Linux Operating System Security Testing Case Study: FTP Security in Metasploitable 2

Muhammad Anis Al Hilmi[1)], Fauziah Herdiyanti[2)]

[1-2)] Informatics Departement, Politeknik Negeri Indramayu, Indramayu, Indonesia

Correspondence Author: alhilmi@polindra.ac.id

Article Info :

Article History :
Received :
24 Dec 2022
Revised :
21 July 2023
Accepted :
25 July 2023
Available Online :
13 August 2023

Keyword :

Metasploitable2, Backdoor, Linux, FTP, NMap, Kali Linux

ABSTRACT

Linux is an operating system like Unix that uses a kernel and includes applications and other support-ing modules to be used properly. Linux is free to use and includes open-source code to be used and devel-oped by all parties. The Linux operating system is widely used as a server, for example, for hosting web applications or used in cloud computing infrastructure. No wonder Linux is one of the targets of cyberat-tacks. In this study, a simulation of attacks on the Linux operating system was carried out, and one type of Linux distribution tested as a target was Metasploitable2. Metasploitable2 is a Linux operating system that is intentionally made vulnerable to attack; the aim is to be experimental material. In testing, Metasploitable2 was treated as the target of the attack and Kali Linux as the attacker. The initial stage of the attack simulation, carried out using NMap, Metasploitable2 security vulnerabilities can be identified and exploited for later attacks with exploits. The type of exploit used is a backdoor because a backdoor can function to penetrate systems, programs, or networks without going through the authentication pro-cess. In this case, Metasploitable2 has a security hole in its FTP port. The loophole is tried to be exploited. In this case, the way to overcome the attack is by closing all possible entry points to be an attack loop-hole; in this case, Metasploitable2 is port 6200 and disabling anonymous account permissions to upload files using FTP.

1. INTRODUCTION

Cybercriminals can exploit many loopholes. They take advantage of security holes to steal data or take advantage of hacking into systems. Hackers take advantage of the web system managers' and public users' unpreparedness [1]. Implementation of security is significant to ensure the system is not interrupted and disturbed. Hardware and operating system protection and security are just as necessary. The operating system is only a tiny part of a system's software.

Linux is an operating system like Unix that uses the kernel as the core and includes applications and other supporting modules to be used properly. Linux is free and includes open-source code so that all parties can use and develop it [2]. The Linux operating system is widely used as a server, for example, for hosting web applications or in cloud computing infrastructure. No wonder Linux is one of the targets of cyber attacks. In this study, an attack simulation was carried out on the Linux operating system, and one type of Linux distribution being tested as a target was Metasploitable2. Metasploitable2 is treated as the target of the attack, and Kali Linux as the attacker.

ISSN Print : 1979-7141
ISSN Online : 2541-1942

1.1 Operating System

In general, the operating system is the first layer of software that is placed in the computer's memory when the computer is turned on, while other software is run after the operating system is running. The operating system will serve needs such as disk access, memory management, task scheduling, and display/user interface [2].

1.2. Linux

Linux is a UNIX system that can be used for networking, software development, and everyday use, such as in the office. Linux is an inexpensive alternative operating system because it is usually free compared to other commercial operating systems [3]. The Linux operating system features true multitasking, shared libraries, demand-loading, proper memory management, and multiple users. Linux supports much software ranging from word processors, X-Windows displays, and GNU C/C++ to TCP/IP.

1.3. Metasploitable2

Metasploitable2 is a Linux-based operating system that is intentionally vulnerable. This OS can be used to conduct security training, test the security of a system, and practice standard penetration testing techniques. In testing, Metasploitable2 is treated as an attack target (acting as a website server), and Kali Linux is an attacker. The initial stage of the attack simulation is to scan Metasploitable2 using the NMap software from the attacker side (Kali Linux); from there, the Metasploitable2 security holes can be identified and exploited for later attacks with exploits.

1.4. FTP

FTP (File Transfer Protocol) generally functions as a medium for exchanging files or data in a TCP network. The FTP used is based on open-source to support a high level of stability and is not easily infected with viruses and malware. FTP is the most appropriate protocol method for fast file/data storage in uploading and downloading from a server computer to a client without using a flash drive to retrieve data from the server computer [4]. File Transfer Protocol (FTP) is a standard network protocol that transfers computer files from one host to another over a TCP-based network like the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and server. Application users can authenticate themselves using a clear login protocol, usually a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects usernames and passwords and encrypts their contents, FTP is often secured with SSL/TLS (FTPS) [5][6].

1.5. IP

The Internet Protocol (IP) is a protocol or set of routing and addressing rules for data packets to travel through a network and reach their proper destination [7]. The function or purpose of the Internet Protocol is to move datagrams through a series of interconnected networks. This is done by passing datagrams from one internet module to another until the destination is reached. The internet module resides on the host and gateway in the internet system. Datagrams are routed from one internet module to another through individual networks based on internet address interpretation. So, one of the essential mechanisms of the internet protocol is the internet address [8].

1.6. NMap

In an attack simulation, there is a stage called scanning, the purpose of which is to obtain information on the condition of the target (Metasploitable2) as initial information for the attacker. This process uses the NMap software from the attacker side (Kali Linux). From there, the Metasploitable2 security holes can be identified, for example, what ports are open on the system and other information regarding potential paths that can be used for attacks. NMap is a network scanner that is widely used by professionals in the field of network security [9];. However, some tools are made explicitly for hacking; they still need to beat NMap's popularity [10]. NMap

ISSN Print : 1979-7141
ISSN Online : 2541-1942

("Network Mapper") is an open-source tool for exploring and auditing network security. It is designed to scan large networks but can also work against a single host. NMap uses raw IP packets in a sophisticated way to determine which hosts are available on the network, what services (application name and version) are provided, what operating system (and version) is used, what type of firewall/packet filter is used, and several other characteristics. Although NMap is primarily used for security auditing, many system and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime [11]. NMap, usually installed on Kali Linux, is often used to perform system security testing [12][13].

2. METHOD

This research begins with an operating system testing plan, in which the Kali Linux operating system is prepared as the attacker, and the Metasploitable2 operating system is the attack target. After that, collect the required operating systems: Kali Linux and Metasploitable2. The operating system extension used is VMDK (Virtual Machine Disk), a file format describing a container for virtual hard disk drives for use in virtual machines such as VMware Workstation or VirtualBox. The two VMDK files are then run in the virtual machine and start configuring the network.

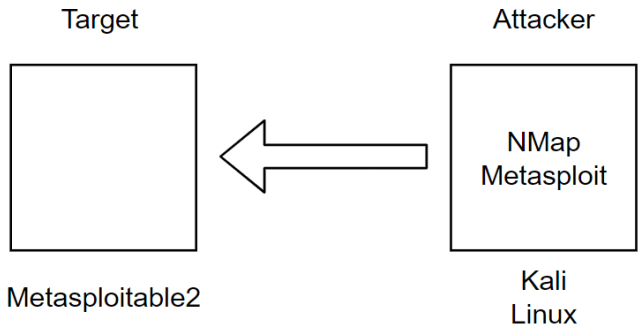

Figure 1. Testing Illustration

The test scenario begins with scanning the target IP using NMap to discover the target's security holes (Metasploitable2). From there, the attacker gets information about the conditions/specifications of the target. With that, it will make it easier for the attacker to determine which path to use for the attack, which tools match the target's condition, and how to enter the target. After knowing the target's security holes, then start exploiting the target. The target exploitation here is to enter into the system and try to take advantage of what is in it, for example, taking over the system, taking valuable data in the system, or manipulating it. This exploit process can be done using tools such as MSF/Metasploit, usually available on Kali Linux.

3. RESULTS AND ANALYSIS

This research was conducted by testing the Metasploitable2 operating system as the target of the attack and Kali Linux as the attacker. With the target IP address as capital, scanning can be done using NMap to find conditions and opportunities for security holes on the target side.

ISSN Print : 1979-7141
ISSN Online : 2541-1942

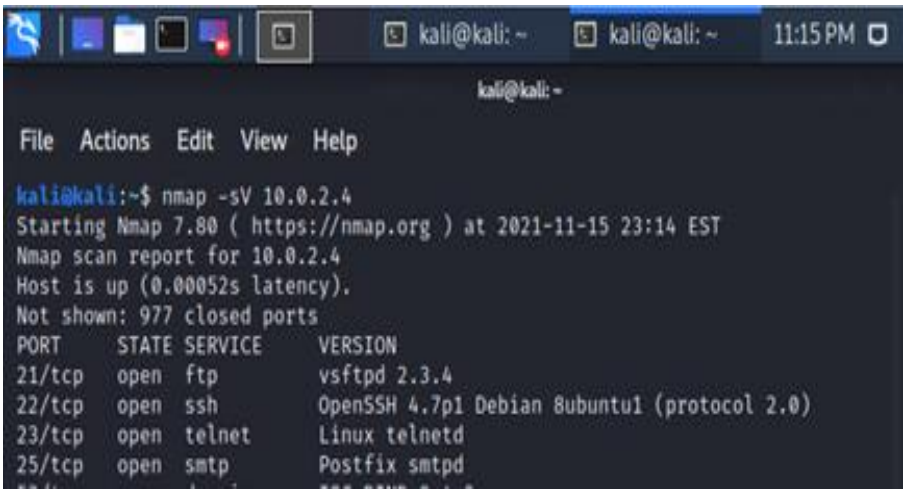

Figure 2. Vulnerability in System

The scanning results above show that the target uses FTP version vsftpd 2.3.4, which contains a security hole on port 21/TCP [14][15]. By utilizing this information, attacks or exploits can be carried out using Kali Linux. The steps for carrying out the attack are as follows:

1. Run Metasploit on Kali Linux with the "mfsconsole" command.
2. The exploit is of the backdoor exploit type, which aims to access the system without handling the authentication process.
3. The set RHOSTS <IP target> command aims to set the target IP to be done remotely.
4. Set the payload to cmd/Unix/interact or specify that the payload of cmd/Unix/interact will be used.
5. The "exploit" command executes the module or attacks the target.

The tested attack was successful, as evidenced by the appearance of the statement "session 1 opened". The impact of this attack is that the attacker can perform Remote Code Execution (RCE) on the attacked system (Metasploitable2). The RCE was carried out by adding libraries and changing the access rights of several files. The results of these attacks are presented in the table below.

Table 1. Result

Exploit Type	Backdoor
Command	exploit/unix/ftp/vsftpd_234_backdoor
Respond	Session opened
Status	Succeed

Kali Linux utilizes the FTP version vsftpd 2.3.4 as a security hole on port 21. The security hole is then exploited using a backdoor by Kali Linux until it successfully opens session 1. From the success of this attack, Kali Linux can upload files freely using FTP on servers. The impact of this exploit will be hazardous for the Metasploitable2 operating system. However, this can be handled in several ways. One way to handle it is presented in table 2.

Table 2. Hardening Process

Configuration File	vsftpd.conf
Syntax	anon_upload_enable = YES ; comment this line with #
Configuration	Block port 6200 (backdoor using this port)
Purpose	Prevent anonymous permissions from uploading files freely, so that later an authentication process is required first.

ISSN Print : 1979-7141
ISSN Online : 2541-1942

The purpose of adding a hash mark to the anon_upload_enable = YES command is so that the command is considered a comment and is inactive. This security hole is caused by a default configuration that allows anonymous accounts (without an authentication process) to upload files using FTP.

4. CONCLUSION

From testing the security of Linux-based systems, namely as targets are servers using the Metasploitable2 distro and attackers (Kali Linux) with NMap and Metasploit, it can be concluded:

1. The Linux-based Metasploitable2 operating system is vulnerable to port 21 or the FTP proto-col version 2.3.4. This security hole can be used to carry out exploit attacks using a backdoor so that attackers can enter the system without going through the proper authentication pro-cess.
2. The security vulnerabilities in Metasploitable2 can be patched by doing several things: clos-ing all possible entry points to become an attack hole, namely by activating the authentica-tion feature in using FTP, or disabling anonymous accounts uploading files and blocking port 6200 (because used by backdoors).

5. ACKNOWLEDGEMENTS

This paper is the result of a student's lab project research.

6. DECLARATION OF COMPETING INTEREST

We declare that we have no conflict of interest.

7. REFERENCES

[1]. K. A. CAHYANTO, M. A. AL HILMI, and M. MUSTAMIIN, ‘Pengujian Rule-Based pada Dataset Log Server Menggunakan Support Vector Machine Berbasis Linear Discriminat Analysis untuk Deteksi Malicious Activity’, Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 9, no. 2, 2021.

[2]. Z. R. Mair, Teori Dan Praktek Sistem Operasi. Deepublish, 2018.

[3]. R. Watrianthos and I. Purnama, Buku Ajar Sistem Operasi. Uwais Inspirasi Indonesia, 2018.

[4]. D. Ruwaida and D. Kurnia, ‘Rancang Bangun File Transfer Protocol (FTP) dengan Pengamanan Open SSL pada Jaringan VPN Mikrotik di SMK Dwiwarna’, CESS (Journal of Computer Engineering, Sys-tem and Science), vol. 3, no. 1, pp. 45–49, 2018.

[5]. M. Arman, ‘Rancang Bangun Pengamanan FTP Server dengan Menggunakan Secure Sockets Layer’, Jurnal Integrasi, vol. 9, no. 1, pp. 16–23, 2017.

[6]. T. Radivilova, L. Kirichenko, D. Ageyev, M. Tawalbeh, and V. Bulakh, ‘Decrypting SSL/TLS traffic for hidden threats detection’, in 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 143–146.

[7]. P.-B. Bök, A. Noack, M. Müller, and D. Behnke, ‘Internet Protocol Version 4’, in Computernetze und Internet of Things, Springer, 2020, pp. 125–155.

[8]. G. Lencse and Y. Kadobayashi, ‘Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis’, IEICE Transactions on Communications, vol. 102, no. 10, pp. 2021–2035, 2019.

[9]. S. Khadafi, S. Nurmuslimah, and F. K. Anggakusuma, ‘Implementasi Firewall Dan Port Knocking Se-bagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server’, Network Engi-neering Research Operation, vol. 4, no. 3, pp. 180–188, 2019.

ISSN Print : 1979-7141
ISSN Online : 2541-1942

[10]. G. Bagyalakshmi et al., "Network Vulnerability Analysis on Brain Signal/Image Databases Using NMap and Wireshark Tools," in IEEE Access, vol. 6, pp. 57144-57151, 2018, doi: 10.1109/ACCESS.2018.2872775.

[11]. S. Sinha, 'Setting Up a Penetration Testing and Network Security Lab', in Beginning Ethical Hacking with Kali Linux, Springer, 2018, pp. 19–40.

[12]. G. Johansen, L. Allen, T. Heriyanto, and S. Ali, Kali Linux 2–Assuring Security by Penetration Test-ing. Packt Publishing Ltd, 2016.

[13]. F. R. Mahtuf, P. Hatta, and E. S. Wihidiyat, 'Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan', JOINTECS (Journal of Information Technology and Computer Science), vol. 4, no. 1, pp. 17–22, 2019.

[14]. E. Cozzi, M. Graziano, Y. Fratantonio and D. Balzarotti, "Understanding Linux Malware," 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 161-175, doi: 10.1109/SP.2018.00054.

[15]. Y. Xie, D. Feng, Z. Tan, and J. Zhou, 'Unifying intrusion detection and forensic analysis via prove-nance awareness', Future Generation Computer Systems, vol. 61, pp. 26–36, 2016.

ISSN Print : 1979-7141
ISSN Online : 2541-1942