JEEMECS (Journal of Electrical Engineering, Mechatronic and Computer Science ISSN 2614-4859
Vol. 6, No. 1, February 2023, pp. xx-xx

Attack in to The Server Message Block (CVE-2020-0796) Vulnerabilities in Windows 10 using Metasploit Framework

M. Faturrohman [a,1,*], Angelita Salsabila [b,2], Zulma Mardiah [b,3], Aqwam Rosadi Kardian [b,4]

[a] Politeknik Siber dan Sandi Negara, Jl. H. Usa, Ciseeng, Kabupaten Bogor, West Java 16120, Indonesia
[b] Sekolah Tinggi Manajemen Informatika dan Komputer Jakarta STI&K, Jl. Bri Radio Dalam No.17, Kebayoran Baru, South Jakarta, Jakarta 12140, Indonesia
[1] faturrohmansugiyarto@gmail.com [*]; [2] angelitasalsabilaaf@gmail.com; [3] zulmam627@gmail.com;
[4] aqwam@staff.jak-stik.ac.id
[*] corresponding author

Keywords
Server Message-Block
Operation System
Framework
Metasploit
CVE 2020-0796

ABSTRACT

Advances in information and communication technology encourage the development of operating systems. Windows 10 is one of the most widely used operating systems today. Unfortunately, there are still many who do not know that in the Windows 10 system there are several system vulnerabilities and some bugs. One example is the vulnerability in Server Message Block (SMB) on Windows 10 (CVE-2020-0796). This vulnerability exploits the Buffer Overflow method on one of the Execution Server Message Block (SMB) files. The impact of this attack is that the attacker can perform Remote Control Access on the target device. One of the reasons why this attack can occur is an operating system that has never been updated or uses an old operating system that has lots of bugs. The automatic updating feature is actually very helpful in overcoming this problem. However, there are still many device users who understand the importance of this. This research will explain how the process of attacking the Windows 10 operating system uses the CVE-2020-0796 vulnerability. The hope is that after understanding the readers can know the importance of using the latest version of the operating system and immediately updating the system.

1. Introduction

The Windows operating system is one of the most popular operating systems in the computer world. Almost every place where there is a computer using the Windows operating system [1]. This is because the Windows operating system has a control system and user interface that is easy for users of all circles to use. The large number of users of the windows operating system causes many hackers to try to attack the windows operating system.

Hackers try to carry out attacks on the Windows operating system for personal gain, starting from carrying out attacks with malware, Denial of Service (DOS), Man in the Middle, and Remote Control Execution (RCE). The main goal of hackers is to take over servers or access rights of computer systems. After that, hackers can exploit data and information owned by the target.

CVE-2020-0796 is a type of vulnerability found in the Windows 10 version 1903-1909 operating system [2]. This vulnerability is a vulnerability to a buffer overflow attack on Microsoft SMB servers [2]. The danger of this attack is that hackers can take over the access rights of the target operating system.

This indicates an attack attempt to exploit a buffer overflow vulnerability in Microsoft SMB servers. The vulnerability is due to an error when the vulnerable software handles a maliciously crafted compressed data packet. A remote, unauthenticated attacker can exploit this to execute arbitrary code within the context of the application.

2. The Proposed Method

2.1. Metasploit Framework

Metasploit Framework is a development platform for creating security tools and exploits. This framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers worldwide.

Metasploit Framework has many modules to carry out various types of attacks against various types of devices and servers. From the Valea and Oprisa experiment, the results showed that the proposed framework is able so solve precisely the machines with common vulnerabilities and public exploits [3]. The main modules are: (1) exploit module, which is a module for carrying out certain attacks, (2) payload module, which is a module for interacting with targets to obtain information and data (3) auxiliary module for scanning targets, and (4) encoder module, which is a module for avoiding antivirus and firewalls.

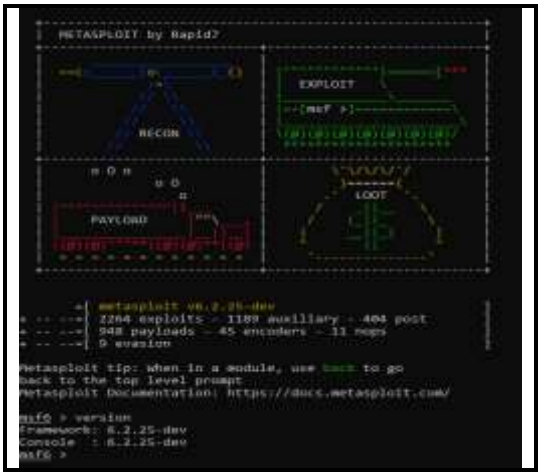

Fig. 1. Metasploit framework version 6.2.25-dev

Metasploit Framework may be a standard penetration testing platform that permits hackers to write down and execute exploit code [4]. Penetration Testing is an activity to simulate attacks that can be carried out against certain network organizations or companies to find weaknesses in the network system. In penetration testing there are 6 phases, namely: (1) information gathering, (2) vulnerabilities analysis, (3) vulnerabilities exploitation, (4) post exploitation and (5) report generation. Each phase is reviewed using automated tools and exploits of Metasploit [5].

2.2. CVE 2020-0796

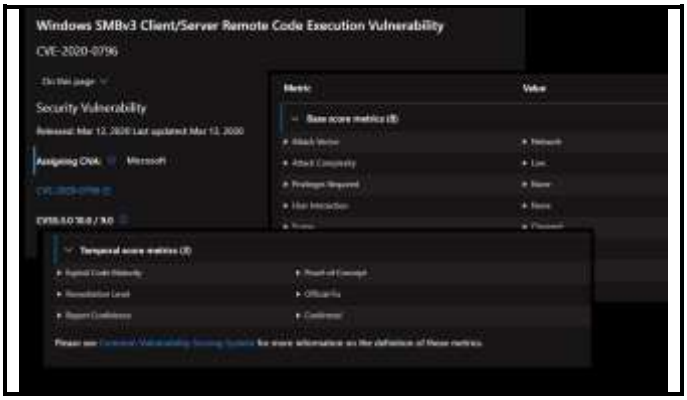

Fig. 2. CVE-2020-0796 on msrc.microsoft.com vulnerability

CVE 2020-0796 is a pre-remote code execution vulnerability that resides in the Server Message Block 3.0 (SMBv3) network communication protocol that handles certain requests. This vulnerability can be resolved by disabling SMBv3 compression and blocking TCP port 445 on firewalls and client computers as a workaround.

2.3. Operating System

The operating system is software in the first stage that is entered into the computer's memory which can carry out the task of controlling and managing hardware as well as other basic operating systems and can also run application programs. The function of the operating system is to boot, process management, memory management, data security, device control, and user interface design. Examples of modern operating systems are Android, iOS, Mac OS X, Microsoft Windows and Linux.

The Windows 10 Operating System has been available to the general public since July 2015. The Windows 10 upgrade planning process at Lehigh has been in progress for a very short period of time [6]. Windows 10 offers six different versions, each designed to fill specific computing needs there are: (1) home, (2) professional, (3) enterprise (4) education, (5) mobile, and (6) mobile enterprise[6]. Windows 10 have interesting feature about the security system. The feature name is Forces Updates that have description, users will no longer have the option to postpone or avoid critical patches and updates [1].

2.4. Server Message Block (SMB)

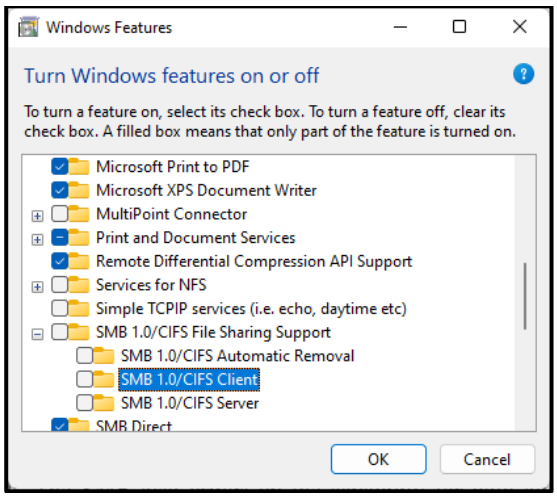

Fig. 3. SMB Feature on Windows 10

The first known development of the SMB protocol was developed by Barry Feigenbaum at IBM in early 1983. The Server Message Block Protocol (SMB) is a client-server communication protocol employed in sharing access to files, printers, serial ports and different assets on a system [6]. Server message block which runs over TCP port 445, is a network protocol that has been designed to enable file sharing, network browsing, printing services, and inter process communication over a network. The SMB also brings up the capability for both clients able to connect to each other without any server in between of it. The SMB protocol transmits multiple messages between a client and a server to establish a connection [6].

2.5. Buffer Overflow

Buffer overflow is a condition in which a data storage area is overloaded. Buffer overflow is used by hackers to exploit a computer application system. This attack is called an input validation attack, where the hacker will input data that exceeds the storage capacity of an application, causing the system to crash or buffer overflow [7].

Buffer overflow vulnerabilities are caused when a program puts data into a buffer but forgets to check the buffer boundary [7]. The easiest method to buffer overflow a program is just give the bunch of input until overloaded. A buffer overflow attack uses one or multiple network packets to overrun a buffer in the victim program and eventually overwrite the target address of some indirect branch instruction [8]. This makes the attacker maybe can gain some reverse shell from the bugs. A reverse shell is a shell, which is initiated by the target machine back to the attacker's machine that will pick up the shell by listening on the particular port [9]. And after getting reverse shell attacker gain full access of system.

There are four basic approaches to defending against buffer overflow vulnerabilities and attacks. The things that are meant are: (1) brute force method, (2) operating systems approach method, (3) direct compiler approach method, and (4) indirect compiler approach method [10].

3. Method

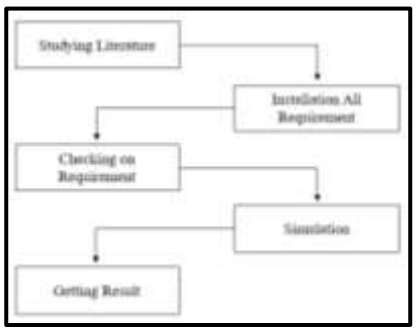

Fig. 4. Framework Research

The study simulated a buffer overflow attack against the CVE-2020-0796 vulnerability in Windows 10 version 1903. The simulation used a computer with the Windows 11 version 21H2 operating system. The target is an operating system that is run using a virtual machine with the VMware Workstation 17 Player community edition application. The target virtual machine specifications are: (1) 2 GB RAM, (2) 2 core processors, and (3) 60 GB hard disk.

The attack simulation was carried out using the Windows 11 operating system using Windows Server Linux (WSL) to run the Metasploit Framework. The computer specifications used are: (1) 16GB RAM, (2) 8 core processors, and (3) 512GB hard disk.

The target operating system is run in host-only mode for network adapter settings so that attackers can carry out attacks on targets. The tools used in the attack are the Metasploit Framework version 6.2.25-dev.

4. Results and Discussion

Vulnerabilities on Microsoft Server Message Block (SMB) make the attacker gain the ability to execute code on the target server client. CVE-2020-0796 caused by a lack of bounds which is directly passed to several subroutines. Passing a large value causes buffer overflow, and crashing the kernel.

This attack attacks the Windows 10 operating system versions 1903 and 1909 and Windows server versions 1903 and 1909. By using a buffer overflow, the attacker will gain access to the target computer. This attack is called Remote Control Execution.

Attacking method:

a. Initiate machine target and Metasploit Framework

Setting up the target operating system and getting the IP 192.168.18.128. This IP will be the target identity of the target to launch the attack.

Fig. 5. Initiate Metasploit Framework

b. The attack was carried out on the Windows 10 version 1903 operating system

Fig. 6. Windows 10 version 1903

c. Open Metasploit Framework and search the payload for cve_2020_0796

In the Metasploit Framework, the search function is useful for performing key searches using the payload module for attacks [11]. Using “search cve_2020_0796” will bring up all attack modules against the CVE-2020-0796 vulnerability.

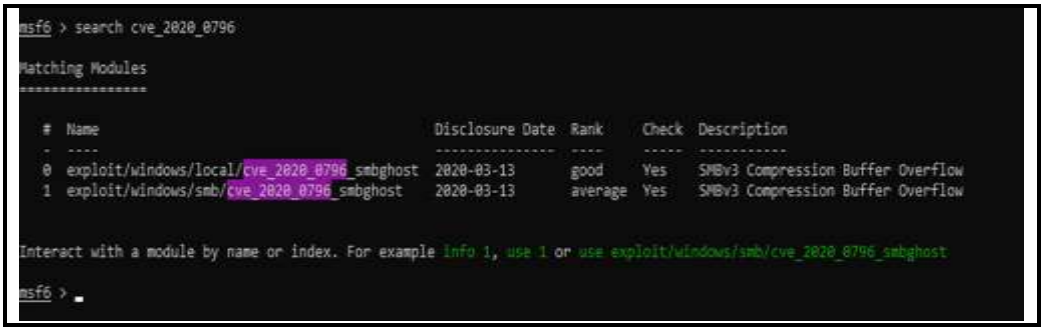

Fig. 7. Searching method on Metasploit Framework

The payload used is the “exploit/windows/smb/cve_2020_0796_smbghost” payload. Use the "use {payload}" command to use the payload.

d. Setting parameters on payload

Using the “SHOW OPTIONS” command to get the parameter information needed by the payload in carrying out the attack [11]. Parameters are all the things that the payload needs in carrying out the attack. Parameters include: (1) attack targets, (2) module settings, and (3) payload settings.

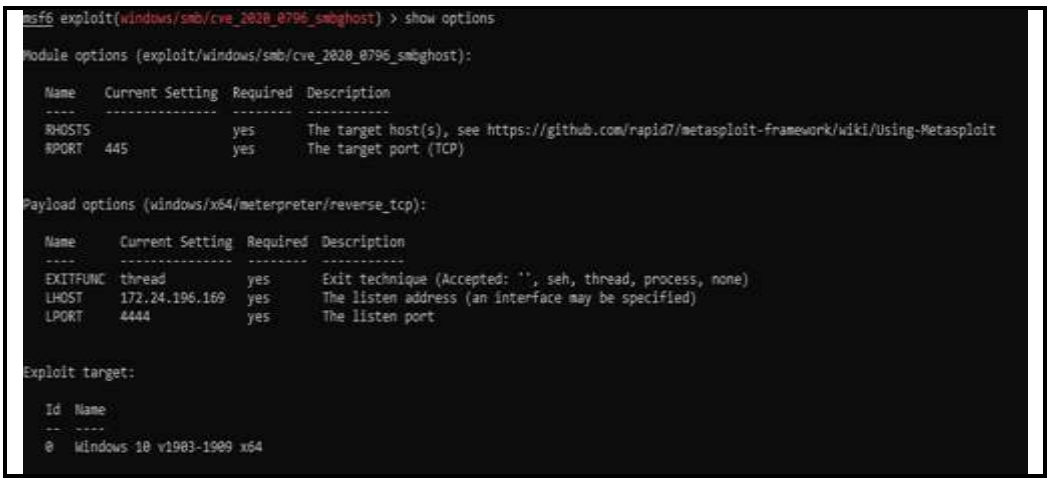

Fig. 8. Setting Payload

e. Setting up the RHOST and session to carry out the attack

Fig. 9. Setting target on Payload

RHOST is the host of the target in the form of target IP information [10]. For SMB Server PORT itself, the default is port 139 and 445. Use the command "set RHOSTS 192.168.18.128" to change the target payload setting for the attack.

f. Running the payload

Command "exploit" or "run" is used to run the attack with my setting mode [10]. After the attack, then usually get some Meterpreter and then get the reverse shell.

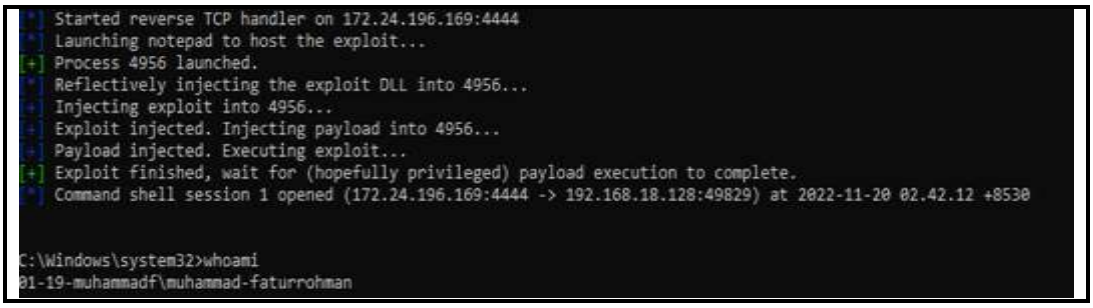

Fig. 10. Get the reverse shell

The attack on CVE-2020-0796 with the Metasploit Framework uses payload available in the Metasploit Framework database. After setting the target with the Metasploit Framework, a hacker can carry out this attack. This proves that this attack is easy for hackers to attack operating systems with CVE-2020-0796 vulnerabilities.

By using the existing payload, hackers are able to set parameters to attack multiple device platforms. Apart from that, settings for avoiding antivirus and firewalls can also be done using the Metasploit Framework. The Metasploit Framework launches an attack against an existing vulnerability using the attack payload database. This framework is used by hackers to simplify attacks and make attacks more flexible and efficient.

The Metasploit Framework makes it easier for hackers to carry out attacks on every device if there is already a payload in the framework database. Because of that, the way to protect the device is by updating the system or patching done by Microsoft. Microsoft must have received a report on a bug or gap that exists and immediately fix it. Updating the system or using the latest system is the most powerful way to prevent attacks from the Metasploit Framework.

5. Conclusion

In this study, it has been explained how attacks using the Metasploit Framework against the Windows 10 operating system vulnerability (CVE-2020-0796). This vulnerability is found in the Windows 10 version 1903-1909 system which is vulnerable to the Buffer Overflow technique in the Server Message Block (SMB) application.

The Metasploit Framework is a tool used by hackers to carry out attacks quickly and efficiently. This framework only requires some knowledge regarding vulnerabilities that exist on a target computer system. Even in the Metasploit Framework there is also an auxiliary module for scanning on targets. With the Metasploit Framework, the attack on CVE-2020-0796 becomes very easy to get

the target reverse shell. Overcoming this problem is enough to update the system or use the latest system that has patches in it.

For Microsoft products, it has actively been released with updates for fixing security issues. Microsoft strongly suggests for users to upgrade to the latest Windows 10 operating system. Windows 10 is the latest operating system and actively updated for the security fix. For those still needing to use the older version of the operating system, Microsoft recommends updating MS17-010 to reduce the risk of being exploited by using Eternal Blue.

References

[1] G. Fritsche, "Understanding Windows 10", Proceedings of the 2015 ACM Annual Conference on SIGUCCS - SIGUCCS '15, 2015.

[2] Windows SMBv3 Client/Server Remote Code Execution Vulnerability CVE-2020-0796. Access on https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0796

[3] O. Valea, C. Oprisa, "Towards Pentesting Automation Using the Metasploit Framework", IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), 2020.

[4] S. Raj, N. K. Walia, "A Study on Metasploit Framework: A Pen-Testing Tool" International Conference on Computational Performance Evaluation (ComPE), July 2–4, 2020.

[5] S. Rani, R. Nagpal, "PENETRATION TESTING USING METASPLOIT FRAMEWORK: AN ETHICAL APPROACH", International Research Journal of Engineering and Technology (IRJET), Vol 06, 2019.

[6] N. A. Mohamed,A. Jantan , O. I. Abiodun, "Protect Governments, and organizations Infrastructure against Cyber Terrorism (Mitigation and Stop of Server Message Block (SMB) Remote Code Execution Attack)", International Journal of Engineering Research and Technology. Volume 11, Number 2, pp. 261-272, 2018.

[7] Dr. S. Kurariya, "Buffer Overflow Attack –Vulnerability in Heap" BSSS Journal of Computer, Vol. XI, pp 1-11, 2020.

[8] A. Smirnov, T. Chiueh, "Automatic Patch Generation for Buffer Overflow Attacks", Third International Symposium on Information Assurance and Security, 2007.

[9] Kaushik, Keshav, et al. "A novel approach to generate a reverse shell: Exploitation and Prevention." *International Journal of Intelligent Communication, Computing and Networks (IJICCN), Open Access Journal* 2, 2021.

[10] C. Cowan, S. Beattie, J. Walpole, C. Pu, and Perry Wagle, "Buffer Overflows:Attacks and Defenses for the Vulnerability of the Decade, Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, 2002.

[11] S. Rahalkar, "Metasploit for Beginners", Packt Publishing Ltd, Livery Place, 35 Livery Street, Birmingham, B3 2PB, UK, July 2017.