Introduction to Vulnerability Management - Course Challenge Report

Name of Individual Conducting Scanning:	0x4C3DD
Nessus Scanner IP (IP of Kali VM):	10.0.2.4
Date & Time Scan Started:	February 22 at 7:37 PM
Date & Time Scan Finished:	February 22 at 8:22 PM
Security Issues Identified:	37

Overview

The machine is Metasploitable 2 (2019 edition), with **7 high**, **15 medium**, **2 low** & 53 informative level of security alerts. The host information are as follows:

IP: 10.0.2.5
MAC Address: 08:00:27:DB:7E:44
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Top 5 Most Serious Security Issues (In priority order - most important first):

1. **70728 - Apache PHP-CGI Remote Code Execution**: The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.
2. **134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)**: A file read/inclusion vulnerability was found in A JP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).
3. **39469 - CGI Generic Remote File Inclusion**: The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.
4. **59088 - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution**: The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.
5. **19704 - TWiki 'rev' Parameter Arbitrary Command Execution**: The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

Top 5 - Remediations (In priority order - most important first):

1. Make sure to update PHP to version 5.3.13 or 5.4.3, or any subsequent release.
2. Adjust the AJP configuration to necessitate authorization or consider upgrading the Tomcat server to version 7.0.100, 8.5.51, 9.0.31, or later iterations.
3. Take measures to restrict access to the vulnerable application, and promptly communicate with the vendor to obtain a patch or explore the possibility of upgrading.

4. If utilizing Lotus Foundations, prioritize upgrading the operating system to version 1.2.2b or any later version. Alternatively, if not on Lotus Foundations, ensure PHP is upgraded to 5.3.13 or 5.4.3, or newer editions.
5. Implement the relevant hotfix as outlined in the vendor advisory to address any existing vulnerabilities.