**Ethical Hacking – Finals**

**Client:** Tech-Scan Corporation

**Date:** May 6, 2024

**Prepared by:** Kristian Bas and Jonalyn Alvaro

**Executive Summary:** This report details the technical findings of an ethical hacking assessment conducted for Tech-Scan Corporation. The assessment aimed to uncover vulnerabilities in the organization's network infrastructure, applications, and systems. Through various testing methodologies, including penetration testing and vulnerability scanning, critical and high-risk issues were identified. This report presents a comprehensive overview of these findings, along with actionable recommendations for mitigation.

**Vulnerability Summary:**

1. **Network Infrastructure:**

* Critical: Remote Command Execution vulnerability (CVE-2024-1234) in Cisco IOS (version 15.1) on core router, allowing unauthorized remote access.
* High: SNMP community strings set to default 'public' on network devices, exposing them to unauthorized queries and potential exploits.

1. **Web Applications:**

* Critical: Unvalidated Redirects and Forwards in Tech-Scan Web Portal, enabling attackers to redirect users to malicious sites.
* High: Missing security headers (e.g., X-Content-Type-Options) in web applications, leaving them vulnerable to content sniffing attacks.

1. **Database Security:**

* Critical: Weak database credentials stored in configuration files of Tech-Scan's main database server.
* High: Lack of SQL injection protection in SQL queries, making the database susceptible to injection attacks.

1. **Operating Systems:**

* Critical: End-of-life Windows 7 systems deployed in critical departments, exposing them to unpatched vulnerabilities.
* High: Insufficient logging and monitoring on Linux servers, hindering the detection of unauthorized access attempts.

1. **Wireless Networks:**

* Critical: Use of outdated WEP encryption on guest Wi-Fi network, susceptible to interception and decryption.
* High: Open authentication on internal Wi-Fi network, allowing unauthorized devices to connect.

1. **Physical Security:**

* Critical: Unsecured server room access with default lock codes, exposing critical infrastructure to physical breaches.
* High: Lack of CCTV coverage in sensitive areas within the corporate premises.

1. **Email Security:**

* Critical: Absence of SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) records in DNS settings, increasing susceptibility to email spoofing and phishing attacks.
* High: Lack of email filtering and content inspection, allowing malicious attachments and URLs to bypass security measures.

1. **Application Patching:**

* Critical: Use of outdated and unpatched third-party applications on employee workstations, exposing systems to known vulnerabilities.
* High: Inadequate application whitelisting policies, enabling unauthorized or potentially malicious applications to execute.

1. **System Hardening:**

* Critical: Default configurations and unnecessary services enabled on critical servers, increasing the attack surface and potential for exploitation.
* High: Lack of regular vulnerability scanning and configuration audits on servers and endpoints, leading to undetected security weaknesses.

1. **User Access Controls:**

* Critical: Use of shared or generic user accounts with high privileges across systems, complicating accountability and increasing the risk of unauthorized access.
* High: Insufficient user access reviews and inactive account management, allowing former employees' accounts to remain active and potentially exploited.

**Recommendations:**

1. **Network Infrastructure:**

* Immediately apply patches for Cisco IOS to address the Remote Command Execution vulnerability.
* Change SNMP community strings to strong, unique values and limit access to authorized IP addresses.

1. **Web Applications:**

* Implement input validation and output encoding to prevent Unvalidated Redirects and Forwards.
* Configure web servers to include necessary security headers (e.g., X-Frame-Options, Content-Security-Policy).

1. **Database Security:**

* Rotate database credentials regularly and store them securely using encrypted methods.
* Conduct code reviews to sanitize input and use parameterized queries to prevent SQL injection.

1. **Operating Systems:**

* Upgrade Windows 7 systems to supported versions or implement compensating controls.
* Enable comprehensive logging and implement intrusion detection systems on Linux servers.

1. **Wireless Networks:**

* Upgrade guest Wi-Fi encryption to WPA2 or WPA3 to enhance confidentiality.
* Implement WPA2-Enterprise with 802.1X authentication on internal Wi-Fi networks.

1. **Physical Security:**

* Change default lock codes and restrict access to server rooms based on role-based access controls.
* Install CCTV cameras in critical areas and ensure proper monitoring and recording.

1. **Email Security:**

* Implement SPF and DKIM records in DNS to authenticate outgoing emails and mitigate email spoofing.
* Deploy an email filtering solution to scan inbound and outbound emails for malicious content and URLs.

1. **Application Patching:**

* Establish a regular patch management process to ensure all third-party applications are up to date.
* Enforce application whitelisting policies to allow only authorized applications to run on employee workstations.

1. **System Hardening:**

* Conduct system hardening by disabling unnecessary services, applying least privilege principles, and implementing secure configurations based on industry standards.
* Implement routine vulnerability scanning and configuration audits to identify and remediate security gaps on servers and endpoints.

1. **User Access Controls:**

* Enforce strict policies against shared or generic user accounts, promoting individual accountability through unique user credentials and role-based access controls.
* Implement regular user access reviews and automate account management processes to promptly deactivate or archive inactive accounts.

**Conclusion:** The findings of this ethical hacking assessment underscore critical vulnerabilities and security weaknesses within Tech-Scan Corporation's infrastructure. By implementing the recommended remediation measures, Tech-Scan Corporation can strengthen its security posture and reduce the risk of cyber threats and unauthorized access.



**Signature:** Kristian Bas and Jonalyn Alvaro

