Cybersecurity Audit Report

Initial Level

Client: [Company Name]

Date: [Report Date]

Audit Type: External Security Assessment – Initial Level

1. Executive Summary

This Initial Level Cybersecurity Audit provides a high-level overview of your company's external security posture. Its primary goal is to pinpoint key internet-facing exposures and offer clear, actionable recommendations to mitigate risks. This assessment is the foundational step in establishing a robust security program, confirming effective practices and highlighting areas requiring enhancement.

2. Key Findings

Penetration Test Report: Key Findings

High Severity

- ❖ **Administration Port Accessible from the Internet:** This port is vulnerable to attacks and could be exploited by malicious actors to gain unauthorized access.
    - ➢ **Recommendation:** Restrict access using a VPN or IP whitelisting.

Medium Severity

- ❖ **Expired Security Certificate:** An expired SSL certificate can cause browser warnings for visitors and compromise encryption reliability.
    - ➢ **Recommendation:** Renew the SSL certificate immediately.
- ❖ **Outdated Software Components:** Known vulnerabilities in outdated software components could be exploited.
    - ➢ **Recommendation:** Update all applications and supporting components.

3. Strengths

- No weak passwords identified during testing.
- Good response times for main public-facing services.
- No signs of obvious data leaks detected.

4. Priority Recommendations

- Restrict access to administrative interfaces.
- Apply pending updates to all systems and applications.
- Improve SSL/TLS encryption configuration.
- Schedule periodic security reviews to maintain strong defenses.

5. Conclusion

This initial assessment highlights critical areas for immediate security improvement, which will significantly reduce your exposure to cyber threats. Addressing these high-priority findings will strengthen your security posture. For a more comprehensive understanding of your internal and application-level security, we recommend considering an Intermediate or Advanced Audit.

6. Next Steps

- Intermediate/Advanced Security Audit – includes internal network and application testing.
- Cybersecurity Awareness Training – equip employees to identify and avoid common threats.
- Continuous Threat Monitoring – proactively detect and respond to emerging risks.

Technical Annex (Confidential – For Internal IT Use Only)

A. External Service Overview

IP Address	Hostname	Service/Port	Status	Notes
203.0.113.25	admin.example.com	TCP/8443 (Admin Interface)	Open	Accessible from public internet – high risk.
203.0.113.27	www.example.com	TCP/443 (HTTPS)	Open	SSL certificate expired 45 days ago.
203.0.113.28	api.example.com	TCP/80 (HTTP)	Open	Redirects to HTTPS; outdated web framework detected.

B. SSL/TLS Assessment

Domain	Protocols Supported	Issues Identified
www.example.com	TLS 1.0, TLS 1.2	TLS 1.0 still enabled (deprecated).
api.example.com	TLS 1.2	No certificate chain issues.

C. Detected Software Versions

Service	Version Detected	Risk
Web Framework	v2.4.7	Known vulnerabilities in public databases.
CMS Plugin	v1.3	Security patches missing.
Server OS	Outdated minor version	Requires vendor updates.

D. Evidence Snapshots

- Screenshot of browser security warning due to expired SSL certificate.
- Terminal capture showing open administrative port accessible from external networks.
- HTTP headers showing outdated software components.

E. Next Steps – Technical Annex

- Patch or decommission the administration interface accessible from the internet.
- Renew the SSL certificate for www.example.com and disable deprecated protocols (TLS 1.0).
- Apply updates to the web framework, CMS plugin, and server OS.
- Perform a follow-up scan to verify successful remediation of identified issues.
- Consider implementing a bi-annual vulnerability scan schedule for continuous monitoring.