VM Scanner Background Report

***Reece Hugo Zunino***

CMIT 421 *<Section #6380>* Threat Management and Vulnerability Assessment

***02/10/2023***

# Introduction

Mrs. McNamara,

There are going to be a few things that I will be going over in this analysis of the Nessus report. Using the report you gave me to analyze, we will go through some of the more critical issues found based on the scan result and the best ways to mitigate those threats. You stated your concerns when you reported to me, and you have a reason to worry based on the contents of the VM scan report. I will also be covering the potential of using Nessus as a primary tool to be used as the vulnerability assessment tool for Mercury USA. Even though it is expensive, it will far outperform the free OpenVAS tool used by the third-party company that did the initial assessment for us previously.

# Part 1: Nessus Vulnerability Report Analysis

A basic network scan was conducted using the Nessus vulnerability scanner on the Mercury USAs network. The report shows that four IP addresses were scanned, and vulnerabilities were detected throughout the network. Below is a summary of what was found on each IP address:

• 192.168.1.10 resulted in (1 High, 1 Medium)

• 192.168.1.25 resulted in (1 High, 2 Medium, 2 Low)

• 192.168.1.30 resulted in (5 Critical, 1 High, 12 Medium, 2 Low)

• 192.168.1.100 resulted in (1 Medium)

Based on the summary above, the first step in mitigating the risk of an outside attack should be addressing the issues with IP 192.168.1.30 first and then moving on to the other hosts patching and mitigating all the critical and high vulnerabilities. This network shows that host 192.168.1.30 has five critical issues that must be addressed. This is why this host should be first when it comes to mitigating the risk to Mercury USA’s network. We will be addressing mainly the high and critical vulnerabilities found on the network.

The **Debian Open Secure Shell (OpenSSH)/ Open Secure Socket Layer (OpenSSL) Package Random Number Generator Weakness** vulnerability must be addressed because an attacker can easily obtain the private part of a remote encryption key and use it to conduct a man-in-the-middle attack. An easy solution to this vulnerability is following the guidance released by Debian security under DSA 1571-1, which means that we have to upgrade our openssl package and regenerate any cryptographic material outlined in the security announcement. The other Debian critical vulnerability will also fall under this security message (Weimer, 2008).

The **Bind Shell Backdoor Detection** vulnerability is quickly addressed. According to the tenable database, “A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly”. This means the remote host could be compromised, but this doesn’t mean it has been through. We would need to verify if the remote host has been compromised, and if it has not, we need to reinstall the system if necessary and monitor that host for any other issues with this Blind Shell Backdoor.

The **Network File System (NFS) Exported Share Information Disclosure** Vulnerability Needs to be configured so that only authorized hosts can mount their remote shares. This way, no one not allowed to on the remote host will be unable to mount an exported NFS Share by a scanning host. If an attacker could exploit this, they would have the ability to read or possibly even write on the files on the remote host.

The **Unix Operating System Unsupported Version Detection** vulnerability means an outdated operating system runs on the remote host. This operating system is no longer supported, so that no security vulnerabilities will be patched in the future. The operating system needs to be upgraded to a version of Unix currently supported. Suppose this operating system is not upgraded, and the attackers can see when they are reconfiguring our systems. In that case, they will notice that we have a host running an unsupported operating system. They could use that to their advantage when trying to find a door into our network.

The **vulnerability of the Secure Socket Layer (SSL) Version 2 and 3 Protocol Detection** is highly severe but is also considered critical by the tenable database. It is recommended to disable SSL 2.0 and 3.0 and to use Transport Layer Security (TLS) 1.2 instead. If it is not disabled, the attacker may be able to downgrade the connection to a web browser using a POODLE attack. “A POODLE vulnerability lets the attacker eavesdrop on encrypted communication. This means the attacker can steal confidential data transmitted, for example, passwords or session cookies, and then impersonate the user (Nidecki, 2020)”.

Regarding the other hosts on the network, we will start with 192.168.1.10. This host has one high vulnerability. The **MS17-010: Security Update for Microsoft Windows Server Message Block (SMB) Server** vulnerability is one that our CEO is most concerned about because it will allow the ransomware WannaCry which is what affected our competitor by utilizing the ETERNALBLUE exploit. This vulnerability can be mitigated by using the solution from Microsoft. “Microsoft has released patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8 (Tenable, 2022)”.

Host 192.168.1.25 has one critical and two medium-severity vulnerabilities found during the scan. As stated, we should concentrate on the higher severity vulnerability and work our way from there. The **Microsoft Windows Server Message Block (SMB) Shares Unprivileged Access** vulnerability is an increased severity but is an easy fix to mitigate the problem. From the tenable database, the solution is “to restrict access under Windows, open Explorer, right-click on each share, go to the 'Sharing' tab, and click on 'Permissions'.”

Now that we have addressed the most important vulnerabilities that need to be addressed based on the report, we can go into more detail about the tool and how it differs from OpenVAS. The reports Nessus generate are superior to those given to us using the OpenVAS tool. Not only are the words easier to read and more organized they are also well-detailed and organized. Each vulnerability found using the Nessus vulnerability tool allows the user to examine each exposure in detail using the tenable database. In that database, even more, information explains the vulnerability and solution. Sometimes, there is also third-party information from either the application or systems manufacturer or other helpful information to help mitigate the risk of that vulnerability. Below is an image of what a Nessus report looks like. This report could be more detailed for those outside the IT department and could be understood. Those dealing with these reports should do a more minor, simplified report for others, like our CEO, that might want a snapshot of what our current network vulnerabilities may look like.

![Graphical user interface, text

Description automatically generated]()

# Part 2: The Business Case

Regarding Mercury USA’s overall security posture, I would say that we are currently in a poor situation, and numerous issues need immediate attention to ensure the security of our information and data and for our customer’s peace of mind as well. After reviewing the Nessus scan report on the four scanned hosts, I would have to determine that we have open doors that would allow attackers numerous ways into our network in its current state. The damage that could be caused to Mercury USA could be catastrophic and a financial burden to recover from versus fixing the problems that currently exist on the network. Our network is presently not Payment Card Industry Data Security Standard (PCI DSS) compliant, which is doing our customers a disservice to our current information security state. There are 12 requirements that we must meet for our company to stay PCI DSS compliant.

The requirements that we are currently failing at are Encrypt Transmitted Data, Properly Updated Software, Restrict Data Access, and Scan and Test for Vulnerabilities, to name a few. According to the digital guardian, “Complying with Payment Card Industry (PCI) Security Standards seems like a daunting task, at the very least. The maze of standards and issues seems like a lot to handle for large organizations, let alone smaller companies. Yet, compliance is becoming more important and may not be as troublesome as you assume, especially if you have the right tools (Groot, 2021)”.

The right tools mean having a good solid vulnerability scanner to start with to ensure our data is safe and protected to stay within compliance. Since our company is a shipping and logistics company and is around the small to medium range as far as how large Mercury USA is, we are still a target for threats, whether it is an outside actor or even a disgruntled employee who may want revenge for being laid off. This is why ensuring information safety is a priority, especially in a logistics company. One of the main concerns from our CEO was trying to ensure that we did not suffer the same fate as our competitor, which was attacked using the ransomware WannaCry. This would be very easy in the company’s current security state because all our hosts have a few, if not many, vulnerabilities, and some have multiple critical vulnerabilities. The network host 192.168.1.30 is a prime example of a host that a black hat hacker can easily exploit to gain information or attempt to take over and encrypt our information for ransom.

# Part 3: Nessus Purchase Recommendation

In my expert opinion, as Mercury USA’s cyber threat analyst, I would recommend either version of the Nessus vulnerability scanning tool differently. “The benefit of buying a product that can perform realistic PCI audits is that when your official quarterly PCI scan is performed, you won't be surprised and will have had a chance to fix issues before your audit occurs. Also, if your scanning service makes an error or has inaccurate results, being able to compare their results with your own can help expedite any incorrectly reported issues (Gula, 2013)”. The Nessus tool is one of the leading tools in the industry regarding network security; 87% of all companies use Tenable Security Center, or one of the Nessus Scanning licenses, as their scanner of choice.

There are many features that the company can benefit from buying either Nessus Expert or Nessus Professional. I would recommend going with the Nessus Expert version because it has more features that would help our company and our CEO’s intent regarding our information security. The Nessus allows us to run unlimited IT assessments of our network and has a user-friendly graphical user interface (GUI). The color coding features on the Nessus report make it easier to know what our department needs to concentrate on in the immediate future and work our way down the list to ensure our company stays within PCI DSS compliance.

The current cost for a Nessus Expert license is $4,990 for one year or up to $14,221.50 for a three-year license. You can also add on advance support for $400 or on-demand training for $250 per person needing training. Compared to what could happen if we succumbed to the same fate as our competitor, this is a small price to pay versus what could happen if we had proprietary information stolen from our company (Tenable, n.d.).

## Conclusion

Within this report, I have covered many areas Mercury USA needs to improve on its security and where we need to start based on the Nessus vulnerability scan report I was given. We also discussed how our company needs to be able to meet the compliance guidelines of the PCI DSS council since this is vital for our line of work as a logistics and shipping company. Finally, we went over how beneficial having the Nessus vulnerability scanning tool on-demand at our company would help keep our information safe, and this would also give our customers ease of mind knowing that we have their information security in their best interests at heart.

## References

Bacon, M. (2020, December 15). What is the CVSS (Common vulnerability scoring system)? SearchSecurity. https://www.techtarget.com/searchsecurity/definition/CVSS-Common-Vulnerability-Scoring-System

Groot, J. (2021, August 12). What is PCI compliance? Digital Guardian. https://digitalguardian.com/blog/what-pci-compliance

Gula, R. (2013, May 13). Can I use Nessus to perform PCI audits? Tenable®. https://www.tenable.com/blog/can-i-use-nessus-to-perform-pci-audits

Nidecki, A. (2020, June 1). 403 forbidden. 403 Forbidden. https://www.acunetix.com/blog/web-security-zone/what-is-poodle-attack/

Tenable. (2022, May 25). MS17-010: Security update for Microsoft Windows SMB server (40... Tenable® - The Cyber Exposure Management Company. https://www.tenable.com/plugins/nessus/97833

Tenable. (n.d.). Nessus Plugin families. Tenable® - The Cyber Exposure Management Company. https://www.tenable.com/plugins/nessus/families

Tenable. (n.d.). Download Nessus vulnerability assessment | Nessus®. Tenable®. https://www.tenable.com/products/nessus

Weimer, F. (2008, May 13). [Security] [DSA 1571-1] new openssl packages fix predictable random number generator. Debian Mailing Lists -- Index. https://lists.debian.org/debian-security-announce/2008/msg00152.html