Vulnerability Analysis Report

☰ Tags	
Files & media	SBT_Vuln_Mgmt_Chall_Rep.odt kb_192.168.6.134.txt

Introduction to Vulnerability
Management - Course Challenge Report Template

Name of Individual Conducting Scanning:	Richard Brandon
Nessus Scanner IP (IP of Kali VM):	192.168.6.132
Date & Time Scan Started:	2023-02-26 @ 6:25 PM
Date & Time Scan Finished:	2023-02-26 @ 6:45 PM
Security Issues Identified:	89

Overview

The machine has 89 different vulnerabilities. In this report, I will provide a detailed analysis of the top 5 most serious security issues and their remediations. These vulnerabilities can be exploited remotely, allowing attackers to gain unauthorized access to the system, steal sensitive information or execute arbitrary code. It is critical that these vulnerabilities be patched as soon as possible to prevent potential attacks.

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

1. NFS Exported Share Information Disclosure: This vulnerability occurs when NFS (Network File System) shares are exported without proper access controls. It allows unauthorized users to access sensitive information on the file system. Exploiting this vulnerability remotely can result in the theft of sensitive data.
2. rexecd Service Detection: rexecd is a remote execution daemon that allows users to execute commands on a remote system. However, if this service is not properly secured, it can be exploited by attackers to execute arbitrary commands on the system. This vulnerability can be exploited remotely and can result in unauthorized access to the system.
3. UnrealIRCd Backdoor Detection: UnrealIRCd is an open-source IRC (Internet Relay Chat) server. In 2010, a backdoor was discovered in the software that allowed attackers to execute

arbitrary commands on the system. This vulnerability can be exploited remotely and can result in unauthorized access to the system.

4. VNC Server 'password' Password: VNC (Virtual Network Computing) is a remote desktop sharing software. If the server is configured with a weak or default password, it can be easily guessed by attackers, allowing them to gain access to the system. This vulnerability can be exploited remotely and can result in unauthorized access to the system.
5. Bash Remote Code Execution (Shellshock): Bash is a popular shell used in many Unix-based systems. In 2014, a vulnerability was discovered in Bash that allowed attackers to execute arbitrary code on the system. This vulnerability can be exploited remotely and can result in the compromise of the entire system.

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

1. NFS Exported Share Information Disclosure: To remediate this vulnerability, ensure that proper access controls are in place for NFS shares. This includes restricting access to only authorized users and groups, and ensuring that sensitive data is not stored in NFS shares.
2. rexecd Service Detection: Disable the rexecd service, or configure it with proper access controls. If the service is required, ensure that it is only accessible to authorized users and groups.
3. UnrealIRCd Backdoor Detection: Upgrade to the latest version of UnrealIRCd that does not contain the backdoor. Additionally, ensure that the server is configured securely and only accessible to authorized users.
4. VNC Server 'password' Password: Ensure that VNC servers are configured with strong, unique passwords that are not easily guessable. Additionally, ensure that the VNC server is only accessible to authorized users, and is properly configured to encrypt all communications.
5. Bash Remote Code Execution (Shellshock): Upgrade to a patched version of Bash that addresses the vulnerability. Additionally, ensure that all software on the system is up to date, and that access controls are in place to restrict access to sensitive areas of the system.