1 Executive Security Assessment Report

1.1 Overview

This security assessment was conducted on the domain **evidence.co.uk**. The analysis commenced on **April 21st** at **07:45** and concluded in a duration of **00h:05m:10s**. The assessment was performed using a Basic scan type. The primary objective was to identify and evaluate potential security vulnerabilities within the specified domain, focusing on High and Medium-risk issues.

1.2 Summary of Findings

The security assessment identified a total of **4** issues, with the most critical being the exposure of email addresses and passwords on the deep web. This High-risk issue poses significant threats such as phishing attacks and unauthorized access to internal systems, which could severely impact business operations and damage the organization's reputation. Additionally, all scanned ports were filtered, indicating robust perimeter security controls, with **100%** of **11** ports filtered. A Low-risk finding noted a shared hosting environment with one host sharing an IP with **6** domains. Lastly, server geographic distribution was normal, with all servers located in Ireland. Immediate actions should focus on mitigating the High-risk credential exposure and verifying the effectiveness of perimeter defenses.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked	High
Shared Hosting Environment Analysis	Low

1.3.1 Email Addresses and/or Passwords Leaked on the Deep Web

Description The assessment revealed that email addresses and passwords associated with the domain **evidence.co.uk** have been leaked on the deep web. A total of **4** credentials were identified across multiple databases, including Adobe and R2Games.com. This exposure poses critical security risks, including unauthorized access, phishing, social engineering, and further data breaches.

Affected Assets

- **Email Addresses:** isabella.peter-liburd@evidence.co.uk, something.som@evidence.co.uk, tom.letcher@evid
- **Total Leaked Credentials: 4**

Recommendations Immediate steps should be taken to mitigate this risk by:

- Promptly notifying affected users to change their passwords.
- Implementing multi-factor authentication (MFA) across all user accounts.
- Conducting regular security awareness training to educate employees about phishing and social engineering threats.
- Monitoring for any suspicious activity related to these credentials.

1.3.2 Shared Hosting Environment Analysis

Description The analysis identified a shared hosting environment where the domain **evidence.co.uk** shares an IP address with **6** other domains. This configuration is considered Low risk but can potentially expose the domain to vulnerabilities affecting other hosted sites.

Affected Assets

- **Hostname:** evidence.co.uk
- **Shared Domains Count: 6**

Recommendations To minimize potential risks associated with shared hosting environments:

- Consider migrating to a dedicated hosting solution to isolate resources.
- Regularly monitor for vulnerabilities that could affect shared environments.
- Ensure that all hosted applications are kept up-to-date with security patches.

1.4 General Recommendations

To enhance overall security posture, it is recommended to:

- Conduct regular security assessments to identify and address emerging threats.
- Implement comprehensive logging and monitoring solutions to detect anomalies in real-time.
- Establish a robust incident response plan to quickly address any security incidents.
- Continuously update security policies and procedures in line with industry best practices.

By addressing these recommendations, the organization can significantly reduce its risk exposure and strengthen its cybersecurity defenses.