5-1 Project One: Security Assessment Recommendations

Joshua Merren

Southern New Hampshire University

CYB-400-13637-M01 Security Assessment & Auditing

Professor Jillian Seabrook

29 November 2024

One of the most critical categories identified in the scan was Scheduled Maintenance, which includes vulnerabilities that need immediate attention to protect the organization's systems. For example, the Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) could allow an attacker to perform a man-in-the-middle attack or gain unauthorized access to sensitive data if left unpatched (BetaFred, 2023). Applying the MS10-012 update addresses these vulnerabilities and reduces the risk of exploitation. Disabling SMBv1, which is outdated and vulnerable, also significantly lowers the attack surface. For instance, in the WannaCry ransomware attack in 2017, attackers exploited SMBv1 vulnerabilities to spread the malware rapidly across networks (BetaFred, 2023). Enabling SMB signing adds an extra layer of security by verifying the authenticity of data transmitted between systems. Similarly, addressing vulnerabilities through the MS17-010 update is crucial, as it resolves multiple critical issues in the SMB protocol that attackers can exploit to execute malicious code remotely. These measures protect the organization from known threats and ensure systems are more resilient against potential zero-day vulnerabilities targeting SMB services.

In the Policy Updates category, vulnerabilities require procedural changes to address risks effectively. For example, the SMB brute-force login vulnerability can be addressed by replacing default credentials, such as "admin:guest," with strong passwords (Postal, 2024). A real-world example of this attack occurred when attackers used default credentials to gain access to corporate systems, leading to data theft and disruption. Implementing account lockout policies ensures that repeated login attempts from an attacker result in account suspension, reducing the risk of brute-force attacks. Another example involves the ASP.NET Information Disclosure vulnerability, where attackers could exploit detailed error messages to learn about the system's configuration (BetaFred, 2023). Applying the MS11-100 update prevents such exploits by limiting the information revealed in error responses. Additionally, updating weak SSL/TLS certificates using more robust algorithms like SHA-256 protects against man-in-the-middle attacks. For instance, websites with outdated SHA-1 certificates have been targeted, allowing attackers to intercept sensitive data during transmission (*Weak Signature Algorithms - Security on the Web | MDN*, 2023). These policy changes improve security, help organizations comply with modern standards, and prevent data breaches.

The first vulnerability in the Other Security Issues category is related to DCE/RPC and MSRPC services enumeration vulnerabilities, which expose services to potential attackers. An attacker could exploit this vulnerability to gather detailed information about the services running on a system, including their versions and configurations, and use that knowledge to gain unauthorized access. Restricting access to RPC services so that only trusted hosts can connect prevents this reconnaissance (BetaFred, 2023). Applying patches to RPC services addresses known vulnerabilities and reduces the risk of exploitation. Additionally, auditing the system to identify and turn off unnecessary RPC services minimizes the attack surface. For example, many organizations have reduced risks by identifying legacy services that are no longer needed and removing them entirely. Monitoring network traffic for unusual activity, such as multiple failed attempts to connect to RPC services, can help detect and stop attacks early. By addressing this vulnerability, the organization can reduce the likelihood of attackers gaining a foothold in the network.

The second vulnerability in this category involves the cleartext transmission of sensitive information via HTTP, which poses a serious risk to data security. For example, attackers could intercept unencrypted data, such as login credentials or personal information, transmitted over HTTP connections. Enforcing HTTPS ensures that all communications are encrypted, protecting sensitive data in transit (Postal, 2024). Redirecting HTTP traffic to HTTPS prevents users from inadvertently accessing unsecured versions of websites, which is a common entry point for attackers. For instance, many organizations have implemented HTTP-to-HTTPS redirects to ensure secure connections for users accessing their web applications. Regularly reviewing and updating HTTPS certificates is also necessary to maintain strong encryption standards, such as SHA-256 (*Weak Signature Algorithms - Security on the Web | MDN*, 2023). For example, organizations that replaced their SHA-1 certificates after 2016 avoided vulnerabilities that could have allowed attackers to forge certificates. Training employees to recognize and report non-secure connections further strengthens this defense. Addressing this vulnerability protects sensitive data and reassures users that their interactions with the organization are secure.

Addressing vulnerabilities in the Scheduled Maintenance category should be the top priority because these issues represent the organization's most immediate and severe risks. For example, vulnerabilities in the SMB server, such as those addressed by the MS17-010 update, could allow attackers to execute malicious code remotely, as was seen in the WannaCry ransomware attack, which exploited SMBv1 vulnerabilities (BetaFred, 2023). Applying this update and disabling SMBv1 actively protects the organization by eliminating exposure to these critical entry points. These steps are relatively quick to implement, as they involve applying vendor-provided patches and making configuration changes that do not require significant downtime. Disabling SMBv1 and enabling SMB signing can be completed within hours, providing an immediate boost to the organization's security posture. Additionally, prioritizing these vulnerabilities prevents attackers from exploiting them to gain unauthorized access or disrupt operations. After resolving these issues, the organization can actively tackle vulnerabilities with longer implementation timelines, such as updating policies or fixing HTTP-related weaknesses. This step-by-step approach ensures that the most critical threats are neutralized first, minimizing the risk of severe breaches and improving overall security.

References

BetaFred. (2023, June 7). *Microsoft Security Bulletin MS10-012 - Important*. Microsoft Learn. https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-012

BetaFred. (2023, March 1). *Microsoft Security Bulletin MS17-010 - Critical*. Microsoft Learn. Retrieved November 29, 2024, from https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010

Postal, C. (2024, November 18). *How to identify and strengthen weak SSL | UpGuard*. Retrieved November 29, 2024, from https://www.upguard.com/blog/weak-ssl

Weak signature algorithms - Security on the web | MDN. (2023, July 4). MDN Web Docs. Retrieved November 29, 2024, from https://developer.mozilla.org/en-US/docs/Web/Security/Weak_Signature_Algorithm