Southern New Hampshire University

CYB 400 Project One Milestone Template

Complete this template by replacing the bracketed text with the relevant information. One vulnerability has been added as an example.
Note: For this assignment, include only five of the same vulnerability differentiated by Vulnerability Detection Result.

Vulnerability Categorization		
Scheduled Maintenance	Policy Update	Other Security Issues
List the vulnerabilities from the scan that can be reasonably addressed in one week ● NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) ● NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) ● NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) ● NVT: Microsoft SQL Server Multiple Vulnerabilities (3065718) – Remote ● NVT: Microsoft SQL Server End Of Life Detection	List the vulnerabilities from the scan that can be reasonably addressed in one month ● NVT: SMB Brute Force Logins With Default Credentials (admin:guest) ● NVT: SMB Brute Force Logins With Default Credentials (multiple entries) ● NVT: Microsoft ASP.NET Information Disclosure Vulnerability (2418042) ● NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	List the vulnerabilities from the scan that can be reasonably addressed in two months ● NVT: DCE/RPC and MSRPC Services Enumeration Reporting ● NVT: SSL/TLS: Report Weak Cipher Suites ● NVT: Cleartext Transmission of Sensitive Information via HTTP ● NVT: Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) – Remote ● NVT: TCP timestamps
Scheduled Maintenance Rationale	Policy Update Rationale	Other Security Issues Rationale
The vulnerabilities categorized under Scheduled Maintenance pose immediate and significant risks to network services and data integrity and availability. These	Procedural and administrative changes to how the organization handles security protocols and sensitive data update the policies addressing vulnerabilities.	This category includes vulnerabilities that, while they pose significant security risks, allow for a longer response window due to their complexity or reliance on more

Vulnerability Categorization		
Scheduled Maintenance	Policy Update	Other Security Issues
include severe threats like remote code execution, privilege escalation, and unauthorized access, primarily associated with widely used services such as SMB and HTTP protocols and SQL servers. Due to their high impact and the potential for rapid exploitation by attackers, these vulnerabilities require urgent patches and updates to close security holes. Immediate attention to these issues will help prevent breaches that could disrupt operations, lead to data loss, or allow further penetration into network systems. Moreover, these are vulnerabilities for which vendors have already provided fixes, meaning they can be fixed quickly with minimal testing to provide compatibility.	Including enforcing more robust authentication measures to counter brute force attacks, updating encryption standards to secure data transmissions, and revising policies to ensure the use of secure cryptographic algorithms in SSL/TLS certificates. Addressing these vulnerabilities requires technical solutions and changes to organizational policies and user behaviors, such as mandating complex passwords, regular password changes, and secure communication protocols. Implementation might require extended staff training, updating of security policies, and system configurations, which naturally take longer to deploy organization-wide. Such changes are crucial for long-term security enhancements and reducing surface areas for attacks.	expansive system upgrades. For example, vulnerabilities related to end-of-life software or those requiring extensive changes to network architecture (like turning off outdated protocols and services or enhancing encryption methods across multiple systems) fall into this group. These issues often require in-depth testing, new software or hardware procurement, and detailed planning to ensure that changes do not disrupt existing operations or introduce new vulnerabilities. The extended timeline also allows for good risk assessment, stakeholder communication, and training to ensure all system users are aware of changes and new security practices.