1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **gvpn.cbre.co.il**. The analysis commenced on **June 28th at 08:45** and concluded in **00h:14m:42s**. This evaluation was performed using a Basic scan type. The assessment focused on identifying vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** High, **2** Medium, **1** Low, and **15** informational. The most critical findings include Medium-risk vulnerabilities such as an open HTTP port **80**, which lacks encryption and may expose sensitive data, and a sensitive subdomain that could be an attack vector. These issues could lead to unauthorized access or data breaches if not addressed. The SSL/TLS protocols are secure, with support for TLS **1.3** and **1.2**, and no deprecated protocols detected. Additionally, no API endpoints or brute-force susceptible services were found, indicating a robust security posture in these areas. Immediate action is recommended to secure the HTTP port and review the sensitive subdomain for potential exposure.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description

The assessment revealed that port **80/tcp** is open on IP **84.95.94.229**, providing HTTP services without encryption. This lack of encryption poses a risk of exposing sensitive data to unauthorized parties. The presence of open ports **443/tcp** (SSL/HTTPS) and **2000/tcp** (potentially Cisco SCCP) was also noted.

Affected Assets

- IP: **84.95.94.229**
  - Open Ports: **80/tcp**, **443/tcp**, **2000/tcp**

Recommendations

It is recommended to enforce HTTPS by redirecting HTTP traffic to HTTPS and enabling HTTP Strict Transport Security (HSTS). Regularly monitor and review open ports to ensure they are necessary for business operations and secured appropriately.

1.3.2 Subdomain Naming Security Assessment

Description

The subdomain **gvpn.cbre.co.il** was identified as a sensitive service with a Medium risk level due to its potential to provide access to critical systems and sensitive data. Such subdomains can be attractive targets for attackers seeking entry points into internal networks.

Affected Assets

- Subdomain: `gvpn.cbre.co.il`

Recommendations

Conduct a thorough review of the subdomain's security posture, ensuring that it is adequately protected with strong authentication mechanisms and regular security audits. Consider restricting access to trusted IP addresses and implementing additional monitoring for suspicious activities.

1.3.3 SSL/TLS Protocols Security Assessment

Description

The analysis confirmed that the domain supports TLS **1.3** and TLS **1.2**, which are considered secure protocols. No deprecated protocols such as SSLv3, TLS **1.0**, or TLS **1.1** were detected, indicating a strong cryptographic configuration.

Affected Assets

- **1** endpoint with TLS **1.3** support
- **1** endpoint using TLS **1.2**

Recommendations

Maintain the current configuration by regularly updating cryptographic libraries and ensuring compliance with industry standards for secure communications.

1.4 General Recommendations

To enhance the security posture, it is crucial to address the identified Medium-risk vulnerabilities promptly. Implementing encryption on all communication channels, securing sensitive subdomains, and maintaining up-to-date cryptographic protocols will mitigate potential risks. Continuous monitoring and regular security assessments should be conducted to identify and remediate emerging threats effectively.