VM Scanner Background Report

**Rudy Zimmerman**

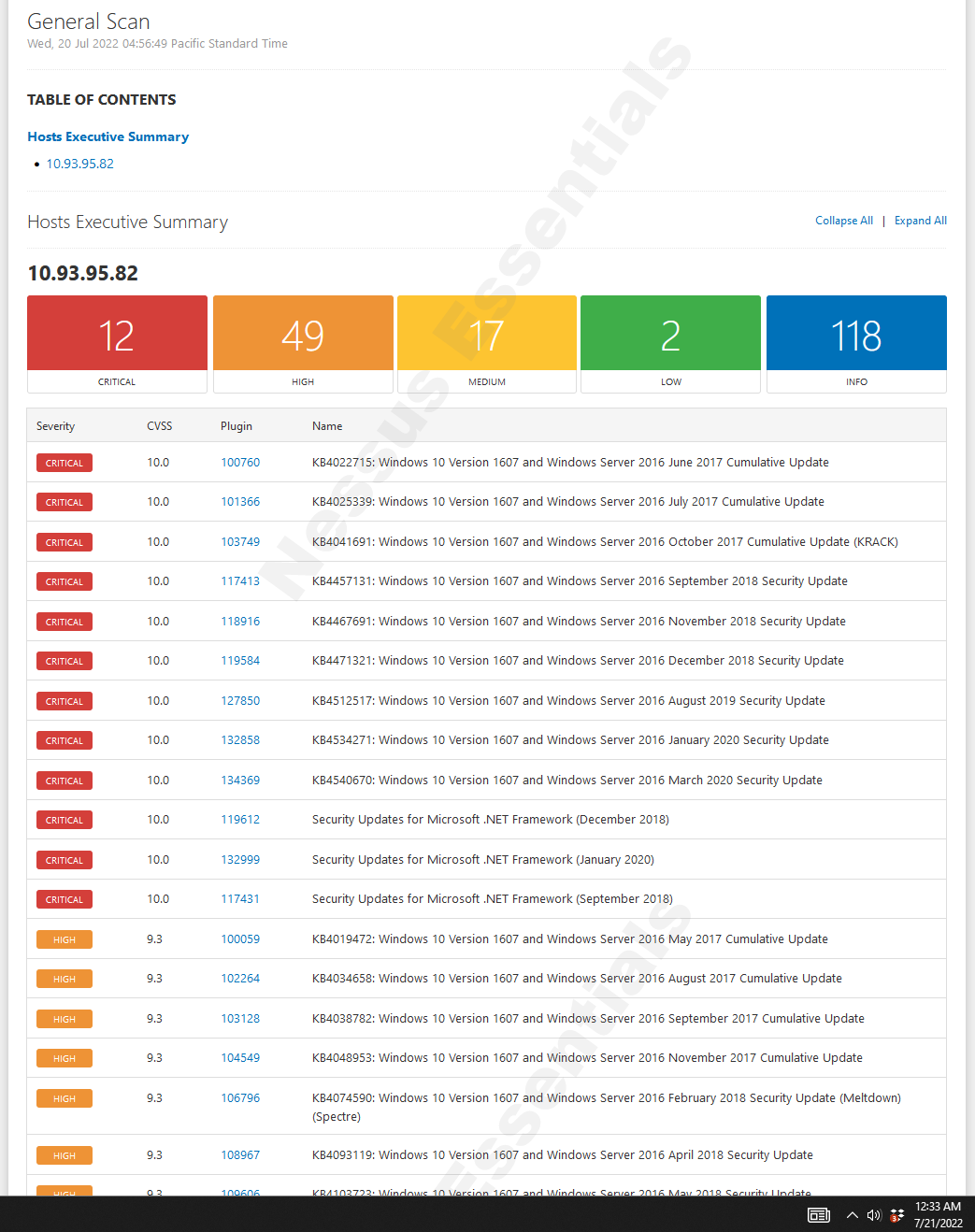
CMIT 421 *<Section #6980>* Threat Management and Vulnerability Assessment

**7/15/2022**

# Introduction

As part of the assessment of Mercury USA’s security posture, I have reviewed a report generated by Nessus using our free trial license. A basic credentialed vulnerability scan was conducted on our machine located at 10.93.95.82. Below, I will discuss the full contents of the Nessus report, including the vulnerabilities found and the solutions proposed by the Nessus database. My discussion will focus on Nessus’s suitability to aid in Mercury USA’s protection of user and company data, with special consideration paid to the CEO’s worries about ransomware attacks against companies in the transportation sector. I have included my final recommendation on whether or not I think Mercury USA should purchase Nessus at this time after the analysis and discussion of Nessus’s potential applications to our business.

# Part 1: Nessus Vulnerability Report Analysis

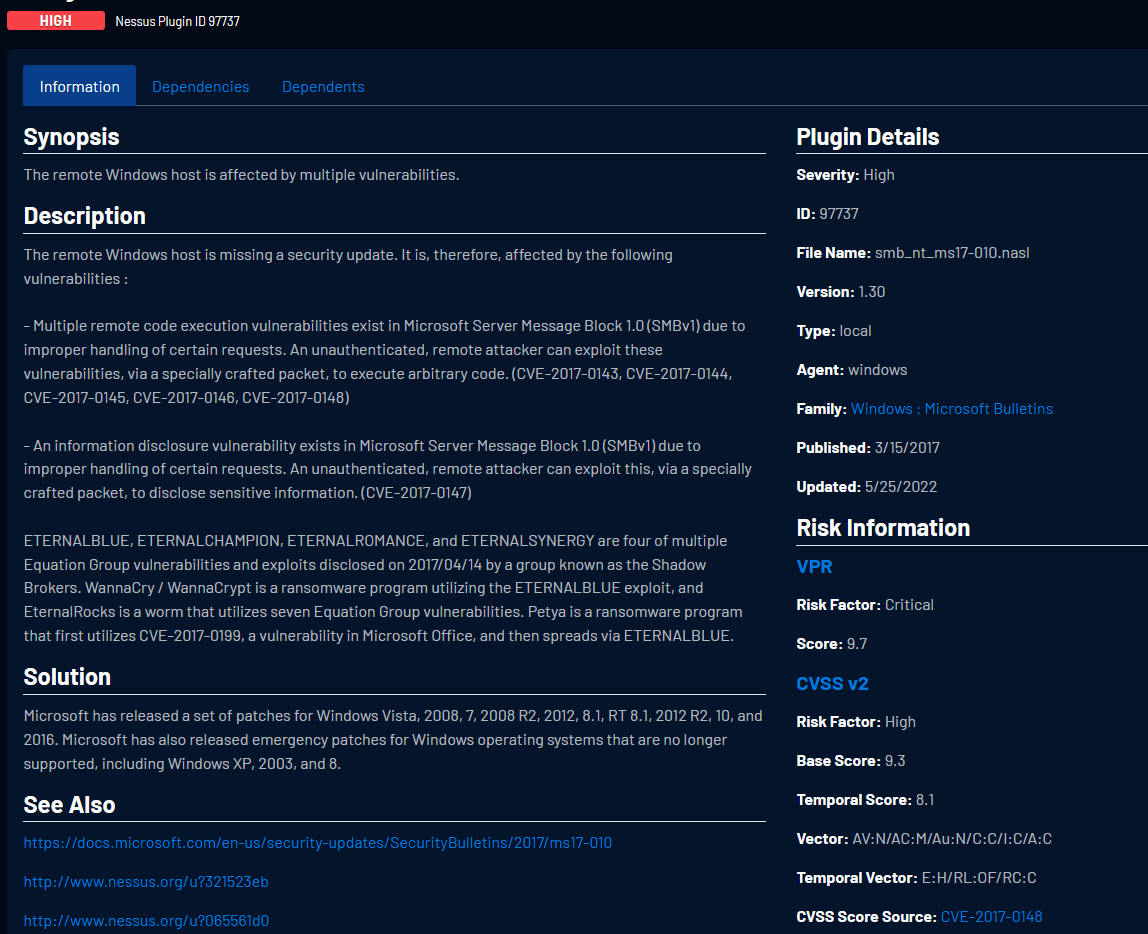


Screenshot 1 – Nessus Report Example

Overall, I find the Nessus report to be very easy to interpret. I like that it is organized into a high-level easy to read report that offers links to pages for further reading on detected vulnerabilities. The executive summary is color-coded, showing critical and high vulnerabilities in orange and red, respectively, and sorts vulnerabilities in order of severity according to their Common Vulnerability Scoring System (CVSS) score. I find that the reports and linked resources give enough detail to form a remediation plan but do not provide so much detail that an analyst would get confused or waste valuable time trying to pick out the most meaningful information. However, analyst interpretation should still be attached to the Nessus report before sending it to management. While IT and security specialists can easily make sense of a Nessus report, there is a lot of information to digest, and it is best to break down the main causes of concern for any managers that may not have experience in security. The “name” field of the executive summary shows labels descriptive enough for an analyst to identify specific vulnerabilities. The most relevant example is the vulnerability to ransomware found on the scanned machine. Knowing that ransomware is a primary concern of the CEO, I could use the search tool to scan this report for “EternalBlue” or “WannaCry” (popular ransomware exploit and software) for example, and immediately verify the existence of this vulnerability on our machine, then have quick access to recommended remediation steps by clicking the hyperlink in the “Plugin” column. The detailed vulnerability view also provides useful information such as the date the vulnerability was published, and the CVSS vector string, which shows information about how the vulnerability can be exploited and which aspects of the CIA triad could be affected. While this EternalBlue vulnerability is officially given a CVSS score in the “high” range, I would consider it a critical vulnerability for Mercury USA given the current threat landscape.



Screenshot 2 – EternalBlue Vulnerability Discovered



Screenshot 3 – Nessus Detailed Vulnerability View (Plugin #97737)

With just a quick glance at the detection breakdown at the top of the executive summary, it is plain to see that there are many more worrisome vulnerabilities present on the machine. Two more detections I’d like to discuss that are officially in the “critical” risk range involve the lack of necessary security updates, with plugin ID numbers 100760 and 119612. Plugin ID #100760 is the detection of missing security update KB4022715 and plugin #119612 concerns a missing security update to the Microsoft .NET Framework, which is a software development framework for building and running applications on Windows. Each of these plugins actually represents a bundle of vulnerabilities that pose a high risk to every aspect of the CIA triad and can be exploited with network access via a low-complexity attack, which is all shown on their respective Nessus plugin pages. Furthermore, these bundles include vulnerabilities to remote command execution which could possibly lead to ransomware attacks [4], just like the SMB/EternalBlue vulnerability detection mentioned above. The presence of so many vulnerabilities on this machine indicates the need to isolate the machine immediately, if possible, so that important security updates can be installed. Every minute that the machine is left in this vulnerable state increases the risk of infection to neighboring network devices and compromise to business and client data. Furthermore, staff should receive instructions and training to be extra vigilant against possible social engineering attacks while we work to strengthen our security posture. Going forward, we should observe a rigorous update schedule, automate vulnerability scans, and be sure that our network is properly segmented to prevent Mercury USA’s network from falling into such a vulnerable state as the current one.

# Part 2: The Business Case

After reviewing the Nessus report, I can easily say that Mercury USA’s security posture is very weak. There are multiple vulnerabilities that would allow easily exploitable attack vectors for a remote attacker to gain access to system data and possibly compromise multiple systems within the network. This is evidenced by the 12 critical and 49 high risk vulnerabilities highlighted on the Nessus report. The information that is at risk here includes business, employee, and customer data such as proprietary information, route/schedule information, personal identifiable information (PII), and credit card data. The compromise of these kinds of data could damage the operability and the reputation of Mercury USA, as well as subject the company to fines and lawsuits. It is imperative that the security posture be strengthened immediately and brought into compliance with applicable standards such as PCI DSS, which we are required by law to meet as long as we accept credit card payments [2].   
 As the CEO’s main concern is ransomware, the priority of the IT department should be to address Mercury’s current vulnerability to such attacks. A hacker looking to install ransomware would most likely target the 192.168.1.10 machine with vulnerability ID #97833. This vulnerability lies within the Microsoft SMBv1 and allows for remote code execution via exploits such as EternalBlue. EternalBlue is the exploit used by the WannaCry ransomware, which infected over 300,000 machines in 2017, when it was first deployed [3]. Fortunately, Nessus did not detect an end-of-life OS running on this machine, so the recommended solution of applying official Microsoft patches should be simple and fast.

# Part 3: Nessus Purchase Recommendation

It is clear that Nessus was able to generate a report that highlights the existence of multiple vulnerabilities across a number of machines across our network, and even takes the added step of providing us with potential paths toward remediation. The high-level report clearly highlights the most critical vulnerabilities and provides a simple description of all vulnerabilities, making for a great general overview to be presented to non-technical management alongside a brief interpretation. The detailed view of each vulnerability provides all of the statistics and information that a security analyst would require in the process of remediation. Nessus has options for customizability in scan types, scope definition, and scan scheduling. This product offers a service that is exceedingly capable of improving the security posture at Mercury USA and bringing us into compliance with standards such as PCI DSS and would be a fantastic addition to our cybersecurity toolbox. It may be surprising, then, that my recommendation is that Mercury USA does not purchase Nessus just yet.  
 My recommendation against the purchase of Nessus comes down to the cost. The subscription to Nessus Professional costs $3,390 per year. It has been made clear to me via correspondence with IT manager Judy McNamara that this is considered expensive for Mercury USA. Because there are free vulnerability scanners that are also very good, such as OpenVAS (covered in the memo I sent out on July 5th), I would consider the purchase of a paid scanner to be low priority. If the IT budget is truly limited, it would be better spent making upgrades in other areas such as back-up servers, off-site data storage, employee training, firewalls, and/or intruder prevention systems. Based on what I have seen at Mercury USA so far, I suspect that controls such as these are outdated or missing completely.

Conclusion  
  
 To summarize, Nessus provided a report that is organized in a way that provides an understandable overview of vulnerabilities present on machines across the network, while also giving the option to dig deeper into found vulnerabilities to give analysts and technicians a more detailed view of threats and how to mitigate them. The report exposed vulnerabilities present on our network, showing the data of Mercury USA and its customers to be at high risk of compromise. Particularly noteworthy, due to our CEO’s specific worries, is the discovered vulnerability to the EternalBlue SMB exploit, meaning that our network is currently vulnerable to popular ransomware attacks. The patching of this vulnerability, recommended by Nessus, should be initiated immediately.  
 In spite of the helpful information provided to us by the Nessus report, it is my recommendation that we hold off on subscribing to the Nessus Professional service at this time. Because of the cost, it is in Mercury USA’s best interest to spend our IT budget on other defensive controls for our organization. This report should be saved and referred to in the future, when we can re-evaluate our budget, and the timing may be better to add Nessus Professional to our toolbox.

# References

[1] "Chapter 5: Implementing an Information Security Vulnerability Management Process", Pearson CompTIA Cybersecurity Analyst (CySA+), 2020. [Online]. Available: <https://www.ucertify.com/>. [Accessed: 28-Apr-2020].  
  
[2] “PCI Compliance Guide Frequently Asked Questions | PCI DSS FAQs,” *PCI Compliance Guide*, 2016. https://www.pcicomplianceguide.org/faq/  
  
[3] H. Landi, “Report: 40% of healthcare organizations hit by WannaCry in past 6 months,” *Fierce Healthcare*, May 29, 2019. https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months (accessed Jul. 20, 2022).

[4]“What is Remote Code Execution (RCE)?,” *Check Point Software*. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-remote-code-execution-rce/

‌

‌