Assets

- Host: **web-bff.smartfm.cbre.com (45.223.163.4)**

1.5.3 Recommendations

Review and standardize port configurations to align with best practices. Ensure that all services are correctly configured and unnecessary services are disabled to minimize exposure.

1.6 Nmap Port Scan Results Analysis

1.6.1 Description

The scan identified several ports with services that may pose security risks, such as clear text authentication and web service vulnerabilities. A total of **9** open ports were detected on the host **45.223.163.4**, indicating potential exposure to unauthorized access and data interception.

1.6.2 Affected Assets

- IP Address: **45.223.163.4**

1.6.3 Recommendations

Conduct a thorough review of all open ports and associated services. Implement encryption for data in transit and enforce strong authentication mechanisms to protect against unauthorized access.

1.7 Service Density Analysis

1.7.1 Description

The host **45.223.163.4** was found to have a high service density with **9** services, increasing the attack surface significantly. Ports marked with warnings (21, 25, 110, 8080) are potentially insecure and require additional security measures.

1.7.2 Affected Assets

- Host IP: **45.223.163.4**

1.7.3 Recommendations

Reduce the number of exposed services by disabling unnecessary ones and consolidating functions where possible. Regularly audit service configurations to ensure compliance with security policies.

1.8 General Recommendation

To enhance overall security posture, it is crucial to address High-risk vulnerabilities immediately while also implementing robust monitoring solutions for ongoing threat detection and response. Regular security audits and adherence to industry best practices will help maintain a secure environment and protect against evolving threats.