VM Scanner Background Report

***Jordan Lee***

CMIT 421 *Section #6980* Threat Management and Vulnerability Assessment

***22 October 2024***

**Introduction:**

This report assesses the Nessus Vulnerability Report and its effectiveness in convincing Mercury USA's leadership to incorporate the tool into its security strategy. The scan ran successfully on Wednesday, April 8th, and the report's findings examined four network hosts: 192.168.1.10, 192.168.1.25, 192.168.1.30, and 192.168.1.100. Vulnerabilities were found on all of the hosts. The host system with IP address 192.168.1.30 identified twenty vulnerabilities, five critical threats, one high threat, twelve medium-critical threats, and two low-critical threat levels.

This report aims to highlight three of the most severe flaws and explain how they might endanger Mercury USA's network infrastructure within the transportation sector. It will also examine and identify how an attacker could target the organization by exploiting the three most critical vulnerabilities. The report will examine Mercury USA's overall security posture, how it affects its capacity to offer shipping and logistics services to the transportation sector, and how it safeguards PII, credit card transactions, proprietary software, customer lists, order data, and customer information.

**Part 1: Nessus Vulnerability Report Analysis**

                The report stresses the importance of the Nessus Vulnerability Report in understanding and addressing network vulnerabilities, making the audience feel the value of the report. All the threats identified in the Nessus report are significant threats to Mercury USA because they allow attackers to gain administrative access to a system, enumerate hosts, execute commands by connecting to a shell listening on a remote port, and execute malicious code on a server. If an attacker is successful in carrying out one or more malicious actions, Mercury USA will be severely damaged by data exfiltration, denial of service (DoS), distributed denial of service (DDoS), and other sophisticated network attacks. The Nessus scan report is not only suitable for distribution to the Mercury USA leadership team, but it is also a powerful tool for understanding and addressing network vulnerabilities. It is designed to be easily readable and offers sufficient detail for readers of any professional background to comprehend the information.

The cybersecurity analyst can distinguish between critical and less severe vulnerabilities in the report using the Nessus Plugin IDs assigned to each vulnerability. These IDs hyperlink to a more detailed description and a suggested fix. The report also focuses on the vulnerabilities pertinent to Mercury USA, saving the analyst time and effort in sifting through a mountain of information. The report also includes sufficient details to address and fix vulnerabilities, including the three most serious ones that were previously found. It describes the vulnerability and the affected service or protocol and links to the Tenable Plugin entry, which offers more details and a possible fix.

The report provides crucial network vulnerability health information, empowering executives to assess and address these threats. It is available in an executive summary format, with threats categorized by severity and a comprehensive 'info' section for each threat. The host with the IP address 192.168.1.10 is responsible for the first and most serious vulnerability found. It has a high severity rating and a base score of 9.3 on the expected standard vulnerability scoring system, indicating that a critical security update for Microsoft Windows SMB (server message block) Server is missing. According to the Nessus Report, MS17-010 is a crucial security patch that addresses multiple vulnerabilities in

Microsoft Windows-based systems. According to [3], the "CVSS vector uses a single-line format to convey a vulnerability's ratings on all metrics described: physical, local, adjacent network, and network." The metrics previously described are used by the common standard vulnerability scoring system (CVSS)to assess the severity of vulnerabilities. This vulnerability can allow remote code execution if an attacker targets a Microsoft Server Message Block (SMB) server with maliciously constructed messages. If addressed, this vulnerability can lead to severe consequences. Attackers could exploit this vulnerability to execute remote code, compromising the system and potentially taking the network offline. The potential damage to the system is significant. They could also install persistent backdoors, run malicious code, increase privileges, and launch assaults against other weak systems on the network. Mercury USA should install the MS17-010 Critical Security update as soon as possible to close this vulnerability and prevent an internal or external threat from exploiting it.

The host with IP address 192.168.1.30 is the subject of the second and subsequent most critical vulnerability detected in the Nessus Report. It has been assigned a critical severity rating and a base score 10.0 on the standard vulnerability scoring system, indicating a "Bind Shell Backdoor Detection." It is assumed that a backdoor has been set up, giving the attacker access to the system through an unauthorized window, and it also signifies that the remote host was compromised. With enough privileges and unrestricted access, hackers can run commands to install malware, create a backdoor for future access, and compromise the system altogether; they might even use the compromised system as a launch point for more attacks against other systems on the network. To remediate this vulnerability, the IT cyber professionals at Mercury USA need to determine whether the remote host has been compromised. If the host is determined to be compromised, then Mercury USA needs to patch, reinstall, and re-authenticate users before access can be granted. The host with IP address 192.168.1.30 is the third and last of the three most critical vulnerabilities in the Nessus Report. Its critical severity rating and base score of 10.0 on the standard vulnerability scoring system indicate that the operating system has already reached the end of its lifecycle.

Based on the results, the Nessus scanning tool has identified an outdated operating system installed on the host. If this kind of vulnerability is found, the vendor does not provide patches, security updates, or updates. Unix Operating System Unsupported Version Detection is the name of the vulnerability that the Nessus scan caught.

Since the operating system is no longer upgradeable, an attacker can quickly identify and exploit its security flaws. This vulnerability allows the attacker to compromise the system and use that same system for future attacks, especially DDoS attacks and other network attacks. Since the UNIX operating system is no longer supported, the software company is less likely to address and disclose the vulnerability. According to [6], using an unsupported operating system can pose security issues and risk your system and business. To help protect against these dangers, using supported software that receives regular updates and patches is generally recommended. To remediate this vulnerability, users/companies need to upgrade/switch to a version of the operating system supported with security patches and updates.

# A computer screen shot of a computer Description automatically generated

A screenshot of a desktop

Description automatically generated

**Part 2: The Business Case**

                Mercury USA's current security posture regarding its IT infrastructure is inadequate and requires immediate and critical changes. The Nessus vulnerability scan has identified multiple critical vulnerabilities that could lead to significant damage if not addressed promptly. For example, if a hacker's intention is to gain unauthorized access, elevate privileges, and initiate network-wide attacks, they could easily compromise two systems: the hosts with the IP addresses 192.168.1.10 and 192.168.1.30. Remember that IP 192.168.1.10 is associated with MS17-010: Security Update for Microsoft Windows SMB Server, and IP 192.168.1.30 is associated with five critical vulnerabilities. Referring to the Nessus vulnerability report, it is evident that a hacker could easily take advantage of the vulnerabilities stemming from the missing MS17-010 critical security update. The attacker could easily compromise Mercury USA's IT systems using different techniques. With this information in mind, the attacker will likely obtain access to the servers that house the organization's most sensitive data. This data may include customer lists, personally identifiable information (PII), credit card information and transactions, proprietary software, and payment card industry data security standards (PCI DSS).

The other critical threat that needs to be discussed is host 192.168.1.30, with a critical-threat-level vulnerability discovered. The UNIX operating system installed on the system is outdated and no longer supported by the vendor; as a result, the operating system becomes a constant target for vulnerabilities and attacks, essentially acting as a backdoor. Security updates and patches are not getting pushed to that OS, so Mercury USA needs to update that system running the outdated OS or upgrade to an OS version the vendor will support. The security team with Mercury USA needs to address the most critical vulnerabilities, starting with installing security updates and updating operating systems, software, and applications as needed. The vulnerabilities found are severe and could pose significant risks to the organization. Applying the necessary updates, patches, and fixes would no longer allow attackers to access the systems. It is worth noting that even though the security team at Mercury USA took the required actions to remediate the vulnerabilities mentioned, there is still the possibility that attackers have already exploited those vulnerabilities and attempted to hack into their systems. If that is the case, there should be evidence and log files indicating such activity and evidence of prior attacks based on unusual network traffic.

**Part 3: Nessus Purchase Recommendation**

With its user-friendly graphical user interface, Nessus is a reliable and industry-best standard vulnerability scanning tool that enables organizations to perform various scans based on their specific needs. With both automated and manual tools, users can scan anything from a single host to an entire network, and each scan is guaranteed to produce detailed results based on common vulnerabilities and exposures (CVEs) while eliminating the possibility of outputting false positives. Nessus features incorporate a color-coded severity rating indicating the vulnerability's level of criticality based on known information and the standard vulnerability scoring system (CVSS) base score as determined by the CVE(s) linked to the vulnerability. Red is classified as critical; orange is classified as high; yellow is medium; green is low; and blue is classified as info regarding other scan details concerning the scanned host. Suppose a security professional reads the report and notices the word critical in a red box, followed by a CVSS base score of 10.0. In that case, it emphasizes that they need to pay attention to vulnerability and identify the potential risks to the host, what impact it will have on the organization if exploited, and focus on remediating the vulnerability.

These are crucial pieces of information because they explain how critical the vulnerability is, what it means, how it is relevant to the organization, and what could happen if left unpaid attention. The overall presentation and detailed report emphasize the most critical vulnerabilities, and the overall presentation and the scoring features are adequate for technical professionals. The most critical vulnerabilities are emphasized first, followed by high, medium, low, and informational vulnerabilities.The Nessus vulnerability tool is crucial in ensuring Mercury USA's compliance with industry standards and regulations, particularly the PCI DSS (payment card industry data security standard). It is designed with these regulatory and standard requirements in mind, ensuring users adhere to all necessary regulations and standards.

Mercury USA is subject to PCI DSS regulations and standards because the company operates and utilizes servers that house credit card data, PII, and transaction history. Tenable, the developer of Nessus, enables users to custom design and create audit policies to fit their needs. About maintaining the PCI DSS requirement, "PCI Audit Policies" are default audit policies designed "for minimum required PCI configuration settings." With this in mind, the organization can use the Nessus vulnerability scanning tool and work with the default. There are three options for purchasing Nessus, with two add-on options. One year of Nessus is $3,990; two years of Nessus is $7,780.50; three years of Nessus is $11,371.50, and the two optional options are advanced technical support and Nessus fundamentals, which teach users how to use the software.Nessus is the recommended scanning tool because it has the features, usability, and efficacy that Mercury USA needs to properly detect and remediate vulnerabilities while establishing compliance with all applicable regulatory and standard requirements.

OpenVAS, which was previously used to scan the network, is one example of an alternative vulnerability scanning tool available on the market. Despite being freely available to everyone, I strongly recommend Nessus, a high-quality product to Mercury USA, given its current security posture and potential for catastrophic consequences. With its presentation of the reports generated, technical details, and cybersecurity and networking terminology, the Nessus report must be more suitable and understandable for senior executives or management. Anyone with a background in these fields may need help understanding.

**Conclusion**

The Nessus vulnerability scanner report produced results that scanned four hosts showing vulnerabilities relevant to Mercury USA. However, the overall performance and scoring features make it simple to identify the most critical vulnerabilities. Nessus is a user-friendly vulnerability scanning tool that leverages more than 50,000 common vulnerability exposures (CVEs), Tenable's database of vulnerabilities and recommended solutions, and a powerful engine to detect vulnerabilities accurately. The report's technical details help a cybersecurity professional understand the vulnerability and recommended solutions. If more information is needed, clicking on the plugin ID will take users to Tenable's website to find more details about the vulnerability and a solution.

Furthermore, Nessus can be used to ensure that organizations do not violate any regulations or standards. Nessus is good for workers, management, and the company. It has all the features needed to scan the network for vulnerabilities thoroughly, figure out how to fix them, and audit target systems to ensure compliance. I strongly advise Mercury USA to invest in Nessus, purchase the one-year license, and spend an extra $400 for advanced technical support. While acquiring a license significantly strengthens the network's security posture, it is essential to remember that Nessus is just one part of the solution. When used with OpenVAS and a proficient cybersecurity team, Nessus ensures that vulnerabilities are promptly addressed, the network is regularly rescanned, and strict compliance is maintained. The overarching objective is to significantly bolster Mercury USA's security posture and safeguard its infrastructure from internal and external threats.

**References**

[1] "Chapter 5: Implementing an Information Security Vulnerability Management Process", Pearson CompTIA Cybersecurity Analyst (CySA+), 2020. [Online]. Available: <https://www.ucertify.com/>. [Accessed: 30-October-2024].

[2] “My Basic Network Scan”, Nessus, 08-Apr-2020. [Online]. Available: <https://learn.umgc.edu/content/enforced/1277340-027858-01-2248-US2-6980/My_Basic_Network_Scan_qw3e2d%20(2).html#idp1874872243> [Accessed on 14-Oct-2024].

[3] Chapple, M., & Seidl, D. (2023). Chapter 7 Analyzing Vulnerability Scans. In CompTIA CySA+ Study Guide Exam CS0-003 (3rd ed., pp. 245–284). essay, John Wiley & Sons, Inc.

[4] Chapple, M., & Seidl, D. (2023). Chapter 8 Responding to Vulnerabilities. In CompTIA CySA+ Study Guide Exam CS0-003 (3rd ed., pp. 293–333). essay, John Wiley & Sons, Inc.

[5] Chapple, M., & Seidl, D. (2023). Chapter 8 Responding to Vulnerabilities. In *CompTIA CySA+ Study Guide Exam CS0-003* (3rd ed., pp. 293–333). essay, John Wiley & Sons, Inc.

[6] IT Convergence. (2023, March 9). 5 security issues from using an unsupported operating system. <https://www.itconvergence.com/blog/how-safe-are-your-unsupported-legacy-operating-systems-and-software/>

[7] How to: Run your first vulnerability scan with nessus. Tenable®. (2019, August 22). <https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus>