1 Executive Security Assessment Report for Capital-Center.com

1.1 Scan Details

- **Domain Analyzed:** capital-center.com
- **Tracking ID:** 096e9b67b919
- **Type of Analysis:** Basic
- **Initiation Date and Time:** December 3rd, 16:00
- **Duration: 10** minutes and **2** seconds

1.2 Short Summary of Main Issues

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 on capital-center.com could indicate attempts to evade detection, posing a significant threat to system integrity. The shared hosting environment, with over **393 domains** on a single IP, increases the risk of cross-domain vulnerabilities. Medium-risk issues such as the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts and insecure subdomain naming further elevate the risk of unauthorized access and data breaches. Immediate actions should focus on implementing a WAF, securing port configurations, and evaluating shared hosting risks to mitigate potential threats.

1.3 Key Security Issues

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

1.4 Unusual Port Assignments Detected

Description:

Unusual port assignments were detected on the host capital-center.com, particularly on port **443**. This port is typically used for HTTPS traffic but was found running unexpected services. Such configurations may indicate attempts to evade detection or misconfigurations that could be exploited by malicious actors.

Affected Assets:

- Host: **capital-center.com (208.68.246.151)**
- Port: **443**

Recommendations:

Conduct a thorough review of port configurations to ensure they align with expected service protocols. Implement strict access controls and monitoring to detect any unauthorized service changes or access attempts.

1.5 Shared Hosting Environment Analysis

Description:

The domain capital-center.com is hosted in a shared environment with over **393 domains** on the same IP address. This significantly increases the risk of cross-site vulnerabilities and potential exposure through neighboring domains.

Affected Assets:

- Hostname: **capital-center.com**

Recommendations:

Consider migrating to a dedicated hosting environment to minimize exposure risks. If shared hosting is necessary, ensure robust isolation measures are in place and regularly audit neighboring domains for security compliance.

1.6 Absence of WAF

Description:

The analysis revealed that all hosts analyzed lack Web Application Firewall (WAF) protection, resulting in a **100% vulnerability rate**. This absence elevates the risk of successful cyber-attacks, particularly those based on injection techniques.

Affected Assets:

- Host: **capital-center.com**

Recommendations:

Deploy a Web Application Firewall (WAF) to protect against common web-based attacks such as SQL injection and cross-site scripting (XSS). Regularly update and configure the WAF rules to adapt to evolving threats.

1.7 Nmap Port Scan Results Analysis

Description:

The scan identified open ports **80/tcp** and **443/tcp**, with port **80** running HTTP service on Microsoft IIS httpd **8.5** without encryption, suggesting a need for HTTPS redirection or HSTS implementation.

Affected Assets:

- IP: **208.68.246.151**
- Ports: **80/tcp** (http), **443/tcp** (https?)

Recommendations:

Ensure that HTTP traffic is redirected to HTTPS and implement HSTS to enforce secure connections. Regularly update server software to mitigate vulnerabilities associated with outdated versions.

1.8 Subdomain Naming Security Assessment

Description:

Sensitive subdomains have been identified under capital-center.com, which may provide unauthorized access to critical systems and sensitive data.

Affected Assets:

- Subdomain: **capital-center.com**

Recommendations:

Conduct a comprehensive review of subdomain configurations and access controls. Ensure sensitive subdomains are secured with appropriate authentication and encryption measures.

1.9 General Recommendations

To enhance the security posture of capital-center.com, it is recommended to implement a multi-layered defense strategy that includes deploying a Web Application Firewall (WAF), securing port configurations, migrating to dedicated hosting where feasible, and continuously monitoring for vulnerabilities across all assets. Regular security audits and updates should be conducted to address emerging threats promptly.