1 Executive Security Assessment Report

1.1 Introduction

This report details the findings from a comprehensive security assessment conducted on the domain **ecmdev.cbre.com**. The analysis was initiated on **July 7th at 18:45** and completed in **00h:30m:09s**. The assessment was performed using a Basic scan type, with the tracking ID **0ad15de5b8a1**. The evaluation focused on identifying High and Medium-risk issues within the infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Key Issues

The security assessment identified a total of **18 issues**, categorized as **1 High-risk**, **4 Medium-risk**, **2 Low-risk**, and **11 informational**. The most critical finding involves unusual port assignments, with services running on non-standard ports, including a High-risk assignment on port **3389**, which could indicate attempts to evade detection and poses a significant security threat. Medium-risk issues include vulnerabilities to brute force attacks on services like MSSQL and SMTP, and high service density on a single host, increasing the attack surface. Notably, **41 endpoints** support modern TLS 1.3, ensuring strong encryption. Immediate attention is required to address High-risk port configurations and enhance brute force protection mechanisms to mitigate potential unauthorized access.

1.3 Issues Table

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

1.4 Unusual Port Assignments Detected

Description

The assessment revealed that services are running on non-standard ports or unexpected services are running on standard ports. This configuration may indicate attempts to evade detection, proxy services, or misconfigured applications. A particularly critical finding is the High-risk assignment on port **3389**, which is typically used for Remote Desktop Protocol (RDP) and poses a significant security risk.

Affected Assets:

- Host: **ecmdev.cbre.com** (IP: **45.223.56.188**)

Recommendations:

- Reconfigure services to use standard ports where applicable. - Implement network segmentation to isolate critical services. - Regularly audit port configurations to ensure compliance with security policies. - Deploy intrusion detection systems to monitor for unusual traffic patterns.

1.5 Nmap Port Scan Results Analysis

Description:
The analysis identified several open ports associated with potentially insecure services or protocols, such as FTP, SMTP, HTTP, POP3, NetBIOS, IMAP, SQL Server, NFS, VNC, X11, and various web services. These ports are linked to risks like clear text authentication, anonymous access, email spoofing, relay attacks, and various vulnerabilities specific to the services running on those ports.

Affected Assets:
- IP: **45.223.56.188**

Recommendations:
- Disable unnecessary services and close unused ports. - Implement secure configurations for all active services. - Use encryption protocols for data transmission where possible. - Regularly update software to patch known vulnerabilities.

1.6 Service Density Analysis

Description:
A high service density was detected on the host, with **30 services** running concurrently. This increases the attack surface and the likelihood of vulnerabilities being exploited.

Affected Assets:
- Host IP: **45.223.56.188**

Recommendations:
- Review and reduce the number of active services per host. - Implement network segmentation to distribute services across multiple hosts. - Conduct regular audits to identify and decommission obsolete services.

1.7 Subdomain Naming Security Assessment

Description:
The subdomain **ecmdev.cbre.com** is associated with development/staging environments, which may contain unpatched vulnerabilities or debug information. These endpoints could provide access to critical systems and sensitive data.

Affected Assets:
- Subdomain: **ecmdev.cbre.com**

Recommendations:
- Restrict access to development/staging environments. - Regularly update and patch development environments. - Implement strict access controls and monitoring for sensitive subdomains.

1.8 Services Vulnerable to Brute Force Attacks

Description:
Several services were identified as vulnerable to brute force attacks due to the lack of account lockout mechanisms and weak password policies. Services affected include MSSQL, SMTP, IMAP, FTP, POP3, VNC, MySQL, and RDP.

Affected Assets:
- IP Address: **45.223.56.188**

Recommendations:
- Implement account lockout policies after a set number of failed login attempts. - Enforce strong password policies across all services. - Utilize multi-factor authentication where possible. - Monitor authentication logs for suspicious activity.

1.9 General Recommendations

To enhance overall security posture, it is recommended that the organization implements a comprehensive security strategy that includes regular vulnerability assessments, continuous monitoring of network traffic, and adherence to best practices for secure configurations. Additionally, employee training on cybersecurity awareness should be conducted to mitigate risks associated with human factors.