1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings of a security assessment conducted on the domain **mtnmo-moagent.mtn.co.za**. The analysis was initiated on **August 7th** at **03:00** and completed in **26 minutes and 1 second**. The assessment, performed using a Basic scan type, focused on identifying High and Medium-risk vulnerabilities within the target infrastructure. The methodology employed aligns with OWASP and OSCP standards, ensuring a comprehensive evaluation of the domain's security posture.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **1 High-risk**, **2 Medium-risk**, **2 Low-risk**, and **13 informational**. The most critical finding is the use of deprecated and vulnerable SSL/TLS protocols, including TLS 1.0 and TLS 1.1, on three endpoints, posing significant risks of exploitation. Additionally, unusual port assignments and potentially insecure open ports were detected, which may indicate misconfigurations or attempts to bypass security controls. The SSL certificate for one domain is set to expire in **98 days**, requiring monitoring. While no immediate High-risk threats were found in shared hosting or geographic distribution, the presence of multiple services on a single host increases the attack surface. Immediate remediation of SSL/TLS vulnerabilities and regular monitoring of service configurations are recommended to enhance security posture.

1.3 Key Security Issues

Title	Risk
SSL/TLS Protocols Security Assessment	High
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Low
SSL Certificate Expiration Analysis	Low

1.4 SSL/TLS Protocols Security Assessment

Description:

The assessment revealed that deprecated and vulnerable SSL/TLS protocols, specifically TLS 1.0 and TLS 1.1, are in use across three endpoints. These protocols are susceptible to known attacks such as BEAST and lack modern cryptographic algorithms, posing significant security risks.

Affected Assets:

- **3 endpoints** using TLS 1.0
- **3 endpoints** using TLS 1.1
- **3 endpoints** using TLS 1.2

Recommendations:

Immediate upgrade to TLS 1.2 or higher is recommended to mitigate vulnerabilities associated with deprecated protocols. Implementing TLS 1.3 is advised for enhanced security and performance.

1.5 Unusual Port Assignments Detected

Description:

An analysis of port assignments revealed non-standard ports or unexpected services running on standard ports, which may indicate misconfigurations or attempts to evade detection.

Affected Assets:

- Host: **mtnmomoagent.mtn.co.za (196.11.240.215)**
- Port: **80**

Recommendations:

Review and reconfigure port assignments to ensure they align with expected services. Conduct regular audits to detect and rectify any unauthorized changes.

1.6 Nmap Port Scan Results Analysis

Description:

The scan identified several open ports, with ports **80** and **8080** highlighted as potentially insecure due to lack of encryption and possible web service vulnerabilities.

Affected Assets:

- IP Address: **196.11.240.215** with multiple open ports.

Recommendations:

Ensure that HTTP traffic is redirected to HTTPS and consider implementing HSTS. Regularly update web services to mitigate known vulnerabilities.

1.7 Service Density Analysis

Description:

The analysis indicated a high service density on a single host, increasing the attack surface and potential for exploitation.

Affected Assets:

- Host: **196.11.240.215**

Recommendations:

Consider distributing services across multiple hosts to reduce risk exposure. Implement network segmentation to limit potential attack vectors.

1.8 SSL Certificate Expiration Analysis

Description:

The SSL certificate for the domain is set to expire in **98 days**, which requires monitoring to ensure timely renewal.

Affected Assets:

- Domain: **mtnmomoagent.mtn.co.za**

Recommendations:

Establish a monitoring system for certificate expiration dates to ensure timely renewals and avoid service disruptions.

1.9 General Recommendation

To enhance the overall security posture, it is recommended to prioritize the remediation of High-risk vulnerabilities, particularly those related to SSL/TLS protocols. Regular audits of port configurations and service distributions should be conducted to identify and rectify potential misconfigurations promptly. Additionally, implementing a robust monitoring system for SSL certificates will help maintain secure communications and prevent service interruptions due to expired certificates.