1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **visionhub.cbre.com**. The analysis began on **April 26th at 20:45** and concluded in a duration of **15 minutes and 24 seconds**. The assessment was identified with the tracking ID **091e8fd1748d** and was categorized as a **Basic** type analysis. The scope of the work included a comprehensive evaluation of the domain's infrastructure, focusing on identifying High and Medium-risk issues that could impact the security posture of the organization.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 risks**: **1 High-risk**, **3 Medium-risk**, **4 Low-risk**, and **10 informational issues**. The most critical finding is the High-risk shared hosting environment, with **visionhub.cbre.com** sharing its IP with over **100 domains**, increasing the potential for cross-domain vulnerabilities. Medium-risk issues include unusual port assignments and high service density, with **100%** of hosts having more than four services, which expands the attack surface. Additionally, **5 unusual port assignments** were detected, indicating possible evasion of security controls. While SSL/TLS protocols are generally secure, with **5 endpoints** supporting TLS 1.3, the presence of services vulnerable to brute force attacks on ports 21, 25, 110, and 3306 requires immediate attention to enhance authentication security.

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

1.4 Shared Hosting Environment Analysis

Description:

The domain **visionhub.cbre.com** is hosted in a shared environment with over **100 other domains**. This configuration poses a High risk due to the potential for cross-domain vulnerabilities and shared infrastructure weaknesses.

Affected Assets:

- Hostname: **visionhub.cbre.com**

Recommendations:

- Consider migrating to a dedicated hosting environment to minimize exposure to vulnerabilities associated with shared hosting. - Implement strict access controls and monitoring to detect any unauthorized access attempts.

1.5 Unusual Port Assignments Detected

Description:

A total of **5 unusual port assignments** were identified on the host **visionhub.cbre.com (45.223.56.188)**.

Services are running on non-standard ports or ports running unexpected services, which may indicate attempts to evade detection or misconfigured applications.

Affected Assets:

- Host: **visionhub.cbre.com (45.223.56.188)**

Recommendations:

- Review and reconfigure services to use standard ports where applicable. - Implement network segmentation and firewall rules to restrict access to non-standard ports. - Conduct regular audits to ensure compliance with security policies.

1.6 Nmap Port Scan Results Analysis

Description:

The scan revealed **9 open ports** on the host **45.223.56.188**, associated with potentially insecure services or protocols. These include ports that may allow clear text authentication or unauthorized access.

Affected Assets:

- IP Address: **45.223.56.188**

Recommendations:

- Disable unnecessary services and close unused ports. - Ensure all services are configured to use secure protocols and encryption. - Regularly update software to patch known vulnerabilities.

1.7 Service Density Analysis

Description:

The host **45.223.56.188** exhibits high service density with **9 services running**, increasing the attack surface and potential for exploitation.

Affected Assets:

- Host IP: **45.223.56.188**

Recommendations:

- Reduce the number of exposed services by consolidating functions where possible. - Implement robust monitoring and intrusion detection systems to detect anomalous activities. - Conduct regular vulnerability assessments to identify and mitigate risks associated with high service density.

1.8 General Recommendation

To enhance the overall security posture, it is recommended to implement a comprehensive security management program that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network activities. Additionally, adopting a defense-in-depth strategy will provide multiple layers of security controls to protect against potential threats effectively.