Introduction to Vulnerability Management - Course Challenge Report Template

Name of Individual Conducting Scanning:	Alejandro Fonseca
Nessus Scanner IP (IP of Kali VM):	I used my Mac not Kali.
Date & Time Scan Started:	10:02 PM PST, 7/17/24
Date & Time Scan Finished:	10:11 PM PST, 7/17/24
Security Issues Identified:	22

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. Most serious issue **NFS Exported Share Information Disclosure**
2. Security flaw **VNC Server 'Password' Password**
3. Security flaw **SSL Version 2 Scan/ Plugin #2007**
4. Security flaw **Bind Shell Backdoor Detecion**
5. Security flaw **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**

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. Most serious issue remediation
    a. Reconfigure the NFS on the remote host so that only authorized users can mount its remote shares.
2. Security flaw remediation
    a. Secure the VNC service with a stronger password
3. Security flaw remediation

    a. Disable SSL 2.0 and 3.0
        i. Use TLS 1.2 or higher
4. Security flaw remediation
    a. Verify to see if the remote host has been compromised and reinstall the system if necessary.
5. Security flaw remediation
    a. All SSH/ SSL/ OpenVPN key material should be regenerated.