Ethical Hacking Technical Report

Client: Kiel Corporation

Date: May 11, 2024

Prepared by: Colarina, Peter Kenjie and Samillano, Niel Marc

Executive Summary: This report presents the results of an ethical hacking assessment conducted for Kiel Corporation to identify vulnerabilities in their network infrastructure, applications, and systems. Critical issues were discovered, requiring immediate attention. This report provides detailed descriptions of these findings and actionable recommendations for remediation.

Vulnerability Summary:

1. Network Infrastructure:

Critical: Remote Code Execution vulnerability (CVE-XXXX-XXXX) in the Apache Struts framework (version X.X.X) on Server-A, allowing arbitrary code execution.

High: Misconfigured firewall rules on Server-B permitting unrestricted external IP access to critical services like SSH and RDP.

2. Web Applications:

Critical: SQL Injection vulnerability in the login form of App-X, exposing sensitive database information.

High: Cross-Site Scripting (XSS) vulnerability in App-Y, enabling malicious script execution in user browsers.

3. Operating Systems:

Critical: Outdated and unpatched Windows Server 2008 R2 on Server-C, vulnerable to known exploits.

High: Weak password policies on domain user accounts, making them susceptible to brute-force attacks.

4. Wireless Networks:

Critical: Weak WEP encryption used in wireless networks, allowing data interception and decryption.

5. Social Engineering:

High: Successful phishing attacks resulting in employees disclosing credentials and sensitive information.

Recommendations:

1. Network Infrastructure:

- Immediately patch Apache Struts to the latest version on Server-A.
- Review and restrict firewall rules on Server-B based on the principle of least privilege.

2. Web Applications:

- Conduct a thorough code review and implement input validation in App-X to prevent SQL Injection and XSS attacks.
- Implement security headers like Content Security Policy in App-Y to mitigate XSS vulnerabilities.

3. Operating Systems:

- Develop a patch management process for regular OS updates on Server-C.
- Enforce strong password policies and consider multi-factor authentication for domain user accounts.

4. Wireless Networks:

- Upgrade wireless encryption to WPA2/WPA3 for secure wireless communications.

5. Social Engineering:

- Conduct periodic security awareness training sessions to educate employees on identifying and reporting phishing emails.

Conclusion: Addressing these vulnerabilities and implementing the recommended remediation measures will significantly enhance Kiel Corporation's security posture, reducing the risk of cyber threats and data breaches.

Signature:

Colarina, Peter Kenjie
Ethical Hacker

Samillano, Niel Marc
Ethical Hacker