MEMO

November 9, 2021

Micah Martinez; CMIT 421 7380

To the Cybersecurity Manager:

Overview

Recently in the transportation sector, there has been an increase in ransomware attacks. To reduce the likelihood of a successful attack on Mercury USA, I propose implementing a vulnerability management (VM) process. The process has already begun, and by using the OpenVAS results from the penetration test, we can secure the high severity vulnerability found. Furthermore, a VM process will allow Mercury USA to constantly assess and enhance its security posture to mitigate the most dangerous vulnerabilities using a VM process.

Part 1: Vulnerability Management (VM) Process Recommendation

I recommend the VM process found in the Transportation Systems Sector (TSS) Cybersecurity Framework Implementation Guidance and its companion workbook [1]. The three main elements in this VM process are: determining risk profile, establishing priorities, and implementing solutions. Determining the risk profile involves finding internal and external threats, which can be done with third-party penetration tests and vulnerability scans. The desired outcome is for your organization to be aware of possible vulnerabilities and know how much risk you are willing to assume. Establishing priorities is broken down into three categories: highest risk first, disruption to business operations, and lowest risk/easy wins. Finally, implementing solutions involves testing and applying or postponing fixes.

To scan the system for vulnerabilities, I recommend using at least two scanning tools, and these can be a combination of open-source software, like Nmap [2] and OpenVAS [3], or commercial software, like Nessus [4]. In addition, there is a list of scanners compiled by the Open Web Application Security Project (OWASP) on the web [5]. The scanning frequency depends on a few factors, including acceptable risk levels, regulatory requirements, technical and business constraints, and licensing limitations. However, at minimum, I would recommend scanning after any software and hardware changes and at least twice a month.

Once a scan is complete, the report from the scanner will be reviewed by a cybersecurity analyst. After review, the analyst will create a summary of the results and recommend fixes or actions.

Part 2: Vulnerability Scanning Tool Evaluation and Recommendations

The scanner used to create this report is called OpenVAS. OpenVAS is an open-source vulnerability assessment tool that is widely used in the cybersecurity community [6]. One of the best advantages of using OpenVAS is that it is free while still providing quality output that can assist vulnerability analysts in finding and correcting common vulnerabilities. The scan results include references for more information about the vulnerability, including the Common Vulnerabilities and Exposures (CVE) reference number, how the impact can impact your system, possible fixes, and more. However, OpenVAS covers fewer CVE vulnerabilities than some commercial scanners, lacks policy management tools, and has limited compatibility with operating systems (OS) [7].

The scan results do a decent job at going over how to mitigate most risks, but some vulnerabilities, like the end-of-life vulnerabilities, do not have much detail on how to fix those risks. In addition, although these reports are great for someone who understands what they represent, they are not suitable for those without technical knowledge. Therefore, it would be best not to automatically distribute or hand these reports directly to management without someone first summarizing the results to make them more understandable.

Even though OpenVAS is not perfect, I recommend the Mercury USA uses it as an initial scan. Having an OpenVAS report is a great starting place to expose and secure high severity vulnerabilities.

Part 3: Business Case Example

If Mercury USA does not implement a VM process, they could lose control of their system and even allow customer information to be distributed to the public. For example, an attacker exploiting the Windows SMB Server vulnerabilities [8] [9] that the OpenVAS scan discovered on our systems. These vulnerabilities, if exploited, will allow a hacker to execute commands on our system remotely, leading to many unfortunate events, including uploaded viruses/malware or the download, encryption, and ransom of sensitive or critical information and systems.

Implementing the VM process above will allow Mercury USA to find severe vulnerabilities, prioritize them by severity, and apply the proper fix. In addition, using this process in a cycle will create a more robust security posture, building trust between Mercury USA and our customers.

Unfortunately, I do not believe that relying solely on OpenVAS will be sufficient. Although OpenVAS is a great scanner, it will not catch every vulnerability, and it is best practice to multiple scanners to find as many issues as possible.

Closing

After the recent cyber attacks against the transportation sector and our rival company, we must begin taking steps to protect ourselves and our customers. The best way to accomplish this is to implement a VM process to understand our security posture better. Mercury USA is off to a good start; the process of determining our risk profile has already begun with the third-party penetration test and the OpenVAS scan. However, the OpenVAS scan is not enough, and by using multiple scanners, Mercury USA will discover vulnerabilities previous scanners did not.

Additionally, securing our systems and data is not a one-time process; the cybersecurity world is constantly changing, with new vulnerabilities discovered daily. Using a VM process will ensure that Mercury USA stays ahead of the curve and attacks on our system stay to a minimum.

Respectfully,

Micah Martinez
Cybersecurity Threat Analyst
Mercury USA

References

[1] Cybersecurity & Infrastructure Security Agency, "Transportation Systems Sector Cybersecurity Framework Implementation Guide," Cybersecurity & Infrastructure Security Agency, 2021. [Online]. Available: https://www.cisa.gov/publication/tss-cybersecurity-framework-implementation-guide. [Accessed 8 November 2021].

[2] G. Lyon, "Nmap Free Security Scanner," 7 August 2021. [Online]. Available: https://nmap.org/. [Accessed 6 September 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] Tenable, "Nessus," Tenable, 2021. [Online]. Available: https://www.tenable.com/products/nessus. [Accessed 8 November 2021].

[5] OWASP, "Vulnerability Scanning Tools," OWASP, 2021. [Online]. Available: https://owasp.org/www-community/Vulnerability_Scanning_Tools#. [Accessed 8 November 2021].

[6] Breach Lock, "Top 5 open-source tools for network vulnerability scanning," Breach Lock, 25 March 2021. [Online]. Available: https://www.breachlock.com/top-5-open-source-tools-for-network-vulnerability-scanning/. [Accessed 8 November 2021].

[7] Tamil Hacker, "Nessus VS OpenVAS Advantages and Disadvantages Explained," The Tamil Hackers, 1 January 2021. [Online]. Available: https://thetamilhackers.blogspot.com/2021/01/nessus-

vs-openvas-advantages-and.html. [Accessed 7 November 2021].

[8] Trend Micro, "MS17-010-SMB_REMOTE_CODE_EXECUTION_EXPLOIT appears on the Suspicious Connection logs," Trend Micro, 6 April 2020. [Online]. Available: https://success.trendmicro.com/solution/1121399-ms17-010-smb-remote-code-execution-exploit-appears-on-the-suspicious-connection-logs. [Accessed 8 November 2021].

[9] Microsoft, "Microsoft Security Bulletin MS17-010 - Critical," Microsoft, 3 September 2020. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. [Accessed 8 November 2021].