1 Executive Security Assessment Report

1.1 Overview

The security assessment was conducted on the domain **autoconfig.kingagro.com.ar**. The analysis commenced on **July 17th** at **10:45 AM** and concluded in **00h:21m:32s**. The assessment employed a Basic scan type. The evaluation focused on identifying high and medium-risk issues, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **1 high-risk**, **1 medium-risk**, and **16 informational**. The most critical finding is the use of deprecated and vulnerable SSL/TLS protocols, specifically TLS 1.0 and TLS 1.1, on two endpoints, posing significant security risks such as susceptibility to BEAST attacks. Immediate remediation is advised to upgrade to TLS 1.2 or higher to mitigate potential exploitation. Additionally, a medium-risk issue was detected with open HTTP port **80**, which lacks encryption, necessitating verification of HTTPS redirection or HSTS implementation. While no high-density services or brute-force vulnerabilities were found, continuous monitoring and security hardening are recommended to maintain robust defenses.

1.3 Key Security Issues

Title	Risk
SSL/TLS Protocols Security Assessment	High
Nmap Port Scan Results Analysis	Medium

1.3.1 SSL/TLS Protocols Security Assessment

Description:
The assessment revealed the presence of deprecated and vulnerable SSL/TLS protocols on the analyzed endpoints. Specifically, **TLS 1.0** and **TLS 1.1** were detected on **2 endpoints** each. These protocols are susceptible to known attacks such as BEAST and lack modern cryptographic algorithms, respectively. The absence of TLS 1.3, which offers enhanced security and performance, further exacerbates the risk.

Affected Assets:
- **2 endpoints** using TLS 1.0 - **2 endpoints** using TLS 1.1 - **2 endpoints** using TLS 1.2 - No endpoints with TLS 1.3 support

Recommendations:
Immediate action is required to disable TLS 1.0 and TLS 1.1 across all endpoints. It is recommended to upgrade to TLS 1.2 as a minimum standard and implement TLS 1.3 where possible to ensure optimal security and performance.

1.3.2 Nmap Port Scan Results Analysis

Description:
The scan identified an open HTTP port (**80/tcp**) on the IP address **107.21.123.251**, which is operating without encryption. This configuration exposes data to potential interception and manipulation unless proper redirection to HTTPS or HSTS is enforced.

Affected Assets:
- IP: **107.21.123.251** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:
Verify that HTTP traffic is redirected to HTTPS and consider implementing HTTP Strict Transport Security (HSTS) to enforce secure connections automatically. This will help protect data integrity and confidentiality during transmission.

1.4 General Recommendations

To enhance the overall security posture, it is advised to conduct regular security assessments and ensure that all systems are updated with the latest security patches. Implementing a robust monitoring system will aid in the early detection of potential threats, allowing for timely mitigation actions. Additionally, adopting a comprehensive security policy that includes encryption standards, access controls, and incident response plans will further strengthen defenses against emerging threats.