1 Executive Security Assessment Report

1.1 Overview

This report presents the findings from a comprehensive security assessment conducted on the domain **gilenyago.ca**. The evaluation was carried out using OWASP and OSCP methodologies, leveraging advanced tools for web application and infrastructure penetration testing. The scan was initiated on **March 5th** at **20:00** and concluded in **00h:05m:29s**. The assessment was classified as a "Basic" type. The primary objective was to identify High and Medium-risk vulnerabilities that could potentially impact the security posture of the client's digital assets.

1.2 Short Summary of Main Issues

The recent security assessment revealed no High, Medium, or Low-risk issues, with three informational findings. A key highlight is the robust perimeter security, evidenced by **100%** of scanned ports being filtered, suggesting effective firewall and intrusion prevention systems. Additionally, the analysis confirmed that the infrastructure is dedicated, with no shared hosting risks detected. Geographic distribution analysis showed all servers are located in Canada, with no presence in high-risk areas, indicating a stable and secure server environment. These findings underscore a strong security posture, though continued vigilance and manual verification are recommended to ensure ongoing protection against potential threats.

1.3 Key Security Issues

Title	Risk
No High or Medium Risk Issues Found	N/A

1.4 Detailed Findings

1.4.1 Description

The security assessment did not identify any High or Medium-risk vulnerabilities. The infrastructure demonstrated a strong security posture with all scanned ports being filtered, indicating effective use of firewalls and intrusion prevention systems. The absence of shared hosting risks further strengthens the security framework.

1.4.2 Affected Assets

- Domain: **gilenyago.ca**

1.4.3 Recommendations

1. **Continuous Monitoring**: Implement continuous monitoring solutions to detect any anomalies or potential threats in real-time.
2. **Regular Security Audits**: Schedule regular security audits to ensure that the current security measures remain effective against evolving threats.
3. **Security Awareness Training**: Conduct periodic training sessions for staff to enhance awareness about cybersecurity best practices and emerging threats.
4. **Incident Response Plan**: Develop and maintain a robust incident response plan to quickly address any potential security incidents.

1.5 General Recommendation

Despite the absence of High or Medium-risk vulnerabilities, it is crucial to maintain a proactive approach to cybersecurity. Regular updates to security protocols, continuous monitoring, and employee training are essential to safeguard against future threats. Additionally, consider engaging in periodic third-party security assessments to validate the effectiveness of existing security measures and adapt to new challenges in the cybersecurity landscape.