VM Scanner Background Report

***Abdu Kiyaga***

CMIT 421 *6380* Threat Management and Vulnerability Assessment

***February 9, 2023***

# Introduction

Based on a recent vulnerability scan results performed on Mercury USA’s system. Among the machines that were scanned on the IP range 192.168.1.0/25, the system on 192.168.1.30 was found with the most critical vulnerabilities which need to be solved as soon as possible. In total, the system was found with five vulnerabilities carrying a Common Vulnerability Scoring System (CVSS) rating of 10, which is the highest level of severity. In the following section, we will discuss three of the critical vulnerabilities and the risk they pose to the operations of the company. Later, we will so recommend how the organization can protect itself from such vulnerabilities living on the system and a vulnerability scanner that can periodically check if there are more vulnerabilities on the system.

# Part 1: Nessus Vulnerability Report Analysis

In my view, it is appropriate to distribute the report in this current format because it highlights the vulnerabilities using color codes to emphasize the most critical and those that pose the most risk to company activities. The most critical vulnerabilities are in red with a scale rating of 10 which is the highest rating, medium vulnerabilities are labeled orange while low ranked vulnerabilities are labeled green. This means that Mercury USA can prioritize on the most critical vulnerabilities and shelve others for the future. Furthermore, the report is easy to interpret such that if company executives are provided the html format report, they can click on the plugin number and find out more information on the vulnerability and how to guard against it. In this section, we will discuss three of the five most critical vulnerabilities that are critical threat to the operations of Mercury USA as seen in the provided Nessus vulnerability report. These vulnerabilities are the most critical because they have a vulnerability score of 10/10.

1. Unix Operating System Unsupported Version Detection. According to the scan, the host operating system on which the scan was conducted is out of date and is no longer supported by Linux. The remote host runs on version 1.279 which no longer receives any patch updates from the vendor. This means that any known security vulnerabilities can be exploited (Tenable, 2008). To solve this vulnerability, Mercury USA should upgrade its system to the most recent version to enjoy system updates and security patches.
2. NFS Exported Share Information Disclosure. Besides an out of date operating system, the scan also discovered that attackers could remotely access the Network File System (NFS) on the host. The NFS system allows attackers the privilege to read and modify files on the system by overwriting them. Such a vulnerability puts Mercury USA at risk of facing eavesdropping and impostor attacks. In addition, exploiting this vulnerability can put the company’s data at risk of being wiped out or encrypted by attackers which not only will cause denial of service but could explode into a ransomware attack. This vulnerability can be solved by upgrading to the most recent NFS version, disabling remote access to NFS shares and only allowing local machines to have authorization to access the NFS shares (Sheinin, 2002).
3. Bind Shell Backdoor Detection. For attackers to remain active on the victim system, share files or remove files, they usually need a constant communication channel with the victim system. This connection is usually enabled when an attacker utilizes the netcat utility to connect to open ports to the system. When this happens, the attackers who are usually remote, can execute commands, pivot through the system as well as giving themselves root privileges such as adding or removing users on the system.

|  |
| --- |
| An example of a Nessus scan and system discovered vulnerabilities |

# Part 2: The Business Case

In my assessment, Mercury USA’s overall current security posture is weak and vulnerable to attacks that could not only cause reputational and financial damage, but it could also put customers’ data at risk of being sold to the unscrupulous actors leading to identity theft. Normally, attackers will perform reconnaissance on a company before they perform port scanning. In the case of the host on 192.168.1.30, attackers would be glad to discover that they can mount files onto the file share systems and most importantly for them, they can use other hosts to establish connections using netcat and meterpreter sessions to perform further scans on the systems.

When attackers establish meterpreter sessions, it will take a long time for company administrators to find out that attackers are on the system because they would be using host IP address to move through the system. In this case, attackers can use 192.168.1.30 gain access to the system, perform system scans to discover other hosts such as 192.168.1.25 to modify files.

The types of threats that could manifest from these events include data exfiltration attacks, ransomware denial of service and distributed denial of service as well as advanced persistent threats.

# Part 3: Nessus Purchase Recommendation

To identify vulnerabilities, most industrial players utilize vulnerability scanners such as port scanners and ping scanners. Popular examples include Nessus scanner which would most likely is the scanning program that is advised for use with Mercury USA. With swift, precise scanning and few false-positives, Nessus pinpoints the vulnerabilities that require addressing. In addition, Nessus generates a report highlighting the vulnerabilities, the associated risk and how they could be remediated. Its visually appealing nature of reports using color codes such red for critical vulnerabilities, yellow for medium enables companies to know which vulnerabilities should be prioritized (Wendlandt, n.d)

As highlighted in an earlier section, scoring features within Nessus are adequate for technical professionals because results are presented in an a detailed, easy to read format that enables professionals to focus on the most critical vulnerabilities based on CVSS scores. These scored are also used by regulatory, compliance and threat monitoring bodies such as National Institute of Standards and Technology (NIST) and the National Vulnerability Database (NVD). Suffice to note, Nessus is equipped with a database of 57,000 Common Vulnerabilities and Exposures (CVE) and with the lowest false positive rating with a reported 32 defects for every million scans conducted (Tenable Community, n.d).

There are three Nessus versions on the market; Nessus Essential, Professional and Tenable.io. I would recommend that Mercury USA purchases the Nessus Professional license which costs in the upward of $3000 provides compliance checks for several frameworks such as the Payment Card Industry Security Standard (PCISS), Federal Desktop Core Configuration (FDCC), Center for Internet Security (CIS) and NIST (Cooper, 2022). In addition, Nessus will provide training and around the clock support with this version if Mercury pays an extra $400 a year.

## Conclusion

To prevent cybersecurity breaches, it is essential to have a vulnerability management architecture in place that often scans for emerging vulnerabilities. Loopholes left on the network for extended periods of time without a vulnerability assessment and patch management mechanism allow adversaries more opportunities to take advantage of flaws and launch attacks as a result. It is therefore important for Mercury USA to adopt the Nessus scanning system to identify, detect and remediate against vulnerabilities on its network. The highlighted risks of not having a solution in place are more of a motivation to have one and keep the network hardened and safe. By doing this, Mercury USA can maintain its growth, productivity, and ability to run a successful firm in the transportation sector.

# References

Cooper, S. (2022, October 10). Nessus Vulnerability Scanner Review. Comparitech. <https://www.comparitech.com/net-admin/nessus-vulnerability-scanner-review/>

Sheinin, S. (2002). NFS Security. In Global Information Assurance Certification. SANS Institute. Retrieved February 13, 2023, from <https://www.giac.org/paper/gsec/25/nfs-security/100222#:~:text=NFS%20like%20any%20other%20unprotected,unauthorized%20access%20to%20the%20network>.

Tenable Community. (n.d.). <https://community.tenable.com/s/question/0D53a00008stb3HCAQ/reporting-false-positive-case-on-nessus-pro-vulnerabilities-scanning-on-161691>

Tenable. (2008). *Unix Operating System Unsupported Version Detection*. Tenable®. <https://www.tenable.com/plugins/nessus/33850>

Wendlandt, D. (n.d.). Nessus. Retrieved February 14, 2023, from <https://www.cs.cmu.edu/%7Edwendlan/personal/nessus.html>