**Table of Contents**

1. Introduction
2. Objectives
3. Risk Scoring
4. Risk Results
5. Pentesting Activities
6. Risk Details
7. Conclusion

My name is Cameron Stefanic and this is the pentest report done for Metasploitable 2. I’ve been studying for red team operations now for 2 years and have 4 years of cyber security experience all together.

I have all of the necessary certifications to help your company succeed and am driven to take a step forward with your business. I have taken 1:1 coaching from a professional pentesting company out of Manhattan and have reached the top 6% on TryHackMe’s website.

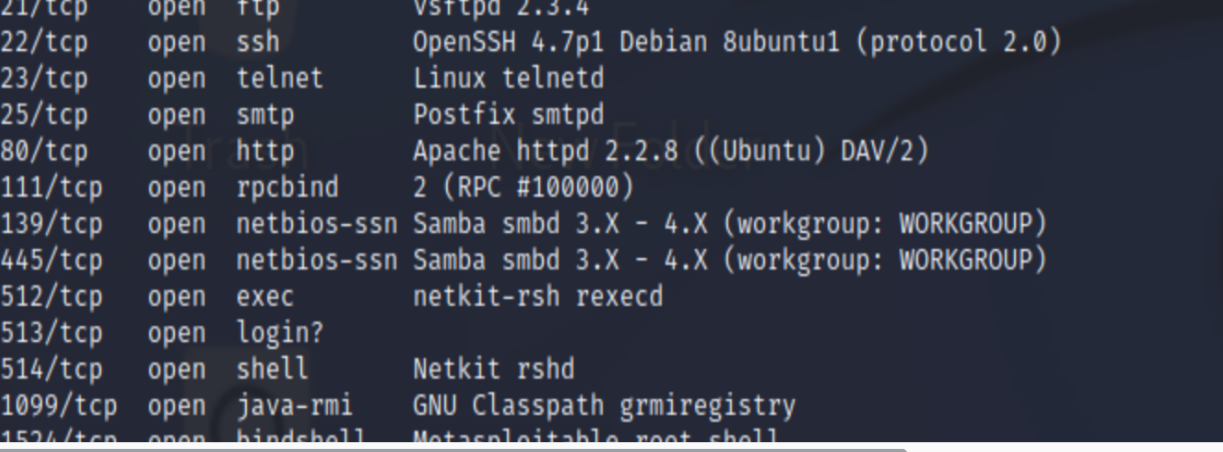
**Objectives**

1. **Vulnerability Metrics**

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

(**https://nvd.nist.gov/vuln-metrics/cvss**)

Text

Description automatically generated

The NMAP scan above showed a variety of vulnerabilities. I decided to pursue the easiest to exploit first and do further testing down the line.

**Graphical user interface, text

Description automatically generated**

**CVSS Score: 10**

A backdoor shell was created for the following vulnerability which allowed me to attack port 21.

Text

Description automatically generated

**CVSS Score: 7.2**

Allows the execution of unauthorized code or commands.

Graphical user interface, text

Description automatically generated

**CVSS Score: 9.8** Allows the execution of backdoor command execution and the available exploit of malicious code.

**Risk Scoring**

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

**Pentesting Activities**

* SMTP-user-enum= Tool for enumerating shares of OS level user accounts
* NMAP- Shows available ports to target
* Metasploit- One of the best weapons on Kali Linux. It was crucial in determining certain openings in the system. Used for the backdoor code execution.

**Conclusion**

The Metasploitable 2 system has many available areas of attack. The most important hardening advice I currently have is to take down the available backdoor openings first.

The ability to craft malicious code and execute it on the network will take down your system availability, cost millions in breach of Confidentiality and Integrity files, and reduce customer trust in the long term.