Southern New Hampshire University

CYB 400 3-3 Project One Milestone: Categorized List of Security Vulnerabilities

Andree Salvo
Southern New Hampshire University
CYB 400
Instructor: Robert Chubbuck

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 SQL Server End Of Life Detection ● NVT: Microsoft SQL Server Elevation of Privilege Vulnerability ● NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability ● NVT: Microsoft SQL Server Multiple Vulnerabilities (3065718) – Remote ● NVT: DEC/RPC and MSRPC ● services enumeration reporting	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: MS15-034 HTTP.sys Remote Code Execution Vulnerability ● NVT: SMB Brute Force Logins With Default Credentials (admin:guest) ● NVT: SMB Brute Force Logins With Default Credentials (ftp:guest) ● NVT: Microsoft SQL Server Multiple Vulnerabilities (3065718) – Remote	List the vulnerabilities from the scan that can be reasonably addressed in two months ● NVT: SSL/TLS: Report Weak Cipher Suites ● NVT: Microsoft ASP.NET Information Disclosure Vulnerability ● NVT: SSL/TLS: Certi cate Signed Using A Weak Signature Algorithm ● NVT: Microsoft SQL Server Elevation of Privilege Vulnerability ● NVT: Cleartext Transmission of Sensitive Information via HTTP
Scheduled Maintenance Rationale	Policy Update Rationale	Other Security Issues Rationale
These vulnerabilities can be fixed during	As for policy and updates, they need to	These take longer since they deal with

Vulnerability Categorization		
Scheduled Maintenance	Policy Update	Other Security Issues
normal operations by patching and disabling services. SQL Server updates, HTTP.sys, and Elevation of Privilege flaws already have vendor fixes, and RPC enumeration can be mitigated with traffic filtering. All if this can be resolved within a week with little disruption.	set stronger rules around passwords and patching. SMB default accounts can show weak credential use, and by keeping the policies updated it will help prevent repeated problems.	encryption, certificates, and app settings. They need more planning and testing before making any further changes.