Introduction to Vulnerability Management - Course Challenge Report Template

Name of Individual Conducting Scanning:	G R Nitin
Nessus Scanner IP (IP of Kali VM):	10.0.2.15
Date & Time Scan Started:	08/09/23 @ 5:46 PM IST
Date & Time Scan Finished:	08/09/23 @ 6:05 PM IST
Security Issues Identified:	69

Instructions

1. Please refer to the Course Challenge Brief for instructions on what you are being asked to do.
2. Answer all questions mentioned below.

Overview

>> Provide an overview of the results from the scan. How vulnerable is this system?<<

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

>> What are the 5 most critical issues with the scanned system? Talk about each one, and what could happen if an attacker exploits the vulnerability <<

1. The remote server's exported NFS shares can be mounted by a scanning host, potentially enabling an attacker to read and write files on the remote host.
2. The Unix operating system on the remote host, based on its reported version, is unsupported, leaving it vulnerable to security issues without vendor-supplied patches.
3. The VNC server on the remote host is vulnerable due to a weak password used by Nessus for authentication, allowing potential remote attackers to gain system control.
4. A shell is open on the remote port without any authentication, enabling potential attackers to connect and send commands directly.
5. Apache Tomcat version 5.5.x or lower is no longer vendor-supported, potentially leaving it susceptible to security vulnerabilities due to the absence of new patches.

Top 5 - Remediations (In priority order - most important first):
>> What are the suggested remediation actions to address the top 5 most critical security flaws? Re-word them, don’t just copy and paste Nessus’ suggestions <<

1. Secure NFS on the remote host to allow only authorized hosts for mounting its shares.
2. Upgrade to a currently supported version of the Unix operating system.
3. Enhance VNC security by configuring it with a robust password.
4. Check for signs of compromise on the remote host and, if needed, reinstall the system for security.
5. Upgrade to a version of Apache Tomcat that is currently supported.