Network Security Applications Using the Port Knocking Method

Network Security Applications Using the Port Knocking Method

Mohammad Idhom[1], HE Wahanani[2], Akhmad Fauzi[3]

[1,2] Department of Informatics, Faculty of Computer Science University of Pembangunan Nasional Veteran Jawa Timur, Surabaya, Indonesia
[3] Department of Economic Development, Faculty of Economic and Business Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya, Indonesia

Email: idhom@upnjatim.ac.id

Abstract. The most important point in network services is security of access in the port . However, the problem that occurs is an open port or access that cannot be accessed with authentication that can facilitate unauthorized users to be accessed by the server. This is the basis for increasing access rights to the server that is built without having to close the port used by the user. Therefore a port knocking method is needed. Port knocking is a security system that can perform a function that is blocking unwanted access. In principle, port knocking successfully closes all ports on the server. If the user needs access to the server, the user does a "knock" to use the service, then if the user has finished accessing the port is closed again. The system built in this study uses three ports, namely port 22 (SSH), port 23 (Telnet), and port 80 (Web). Port Access time is 10 seconds each. Based on the results of the analysis and testing of the system implementation carried out, the results of the system can be run properly and can improve the security of network systems that are built compared to networks that do not use Port Knocking security. In research assessing on public and local networks. According to the results analysis, carrying out a remote server via local time requires faster time from a remote server through the public. In the SSH protocol there is a difference in time of 2.42 seconds, Telnet 2.14 seconds, and Web 2.19 seconds.

Keywords: network security, webserver, port knocking

1. Introduction

In the case of server management, usually the system administrator does not always have to be in the server room. This is because the server room is usually designed to have a fairly cold and stable temperature, which is certainly not good for the body. So usually an administrator performs his duties from outside the server room by using a remote server application [1]. Thus an administrator can simply authenticate to the server and if successful the administrator will get access to manage the server.[2]

Various methods and the number of attacks on a server are increasingly increasing. The opening of several ports that listen indirectly will invite the attackers and certain parties who are not responsible for breaking into the server through that port. The thing that is often done by attackers is trying to exploit various applications that are running through open ports on the server side[3]. To

prevent things that are not desirable, usually the administrator will install a firewall and do some configuration which in essence is to limit anyone who will access the server.

The opening of ports on the server, especially the port for remote server applications, will certainly be the center of attention for the attacker to be exploited. Port knocking [4][5][6] is present as one of the authentication methods that can be used to overcome the above problem. This method has the ability to determine who really has the right to access the server.

2. Research Method

Design to be carried out can be seen in Figure

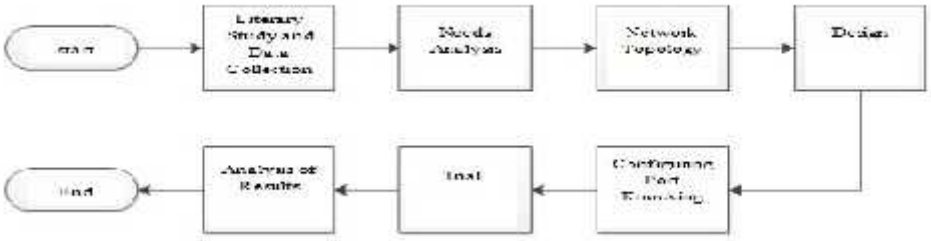

Figure 1. Research Design

1. Data Collection
   The first stage is used to find references from various sources (books, papers, journals, e-books) to assist in supporting the completion of this research.
2. Needs Analysis
   The second stage is used to analyze the needs used during the research, both in terms of software and hardware
3. Network Topology
   The third stage is used to describe the network topology that is implemented according to actual conditions as a test of performance during the research.
4. Design and Design
   The fourth stage is used to design and design the devices and configurations that will be implemented in this study. This design and design includes the provision of IP addresses on each device.
5. Configuring Port Knocking
   The sixth stage is used to configure the firewall using the port knocking method. This stage is the most important stage in this study, because it is an indicator of the success of this research trial.
6. Trial
   The seventh stage is used for testing the network security system that has been created. The trial was conducted through two sides, namely the local side and the public side (internet).
7. Analysis of Results
   The eighth or final stage of this study is used to analyze the results that have been obtained at the implementation of the study.

The topology that will be used in this study can be seen in Figure 2. It is explained that on the local side there is 1 Router-based Mikrotik routerboard, plus a firewall configuration, and a server that has an Ubuntu Server operating system, and 2 clients that have the Windows 8 and Ubuntu operating systems. As for the public side, intruders or hackers try to access the server through the public network. The router has been configured so that the server that is on the local side can be accessed remotely via the public network

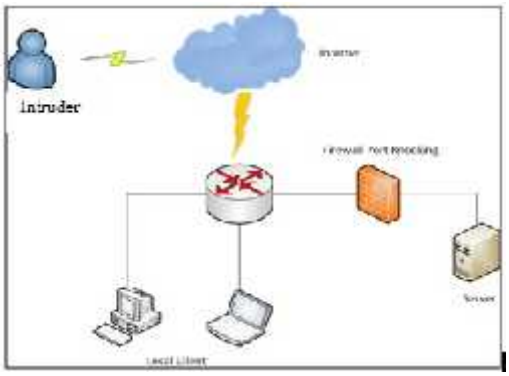

Figure 2. Network Topology

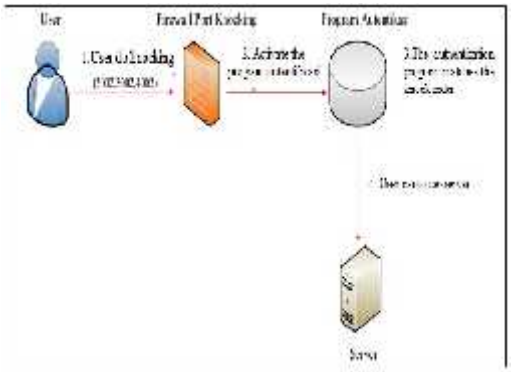

Figure3. Desain Firewall Port Knocking

So that between devices can communicate with each other, configuration is required to connect to it. This research uses port forwading from the router side so that servers on the local side can be accessed or controlled remotely using public networks.

The next design is done in a firewall configuration where in this study using the port knocking method. The concept of port knocking itself is closing ports that are commonly used for network activities such as ports 22, 23, and 80. By closing these ports, intruders will have difficulty accessing ports that are normally open freely. In this research, it will be explained through a flowchart that will explain the systematics or work concepts of port knocking.[14][15]

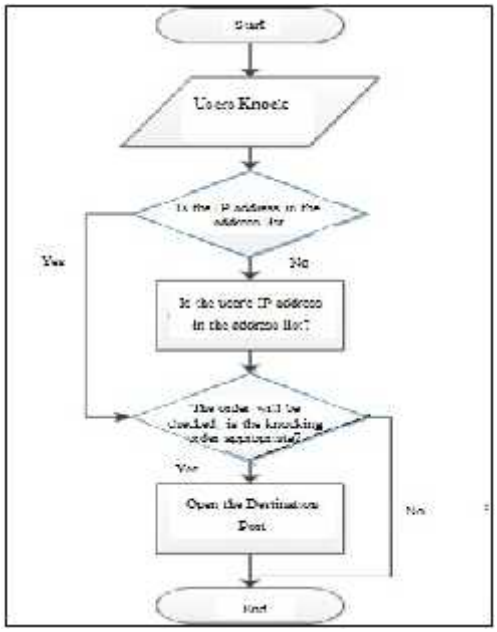

Figure 4. Flowchart Port Knocking

At this stage, the firewall configuration uses the port knocking method which will be implemented on the router. This stage is the most important stage in this research. The indicator of research success lies in testing this firewall[7].

The router knocking configuration is located on the firewall menu. The router functions as a firewall for the server. The knock format used in this design is a port format with a fixed / static mapping and uses three beats to open a port.

The sequence of beats and program scenarios designed in this study can be seen in Figure 3, how the program runs on the client and server side.

There are 2 scenarios that will be carried out in this research trial, namely:

a. Scenarios without the Port Knocking Method

b. Scenarios with the Port Knocking Method

Table 1. Limitation of Trial

Parameter	Value
Software	Nmap, PuTTY, Chrome, Hydra
Attack	Port Scanner Attack, Brute Force
Network	Lokal, Public
Port	22, 23, 80
Knock	2002, 3002, 4002
Waktu	@ 10 Second

Analysis of Results

In this stage an analysis of results is based on the data obtained. This analysis includes the performance results achieved namely port conditions after using a firewall, performing a remote server, and server activity logs are as follows:

a. Port Conditions

To see the port conditions when a port scanner attack is performed. The port will be scanned to find out if the port is open or closed. According to nmap.org, there are 6 different port conditions. Next explained in table 2.

Table 2. Condition Port

Status	Keterangan
Open	Port with open condition
Closed	Port with closed condition
Filtered	The port cannot determine whether the port is open because it prevents scanning from reaching the port.
Unfiltered	The port can be accessed, but cannot determine whether it is open or closed.
Open | Filtered	Ports in this status cannot determine whether the port is open or filtered.
Closed | Filtered	Ports in this state cannot determine whether the port is closed or filtered.

b. Remote Server

To see how the firewall works, the server will be able to be controlled when the user can knock with a specified time limit. Remote uses the PuTTY application to access the SSH server and Telnet server, and Google Chrome to access the Web server.[7][8] Next explained in table 3.

c. Activity Logs and Analysis

To see all activities carried out by the server into the log system. The log will provide reports based on date and time. At this stage, an analysis of server activity is also performed, such as looking at the client's IP address when accessing the server[9][10]. Analyzing using the Wireshark application.

d. *Remote Server Delay.*

The final analysis is to do a delay calculation. While the delay itself is the time delay of the process of sending data from one source point to the destination point. This analysis looks at server delays that can be accessed when on a local and public network.[11][12]

4. Result and Discussion

This study has two scenarios, the first scenario without the port knocking method and the second scenario using port knocking. Each scenario is tested on two network connections, namely local and public.

Scenarios without Methods To test the first scenario, the configuration of the router firewall needs to be turned off first. Select all the rules, then click the red x button.

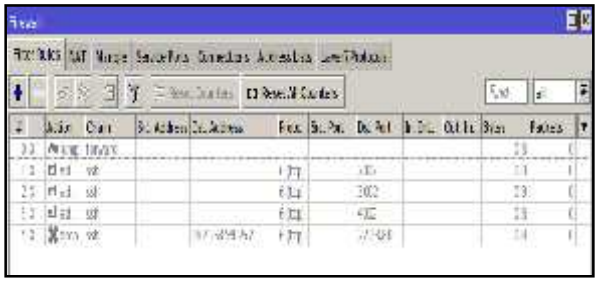

Figure 5. Disable Firewall

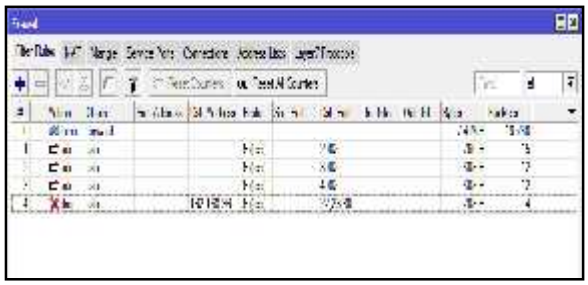

Figure 6. Enable Firewall

Scenarios with Methods
In this second scenario, the test scenario using the port knocking method needs to be activated on the firewall that has been turned off in the first scenario.

To access the server, a method that is used in this research is a port knocking method. The method used in this method is enough to deliberately access certain ports with the intention of entering the identity of the accessor in the address list. If the combination of ports that are tapped in the order with a certain time, then the log will record and the firewall gives an exception to the user who successfully knocking.

After knocking in sequence and in accordance with the specified time, the log address list records with the name port + port2 + port3 with no access time limit. This makes it easier for the admin in operating the server. On Windows operating system clients, the way to do knocking is the same as the linux client. There is no difference at all.

After knocking, the accessor or admin will be given an exception to be able to remotely on a server with ports as configured, namely port 22 (SSH), 23 (Telnet), and 80 (Web / HTTP).
In the results and discussion will be explained the results of trials of the scenarios that have been made previously. The results of this trial will provide an overview of the performance of the firewall that has been built.

Table 3. Conditions Port

Client	Acces Mode	Skenario I	Skenario II
Linux	Port 22 (SSH)	Open	Filtered
	Port 23 (Telnet)	Open	Filtered
	Port 80 (Web)	Open	Filtered
Windows	Port 22 (SSH)	Open	Filtered
	Port 23 (Telnet)	Open	Filtered
	Port 80 (Web)	Open	Filtered

At this stage of the analysis it is also seen from the length of the process of scanning from both the client and both scenarios. Data obtained based on several experiments and taken the fastest.

Table 4. Remote Server

Client	Acces Mode	Scenario I	Scenario II
Linux	Port 22 (SSH)	Succes Login	Failed Login
	Port 23 (Telnet)	Succes Login	Failed Login
	Port 80 (Web)	Succes Acces	Failed Acces
Windows	Port 22 (SSH)	Succes Login	Failed Login
	Port 23 (Telnet)	Succes Login	Failed Login
	Port 80 (Web)	Succes Acces	Failed Acces

Table 5. Test Result

Acces Mode	Testing	Test Equipment (Tools)	Result
Disable Firewall	Scanning	Nmap	Port Open
	Sniffing	Wireshark	SSH encrypted,Telnet Non encrypted
	Remote	PuTTY, Web Browser	Successfully Login, Successfully Access
	Attacking	Hydra	Terindeks
Enable Firewall	Scanning	Nmap	Port Filtered
	Sniffing	Wireshark	Not capture
	Remote	PuTTY, Web Browser	Failed to Login, Failed to Access
	Attacking	Hydra	Error / Not Indexed

Table 6. Delay Remote Server

	Protokol	Delay
Public	SSH	2.90 second
	Telnet	3.28 second
	Web / DNS	2.72 second
Local	SSH	0.48 second
	Telnet	1.14 second
	Web / DNS	0.53 second

Based on table 6, comparison of delay on local and public networks can be made into a graph.

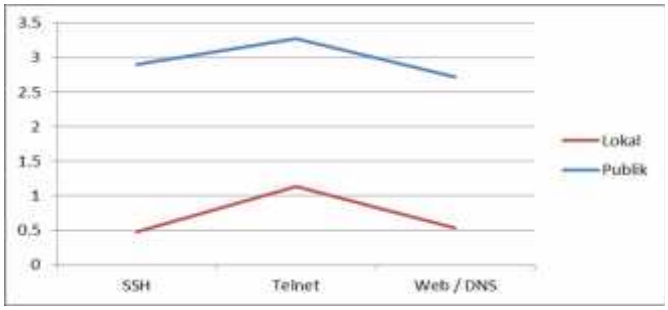

Figure 6. Local and Public Network Delay Comparison Chart

Seen in the graph, accessing a server on a public network takes a few seconds longer than accessing a server via a local network. The SSH protocol has a difference of 2.42 seconds, for the Telnet protocol 2.14 seconds, while for accessing via the Web has a difference of 2.19 seconds. This is also influenced by each other's internet speed.

Analyzing the server log, it can be seen who has accessed the server in terms of IP address, username and password. Run the wireshark application that is installed on the client. When wireshark is running, do SSH connection after knocking.

Based on testing it can be concluded that the difference between the SSH and Telnet processes is that the SSH process is safer than Terlnet. This is because SSH has an encryption process. With SSH, all conversations between server and client are encrypted, meaning that if the conversation is intercepted, eavesdroppers may not understand the contents. So that the communication process is safer. While the equation of the two is equally used to do remote to the server.

After testing with various stages, it is also necessary to analyze the attacks (brute force) that have been carried out to determine the security level of the network that has been built. Attacking is

done when the firewall is not active, the results show that the username and password can be indexed easily. However, when the firewall has been activated, attacking brute force cannot be performed.

Conclusion

Based on research that has been done on network security systems using the port knocking method, it can be concluded that the network security system has been successfully created and in accordance with the expected design. With the port knocking method, communication between computers can be done even through closed ports.. The weakness of the system that is made is still done manually to open and close ports that have been blocked by the firewall system. The research was tested on public and local networks. Doing remote server via local requires faster time than remote server via public. In the SSH protocol, the difference in time is 2.42 seconds, Telnet 2.14 seconds and Web 2.19 seconds.

Acknowledgments

This work is supported by Department of Informatics, Faculty of Computer Science, University of Pembangunan Nasional Veteran Jawa Timur Indonesia.

References

[1] Maata, Rolou Lyn R., et al. "Design and Implementation of Client-Server Based Application using Socket Programming in a Distributed Computing Environment." *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*. IEEE, 2017.

[2] Willinsky, John. "Open journal systems: An example of open source software for journal management and publishing." *Library hi tech* 23.4 (2005): 504-519.

[3] Landoll, Douglas J., and Douglas Landoll. *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press, 2005.

[4] Pourvahab, M., Atani, R. E., & Boroumand, L. (2012). SPKT: Secure Port Knock-Tunneling, an Enhanced Port Security Authentication Mechanism. *IEEE Symposium on Computers & Informatics*.

[5] Kusuma, A. P. (2016). Implementasi Simple Port Knocking Pada Dynamic Routing (OSPF) Menggunakan Simulasi GNS3. *Jurnal Manajemen Informatika Volume 5 Nomor 2*, 7-17.

[6] S. Jeanquier, "An Analysis of Port Knocking and Single Packet," MSc Thesis, Information Security Group, Royal Holloway College, University of London, 2006

[7]Liew, Jiun-Hau, et al. "One-time knocking framework using SPA and IPsec." *2010 2nd International Conference on Education Technology and Computer*. Vol. 5. IEEE, 2010.

[8] Ali, Fakariah Hani Mohd, Rozita Yunos, and Mohd Azuan Mohamad Alias. "Simple port knocking method: Against TCP replay attack and port scanning." *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. IEEE, 2012.

[9] Garg, Ajay, and Ulhas Warrier. "System and method for remotely accessing a home server while preserving end-to-end security." U.S. Patent No. 7,010,608. 7 Mar. 2006.

[10] Daniel Oxenhandler. Desining a Secure Local Area Network [online]. USA: SANS Institute; 2003.

[11] H. Al-Bahadili, A.H. Hadi, "Network Security Using Hybrid Port Knocking," International Journal of Computer Science and Network Security (IJCSNS),Vol. 10, No.8, 2010, pp. 8-12

[12]Gu, Guofei, et al. "Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection." (2008): 139.

[13]Lyu, Michael R., and Lorrien KY Lau. "Firewall security: Policies, testing and performance evaluation." *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000*. IEEE, 2000.

[14] Zhu, M., Yang, G., Yuan, Z., & Wei, S. X. (2004). *U.S. Patent No. 6,763,501*. Washington, DC: U.S. Patent and Trademark Office.

[15] Lai, Chien-Liang, and Pau-Lo Hsu. "Design the remote control system with the time-delay estimator and the adaptive smith predictor." *IEEE Transactions on Industrial Informatics* 6.1 (2009): 73-80.