Metasploitable 2 Vulnerability Assessment Report

Name of Individual Conducting Scanning:	Ariel Bethea
Nessus Scanner IP (IP of Kali VM):	127.0.0.1
Date & Time Scan Started:	1/2/2024 at 9:13 pm
Date & Time Scan Finished:	1/2/2024 at 9:38 pm
Security Issues Identified:	RPC, Remote shell gain, Service detection, Backdoors

Overview

The advanced scan produced 72 security issues, revealing a high level of vulnerability. This report details the high-priority issues, including network file system vulnerabilities, port access, operating system version, password usage, and encryption connections. Identified below are recommended solutions for these issues.

Top 5 Most Serious Security Issues:

1. Critical – 10.0* CVSS | 5.5 VPR
    - NFS Exported Share Information Disclosure
        i. At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to use this vulnerability to read and potentially write files on the remote host.
2. Critical – 10.0 CVSS
    - Unix Operating System Unsupported Version Detection
        i. The Unix operating system running on the remote host is no longer supported, which suggests that the vendor will not release any new security patches. Thus, this version is likely to contain security vulnerabilities.
3. Critical – 10.0* CVSS
    - VNC Server ‘password’ Password
        i. The VNC server running on the remote host lacks security due to a weak password. A remote, unauthenticated attacker could exploit this using brute force to take control of the system.
4. Critical – 9.8 CVSS
    - SSL Version 2 and 3 Protocol Detection
        I. The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. However, due to several cryptographic flaws, NIST has determined that SSL 3.0 is no longer acceptable for secure communications. Additionally, based on the PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. These flaws can be exploited by attackers to conduct man-

in-the-middle attacks or to decrypt communications between the affected service and clients.

5. Critical – 9.8 CVSS
    - Bind Shell Back Door Detection
        i. Lack of authentication requirements on a shell listening on the remote port can be used by attackers to connect to the remote port and send commands directly.

Top 5 - Remediations

1. Update configuration of NFS on remote host so that remote shares cannot be mounted by unauthorized users.
2. Upgrade to a currently supported version of the Unix operating system.
3. Improve security by implementing a stronger password and password policy.
4. Disable SSL 2.0 and 3.0. Enable TLS 1.2 or higher, with approved cypher suites.
5. Delete and reinstall the system if it is verified that the remote server has been compromised.