

Nessus Background Report

Micah Martinez

CMIT 421 7380 Threat Management and Vulnerability Assessment

23 November 2021

Introduction

With the Information Technology (IT) department recently installing the 30-day free trial of Nessus [1], it is crucial to understand how to read the scan results and decide whether to purchase a license. Nessus scans and compares the system with over 66,000 Common Vulnerabilities and Exposures (CVE) [1] [2], in comparison to OpenVAS [3] that examines around 26,000 CVEs [4]. Using the results from the recent scan on Mercury USA's network, three of the most dangerous vulnerabilities will be identified with instructions on finding more information on what they are, how they can be remediated, and what effect they can have on Mercury USA. In addition, an in-depth analysis of Nessus' scan will be provided, and recommendations on how to interpret and disseminate results to those that need to know.

Part 1: Nessus Vulnerability Report Analysis

Nessus' scan reports are well organized and very simple to read. As seen in Figure 1, the report gives the number of vulnerabilities and divides them into five color-coded categories: Critical, High, Medium, Low, and Info. Table 1 [5] has a more detailed description of each category. Below this division, the vulnerabilities are listed from most to least severe by Common Vulnerability Scoring System (CVSS) values [6], allowing the reader to understand the general state of the network's security posture. Alongside the CVSS value is a link to a website where more information on the vulnerability can be found, including possible solutions. Although this information is valuable, it provides little immediate information regarding the vulnerability and requires navigation to a secondary webpage to learn more.

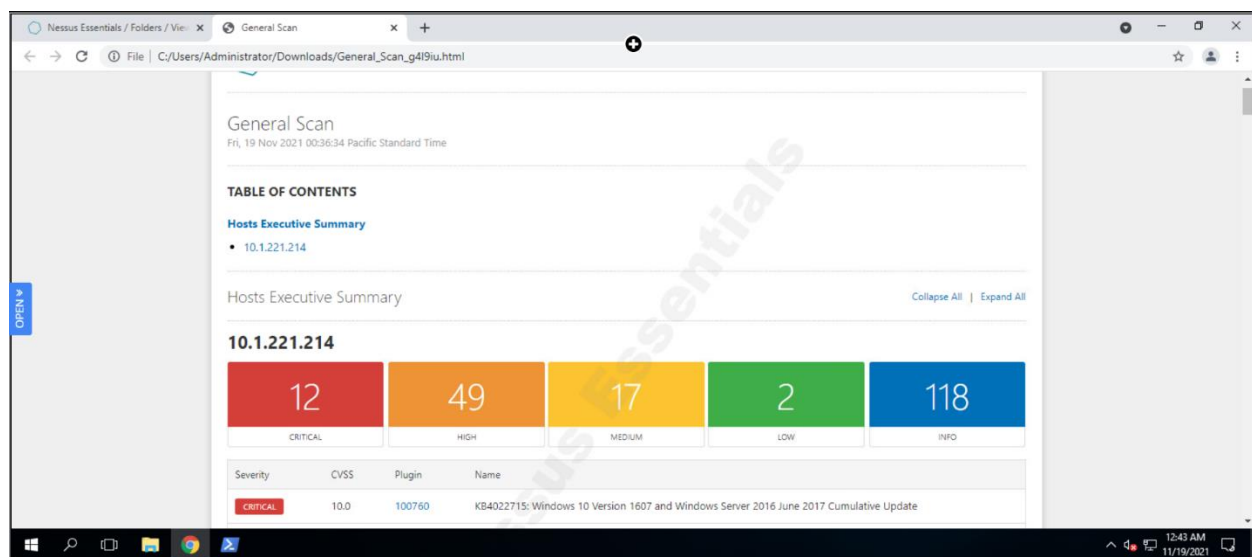


Figure 1: Sample Nessus Scan Report

Table 1: Description of Severity Categories

Severity	CVSSv2 Range	CVSSv3 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.	The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.	The plugin's highest vulnerability CVSSv3 score is between 7.0 and 8.9.
Medium	The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.	The plugin's highest vulnerability CVSSv3 score is between 4.0 and 6.9.
Low	The plugin's highest vulnerability CVSSv2 score is between 0.1 and 3.9.	The plugin's highest vulnerability CVSSv3 score is between 0.1 and 3.9.
Info	The plugin's highest vulnerability CVSSv2 score is 0.	The plugin's highest vulnerability CVSSv3 score is 0.
	- or -	- or -
	The plugin does not search for vulnerabilities.	The plugin does not search for vulnerabilities.

Albeit the results are easily read and well organized, it is not recommended to distribute to management without interpretation. As stated above, the immediate information available is minimal, only consisting of the CVSS value, name of the vulnerability, and the severity level that Nessus have assigned. Without an analysis, some dangerous vulnerabilities may be overlooked. For example, the MS17-010 vulnerability on 192.168.1.10 is labeled as High Severity but may be underestimated due to comparison with the Critical vulnerabilities found on 92.168.1.30 [7]. The Nessus report includes a link to a second webpage, or “plugin,” that provides more detailed information on the vulnerability, including possible mediation, background information, and multiple references. These plugin links offer a great deal of information that an analyst can use to interpret and summarize the results for distribution to management.

The first vulnerability that needs to be addressed is the MS17-010 vulnerability [8] on 192.168.1.10. According to Microsoft, the MS17-010 or “EternalBlue” exploit was created by the National Security Agency (NSA) as part of a program to stockpile and weaponize cybersecurity vulnerabilities [9]. Unfortunately, after a successful attack, the exploit was leaked to a group called Shadow Brokers. Microsoft was able to release two separate patches in an attempt to protect users from this vulnerability. However, in May 2017, the EternalBlue exploit was used in the WannaCry ransomware attack that infected over 230,000 Windows systems in a single day, causing an estimated \$4 billion in damages. A second attack called NotPetya caused an estimated \$10 billion in damages. Companies in the transportation industry were hit hard because of the EternalBlue exploit, including the world’s largest shipping firm Maersk and FedEx [9].

Another vulnerability that needs to be addressed is the backdoor [10] on 192.168.1.30. This backdoor allows a remote host to access the computer without authentication. If this vulnerability is left unchecked, a threat actor may access the system and run arbitrary code, leading to viruses, malware, theft, ransom of data, and much more.

The third issue that should be addressed is the Server Message Block (SMB) signing vulnerability [11]. Even though Nessus categorizes this vulnerability as a medium hazard, it is present on every machine on Mercury USA’s network. Thus, allowing for a larger attack surface which increases the possibility of being exploited. The vulnerability will allow an unauthenticated, remote user to perform a man-in-the-middle (MITM) attack [12] on Mercury USA’s servers. A MITM attack is a general term for when a threat actor positions themselves between two endpoints, usually a user and an application. The threat actor can eavesdrop or impersonate either party, leading to the possible theft of sensitive information, including login information, payment information, and personal information.

Part 2: The Business Case

Overall, Mercury USA's current security posture is not terrible. Once the three vulnerabilities mentioned above are fixed, 192.168.1.10 and 192.168.1.100 will have addressed the most severe threats and create a minimal attack surface. 192.168.1.25 has a remaining high severity vulnerability that is also SMB related and can be fixed simultaneously as the signing vulnerability. Mercury USA's most significant issue is 192.168.1.30. Even with correcting the backdoor and SMB issues, there are still many critical, high, and medium-level vulnerabilities. Many of these are Secure Sockets Layer (SSL) [13] and Secure Shell (SSH) [14] vulnerabilities. However, fixing the SSL and SSH vulnerabilities will correct most issues on 192.168.30, and 192.168.1.25 will have a minimal attack surface. Securing the numerous SSL vulnerabilities will also help secure customer information since SSL is commonly used for credit card transactions, data transfers, and logins. Also, correcting the SSH vulnerabilities will help secure the network by ensuring remote machines used by employees will not be compromised while connecting to company servers.

Based on the vulnerabilities found by Nessus, I believe that there are two that an adversary or black hat hackers will use. Both backdoor on 192.168.1.30 and the MS17-010 vulnerability on 192.168.1.10 will allow a threat actor to execute code to their advantage, gaining access to sensitive business and personal information. The backdoor can be exploited at any time by whoever left it there if they have not already. If found by a threat actor, this vulnerability will allow for easy, possibly unrestricted access to Mercury USA's network. Despite being a few years old, the MS17-010 exploit is still heavily in use, making this a likely exploit; Avast reports that in May of 2019, hundreds of thousands of EternalBlue attacks were blocked, and in June 2020, over 20 million EternalBlue attacks were blocked [9].

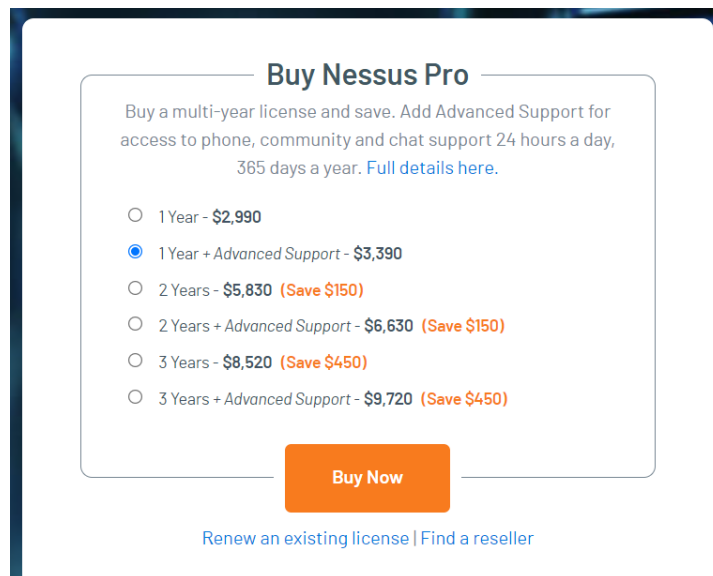
Part 3: Nessus Purchase Recommendation

After analyzing the Nessus report, I recommend that Mercury USA purchases Nessus. Nessus is not only highly reputable and one of the best-known vulnerability scanners on the market, but it also scans for a significant amount of CVEs. As mentioned above, the scan results are also very well organized with a color-coded scheme and a reasonable severity level based on CVSS scores, allowing an analyst to get a basic understanding of the network's security posture at a glance. Nessus also produces a link for more information, providing background information, solutions, and references to any found vulnerabilities.

Unfortunately, I do not think that the results provided by Nessus are suitable for management. Although an analyst may gather much information from the results, I recommend providing a summary, or interpretation, of the scan results to management instead of the results themselves. Analysis of the scan results, no matter how organized and easy to read, will still take time to adequately gather information and solutions on the vulnerabilities found, which is where the cybersecurity analyst comes in.

Even though the cost seems expensive at first, starting at \$2,990 a year [1] with options for up to three years as seen in Figure 2, Nessus is worth it. Nessus is reliable, easy to use, and has 24/7

support with updates weekly. There is also an advanced support line and training opportunities for Mercury USA employees with an upgrade fee.



Buy Nessus Pro

Buy a multi-year license and save. Add Advanced Support for access to phone, community and chat support 24 hours a day, 365 days a year. [Full details here.](#)

- ☐ 1 Year - \$2,990
- ☒ 1 Year + Advanced Support - \$3,390
- ☐ 2 Years - \$5,830 (Save \$150)
- ☐ 2 Years + Advanced Support - \$6,630 (Save \$150)
- ☐ 3 Years - \$8,520 (Save \$450)
- ☐ 3 Years + Advanced Support - \$9,720 (Save \$450)

[Buy Now](#)

[Renew an existing license](#) | [Find a reseller](#)

Figure 2: Nessus Pricing Scheme [1]

Utilizing Nessus will also allow Mercury USA to comply with regulations and standards. Two regulatory and compliance standards that Nessus will help comply with are the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Information Systems and Organizations and Payment Card Industry Data Security Standards (PCI DSS) [15]. As a small to medium-sized transportation business, Mercury USA does business across state lines; as such, being compliant with federal standards, like those from NIST, will only be beneficial in the long run. Mercury USA also conducts business using payment systems like credit cards and uses other cardholder data. Since this is the case, Mercury USA will need to comply with PCI DSS standards, which includes having a process to identify and assign risk to discovered vulnerabilities, a requirement Nessus may fulfill.

Conclusion

In conclusion, Nessus is exceptional as far as vulnerability scanners are concerned. Nessus scans for large numbers of CVEs with easy-to-read results and provides resources for understanding vulnerabilities and their solutions. Security analysts can quickly consolidate the information in the scan results to summarize findings for management. With these findings, Nessus allows Mercury USA to minimize the attack surface of their network, providing security to personal, business, and client data. Mercury USA also benefits from regulatory compliance, including NIST and PCI DSS, by bringing Nessus into their cybersecurity toolbox. Finally, securing the vulnerabilities that Nessus discovers will help keep an incident, like the recent ransomware attack on our rival company, from happening to Mercury USA, helping build confidence among our customers and a positive reputation in the transportation industry. Overall, the benefits of purchasing Nessus will dramatically outweigh the cost.

References

- [1] Tenable, "Nessus," Tenable, 2021. [Online]. Available: <https://www.tenable.com/products/nessus>. [Accessed 8 November 2021].
- [2] The MITRE Corporation, "Frequently Asked Questions," U.S.. Department of Homeland Security Cybersecurity and Infrastructure Security Agency , 2021. [Online]. Available: <https://www.cve.org/ResourcesSupport/FAQs>. [Accessed 19 November 2021].
- [3] Greenbone Networks, "OpenVAS – Open Vulnerability Assessment Scanner," 2 August 2021. [Online]. Available: <https://www.openvas.org/index.html>. [Accessed 6 September 2021].
- [4] J. Hoffman, "OpenVAS vs. Nessus: How Different are the Two?," Wisdom Plexus, 13 May 2020. [Online]. Available: <https://wisdomplexus.com/blogs/openvas-vs-nessus/>. [Accessed 19 November 2021].
- [5] Nessus, "CVSS vs. VPR," Tenable, 2021. [Online]. Available: <https://docs.tenable.com/tenableio/Content/Analysis/RiskMetrics.htm>. [Accessed 19 November 2021].
- [6] National Institute of Standards and Technology, "Vulnerability Metrics," National Vulnerability Database, 2021. [Online]. Available: <https://nvd.nist.gov/vuln-metrics/cvss>. [Accessed 19 November 2021].
- [7] Nessus, "Mercury USA's Nessus Scan Report," Nessus, 8 April 2020. [Online]. Available: [https://learn.umgc.edu/content/enforced/617704-027858-01-2218-OL3-7380/My_Basic_Network_Scan_qw3e2d%20\(2\).html](https://learn.umgc.edu/content/enforced/617704-027858-01-2218-OL3-7380/My_Basic_Network_Scan_qw3e2d%20(2).html). [Accessed 19 November 2021].
- [8] Nessus, "MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)," Tenable, 15 October 2020. [Online]. Available: <https://www.tenable.com/plugins/nessus/97833>. [Accessed 19 November 2021].
- [9] C. Burdova, "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?," Avast, 1 October 2021. [Online]. Available: <https://www.avast.com/c-eternalblue#gref>. [Accessed 19 November 2021].
- [10] Nessus, "Bind Shell Backdoor Detection," Tenable, 10 May 2019. [Online]. Available: <https://www.tenable.com/plugins/nessus/51988>. [Accessed 19 November 2021].
- [11] Nessus, "SMB Signing not required," Tenable, 15 March 2021. [Online]. Available: <https://www.tenable.com/plugins/nessus/57608>. [Accessed 19 November 2021].

- [12] Imperva, "Man in the middle (MITM) attack," Imperva, 2021. [Online]. Available: <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>. [Accessed 19 November 2021].
- [13] GlobalSign, "What is an SSL Certificate?," GMO, 2021. [Online]. Available: <https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate>. [Accessed 19 November 2021].
- [14] University College London, "What is SSH and how do I use it?," University College London, 2021. [Online]. Available: <https://www.ucl.ac.uk/isd/what-ssh-and-how-do-i-use-it>. [Accessed 19 November 2021].
- [15] R. Oerby, "5 Compliance Regulations and Their Impacts on Mainframe Vulnerability Scanning," KRI Security, 9 September 2020. [Online]. Available: <https://www.krisecurity.com/compliance-regulations-mainframe-vulnerability-scanning/>. [Accessed 19 November 2021].