Optimization of Server Computer Security Using the Port Knocking Method on Ubuntu Server 12.04 LTS

Amsar

Department of Computer Engineering, Polytechnic of South Aceh, Tapaktuan Indonesia
amsar@poltas.ac.id

ARTICLE INFO

Article history:
Accepted

ABSTRACT

Each online based server cannot be fully secured from various external attacks that attempt to infiltrate the system. Server security is the most important part for administrators against intruders who carry out their actions in attacking computer systems, there are several attack methods that can be done, method like brute-force are usually deployed to attack computer security systems that are connected to the internet. In this study to overcome attacks penetrating into the server system, the port knocking method can be used as a step taken to prevent attacks that enter the system or also known as the authentication method. By using this port knocking method the administrator can control the system to be more secure from brute-force attackers addressed in certain parts such as SSH server and FTP server. So that users can perform services connected with SSH server and FTP server services, knocked functions as a port knocking daemon that is ready to receive port knocking authentication from the user then rewrites the firewall, so that the connected services can be secured from attacks that try to infiltrate the server system. Furthermore, in tables and uncomplicated firewall functions to build firewalls that will deny connections to the SSH server and FTP server services. So when a foreign user accesses SSH and FTP without first doing the authentication, the firewall will reject the connection, but if the user passes the port knocking authentication stage via sending SYN packets to the port provided in the knocking daemon port, then the knocking daemon port is will rewrite the firewall so users can connect to the SSH server and FTP server services.

I. Introduction

Internet network services have provided enormous benefits for the spread of information, consequently more and more users are accessing it through internet services [1]. Internet media provide many benefits for people who need according to their respective goals such as internet needs by server administration. In order for the server computer to be accessed from an unlimited distance, an internet media service with remote login service is needed for an administrator, so that the server computer access can be done elsewhere, the administrator needs to install a secure shell service (SSH). The concept of a problem in computer network services is caused by the type of computing or the security level of certain computer systems [2]. The level of security in internet services is also a priority, because internet-based information services are vulnerable to abuse by attackers who successfully log in to computer network systems[3]. The severity and number of attacks on the internet and on computer networks have increased rapidly over time. Most security solutions are concentrated on resisting attacks, but cannot eliminate other forms of attack [4]. Access services on this internet network can be done various activities such as uploading files to the server computer, then an administrator must also install the file server application on the server.
computer. Besides that, to be able to access data on the server computer, it is necessary to run a service daemon that can run applications that continue to run by listening on the right port so that the port that is created remains open.

With this opening, it can be accessed by parties other than the server computer user, in this case the administrator, as a result there will be an attack on the server computer. If there is an attack on a computer system, there must be a standby team to prevent hacking of a computer network system by an intruder[5]. Attacks that successfully enter the computer system can ravage the existing system easily, so that data security cannot be controlled anymore by users who have access rights[6]. The system that detects the authentication process of File Transfer Protocol (FTP), Bro, and Snort services are not optimal in the process of delivering intruder information [7]. Intruders who enter the server system are called attackers, entering by means and steps that are known to have a negative impact on the server computer that should not have anyone accessing other than the administrator, usually the intruders access the server computer mostly using brute-force methods and other ways. Intruders who successfully enter the server system can have a devastating effect on data services and important files contained on the server computer, and can even damage the server computer operating system that has been built. After collecting the reasons for the importance of security on a computer that is used as a server computer, the author can perform research by framing optimization of server computer security using the port knocking method on Ubuntu server 12.04 LTS. The system must be able to function properly when the user or administrator is not near the computer system and can also be controlled remotely [8]. The purpose of this research is to secure the server computer using the port knocking method based on the Linux or Ubuntu platform so that the attacker cannot enter the server computer system.

II. Method

This research was conducted using the port knocking method. The port knocking method is a technique used in controlling and securing port access services from unknown users. The method is used to maintain one or several ports that have been previously closed and configured, and can only access users who use the sequence of requests on the port numbers that are registered as access rights.

This port knocking technique is implemented by using several techniques as work patterns that can be carried out by following the steps as follows:

1. Initially, the client computer can access that can be connected to the server computer through one of the ports on the server computer that has been provided, say the connection is made on port 22, but the service connection must be blocked first by the server computer firewall.
2. The second stage, the client accesses services on the port sequences that can be displayed or defined in the port knocking daemon configuration file on the server computer through sending synchronization / acknowledged (SYN / ACK) packages in it, at this stage, the client does not get any response.
3. Third stage, authenticates the experiment and the port knocking daemon records if an attempted connection attempt is made. If the authentication is correct and does not differ from what is defined in the port knocking daemon in this case is the defined port sequence, the knocking port daemon immediately overwrites the rule to open the port that the client wants to connect based on the rule defined in the firewall.
4. The final stage, at this stage if the client is able to access and connect to the directed port that previously used the application as in general and has been authenticated by the client, then security can be controlled so that attackers from other unknown sources cannot infiltrate in the security system.

Prevention of incoming attackers by using a security system aimed at securing the device in order to reduce or minimize the occurrence of conceding access rights [9]. If everything is done, then the client disconnects the connection services with the port then sends the data synchronization (SYN)
packet again so that the port knocking daemon rewrites the firewall rule so that access to port 22 is closed again.

**III. Result And Discussion**

In this study, the identification of problems is by installing and configuring a firewall, how the firewall works, and how the port knocking method works. In addition, several components must be configured to be able to carry out the testing stages using the port knocking method on FTP and SSH service access. In this study the design of network topology uses two client computer units, and uses two computer units as server computers. Each computer, be it a server computer or a client computer, is connected with a switch and a personal computer router with the Ubuntu operating system, in this test the client computer is different from the network computer server as shown in Figure 1.

**A. Analysis of Port-scanning**

Port scanning is an activity or process to find out the port contained on a computer, equipment and even equipment. The purpose of this port scanning is to look for data that is a possible weakness of a system installed on a computer, equipment and even equipment, this is done through an open port. There are two possible ports that are on the computer, equipment and equipment, namely due to a system error or known as a bug that does not understand the owner or user of the server computer system.

In general, hackers before launching a crime will search for information on the target of the attack, by finding out loopholes that can be hacked as far as possible and looking for weak points of the system built to be exploited through the scanning process. One of the tools used by attackers is nmap, as shown in Figure 2.
B. Brute-Force Attack

Next, after finding out which SSH port is open, a brute-force attack is carried out. Many tools can be used, such as Burp suite, Hydra, Medusa, NCrack, Patator and Phrasendrescher. One of them used is hydra. Hydra is a violent password cracking tool. In information security, password cracking is a method of guessing passwords from databases that have been stored in a computer or network system. Hydra can be used for various types of brute-force attacks.

C. Application of the Port Knocking Method

First of all, before running port knocking, first install the program on the server computer which is also useful for observing port beats and on client computer devices to do port beats on the server. Installation is done by typing the command # apt-get install knockd on the server computer or client computer (for client computers typed in the terminal), after successfully installed, the program is ready to be configured. Configuration is done in file knockd.conf, by typing the command #nano /etc/knockd.conf as shown in Figure 4 below.

In the knock conf file, there are three main parts, the first part is the options section, this is a section that serves to show the location of the log file that serves to record all the knock activity. The second part is the port open section which is the part that is used as a configuration to open the port to be addressed. In the open port section there are three command categories namely:

- **Sequence** functions to determine the beat port. It aims to open the directed port.
- **Command** which functions in determining the iptables command that is executed in the form of a command to open the destination port if it is knocked on the knock port.
- **Tcpflags** which serves to show the packet header sent as a port knock.

The third part is to close the port that serves as a configuration to close the destination port again. In the closing port there are three configuration categories, namely:

- **Sequence** which serves to determine the knock port used in closing the destination port.
- **Command** which serves to determine the iptables command that is executed in the form of a command to close the destination port if there is a knock on the destination port.
- **Tcpflags** which shows the packet header that was sent as a port knock.
To determine the knock port, add the command to fileknockd.conf, as shown in Figure 5.

Figure 5. Format knock on the server

In the SSH open section, three knock-port numbers are specified, namely port 2022, port 3022 and port 4022, if there are knocks against the three ports in sequence, the server will open the destination port according to the commands from the specified iptables. In the SSH lid three knock-out port numbers are specified, namely port 3022, port 4022 and port 2022. If there is a knock on the three port numbers in sequence, the server will close the destination port according to the specified iptables command. To determine the iptables command when a port is knocked, a command is added to the knock.conf file, as shown in Figure 6.

Figure 6. Iptables responding client knocks

In the open SSH section, the iptables command, which is executed when there is a knock on port 2022, port 3022, and port 4022, is a command that aims to change the iptables rule, by opening access to the IP addresses of the client's computer, so that it can access port 22 on the server computer. In the close section of SSH, the iptables command, which is executed when there is a knock on port 3022, port 4022, and port 2022, is a command that aims to change the iptables rule, by closing the service access back on the client computer's IP address, so that it can no longer access the port 22 on the server computer.

D. Application of the Program in Computer Network Security Systems

After configuring the knockd.conf file, the application is carried out on a computer network system. This implementation is carried out on two computers connected to each other by a computer network. The computer network topology used can be seen in Figure 7.

Figure 7. Topology in the implementation of network security systems

In Figure 7, the server computer has an IP address 192.168.0.1 and functions as a port knocking server that serves to provide port knocking services, while the client computer has an IP
address 192.168.0.27 and functions as a client in charge of knocking the server computer. The first step taken in implementing the program is to close all ports on the server computer by using the `iptables` command with the aim that all packets going to the server computer will be thrown directly (DROP) so that the server computer cannot be accessed from another computer. The command used to close all ports on the server computer is shown as shown in Figure 8 below.

![Figure 8. The command blocks all TCP ports](image)

The results shown in Figure 8 above are all closed ports on the server computer, which means there is no point of entry on the server computer that can be accessed by other computers. This is justified by scanning the port using Nmap on the server computer, as shown in Figure 9.

![Figure 9. Scanning port results](image)

The second step is to configure the `knockd.conf` file. Configuration made in the `knockd.conf` file, among others, is to determine the format of the knock port to open port 22 (portSSH). Then determine the `iptables` rule that functions to open port 22 (SSH port) and allow the source IP address that makes a tap to access port 22 (SSH port) if there is a knock on port 2022, 30022, 4022 as shown in Figure 10 below.

```bash
start_command = /sbin/iptables -I INPUT -p tcp -j DROP
```

![Figure 10. The iptables command for opening port 22](image)

Determine the format of the knock port to close port 22 (portSSH), as shown in Figure 11.

![Figure 11. Format for closing ports 22](image)

Determine the rules that apply to `iptables` which functions to close port 22 SSH port and not allow other IP addresses to be able to access port 22 SSH port if there is a knock on port 3022, 4022.2022, as shown in Figure 12 and Figure 13 below.

![Figure 12 and Figure 13. Port closure 22](image)

Overall the contents of the `knockd.conf` file are as shown in Figure 14 below.

![Figure 14. Configuration of the knockd.conf file when opening and closing port 22](image)
The third step is to run fileknock on the server computer. The command used is as shown in Figure 15 below:

![Figure 15. Commands running the knock program](image)

The fourth step is to run a knock program on the client computer that functions to do the porting by the client computer to the server computer on ports 2022, 3022, 4022 with the aim that the server computer opens port 22 and gives permission so that the client computer can access port 22 on the server computer. The command used is shown in Figure 16 below:

![Figure 16. Running the knock program to open port 22](image)

After the client computer taps port 2022, 3022, 4022 on the server computer, then the server computer will monitor the port if the port is tapped according to the open knock SSSH port format, as shown in Figure 17 below.

![Figure 17. Monitoring port](image)

In Figure 17, if a knock made by a client computer matches the open SSSH tap format, then the knock program on the server computer will run the iptables command to open port 22 (portSSH) on the server computer and will only give the client computer access to use port 22 (portSSH).

![Figure 18. Chain iptables for opening port 22.](image)

![Figure 19. Access by the client](image)
In figure 19, the client computer connects to the server computer, after the client computer knocks the port, and the server computer opens port 22 only for access by the client computer. When the client computer has accessed port 22 (SSH port) on the server computer, then the fifth step that is passed is that the client computer makes a tap again with the knock format used when resupping port 22 (portSSH) on the server computer, a knock is made is a knock towards port 4022,3022,2022. The command is used as in Figure 20 below.

![Figure 20. Running the Knock Program to Close Port 22.](image)

When the client computer knock port 4022, 3022, 2022 on the server computer, the knock program will monitor the port whether the port is tapped according to the SS knock-close port format. If the knock is correct, the knock program will run the iptables command to close port 22 (portSSH) on the server computer, as shown in Figures 21 and 22.

![Figure 21. Monitoring knock after closing SSH](image)

![Figure 22. Chain iptables after knocking the SSH.](image)

**IV. Conclusion**

Based on the results of the study it can be concluded as follows:

1. The security level of the SSH service has high security, but this service is vulnerable to brute-force attack and system scanning so security is needed for this service.
2. Attacks from scanning systems such as SSH services can be prevented by doing port scanning using port knocking, so that SSH services are not easily tracked and accessed.
3. The server computer access time is doubled compared to system without port knocking authentication.
4. Without using a firewall, the port used for port knocking authentication is not visible when stealth scanning is done using Nmap.
References


