Internasional Journal of Integrative Sciences (IJIS)
Vol.2, No.6, 2023: 861-868

The Effectiveness of the Port Knocking Method in Computer Security

Muhammad Nur[1], Teguh[2], Wasis Waskito[3], Azhar Fathoni[4*], Bagas[5], Yuda[6], Ramadan Galih[7], Alif Ainnun Qoyum[8], Samsoni[9]
Pamulang University
Corresponding Author: Azhar Fathoni fathonimlg@unpam.ac.id

A R T I C L E I N F O

Keywords: Computer Network, Security, Port Knocking

Received : 8 April
Revised : 14 May
Accepted: 23 June

A B S T R A C T

Computer network is a group of autonomous computers that are interconnected with each other using communication protocols through communication media so that they can share information, programs, share hardware devices such as printers, hard disks, and so on. One of the most important network components is network security, computer security involves various aspects, including protection against unauthorized access, data theft, system tampering, and operational disruptions. This research method uses descriptive method. At this stage specifications are determined regarding the system that will be designed to meet the objectives of this study, the Port Knocking method to secure the Router can be applied to Mikrotik routers by utilizing a firewall which functions to guard against illegal access and overcome problems caused by Attackers

DOI: https://doi.org/10.55927/ijis.v2i6.4526
ISSN-E: 2985-9050
https://journal.formosapublisher.org/index.php/ijis

INTRODUCTION

Computer network is a group of autonomous computers that are interconnected with each other using communication protocols through communication media so that they can share information, programs, share hardware devices such as printers, hard disks, and so on. A computer network consists of computers, software, and network devices that work together in one scope, which is called a network. The development of Information Technology (IT) is very rapid, as evidenced by the increasing sophistication of the world of Information Technology from time to time. With the increasing sophistication of information technology, it makes it easy for humans to communicate. TCP/IP (Transmission Control Protocol/Internet Protocol) is used as a data communication standard used by internet users to exchange data between computers on the internet network. This protocol is part of a suite (protocol suite) so it cannot stand alone. This type of protocol is currently the protocol with the highest number of users.

To serve billions of users worldwide, the Internet (an interconnected network) uses a global standard transmission control protocol system/Internet protocol suite (TCP/IP) for packet exchange. A port in the TCP or UDP protocol, a component of the OSI Transport layer, is the port used for communication. Network security is important and must always be a concern, both Local Area Network (LAN) and Wireless or wireless networks connected to the internet are basically insecure and always vulnerable to hacking. Since data has to pass through several terminals to reach its destination, this creates the possibility for other users who are not responsible for changing, replacing, destroying, or even stealing data (Attacker). One of the most important network components is network security. However, network security issues are often overlooked. To increase network security, administrators only try to use the best defenses so far, such as firewalls and intrusion detection systems (IDS). When data is sent, it will go through several terminals before reaching its destination, this gives an opportunity to intercept and modify data by other users who are not responsible. The majority of crackers use the system's open ports to attack network systems. A Dos or ddos attack, which targets a host or target computer with a large number of packets coming from multiple hosts, is an illustration of this type of attack. Crackers need to understand the open ports and targets for this attack to be successful. The stages carried out by the attacker in carrying out the attack are identifying the target computer or the port scanning stage, the attacker can retrieve information on the open ports on the target machine**. *Distributed Denial of Services*** (***DDoS***) attacks Computer security is an effort to protect computer systems and data contained in them from threats and attacks that may occur. Computer security involves various aspects, including protection against unauthorized access, data theft, system tampering, and operational disruptions.

LITERATURE REVIEW

A Computer Network

Network is a telecommunications network that allows computers to communicate with each other by exchanging data. The purpose of a computer network is to be able to achieve its goals, every part of a computer network can request and provide services (service). The party requesting/receiving the service is called the client (client) and the party providing/sending the service is called the server (server). This design is called a client-server system, and is used in almost all computer network.

Computer security

Is the study of the methods, principles and practices used to protect computer systems from threats, attacks and abuse that might undermine the integrity, confidentiality and availability of computer data and resources. Here are some important computer security theories:

1. **System Security**: This theory deals with the protection of computer systems from threats and attacks. This includes the use of security policies, access management, data encryption, and the use of other technologies to protect systems from attacks of various types.
2. **Cryptography**: Cryptography is the science and art of hiding information by converting it into an unreadable (encrypted) form and then returning it to its original form (decryption) using a cryptographic key. Cryptographic theory discusses cryptographic algorithms, security protocols, and encryption strength.
3. **Network Security**: Network security theory focuses on protecting communications and network infrastructure from attacks and threats. This involves using firewalls, intrusion detection, network traffic encryption, and other security techniques to prevent unauthorized access and intrusions.
4. **Application Security**: Application security theory deals with the design, development, and testing of applications to ensure that they are resistant to attack and abuse. This involves implementing safe development practices, such as input validation, avoidance of common vulnerabilities, and protection against injection, cross-site scripting (XSS) attacks, and other attacks..
5. **Security Management**: Security management theory addresses the strategies, policies, and processes used in managing the security of computer systems. This includes risk identification, risk assessment, security monitoring, regulatory compliance and response to security incidents.
6. **Information Security**: Information security theory includes the principles and practices used to protect critical information from threats and attacks. This involves data protection, information use policies, identity and access management, and secure deletion practices.
7. **Physical Security**: The theory of physical security deals with the protection of computer hardware and its physical infrastructure. This includes measures such as physical security of the server room, physical access controls, use of access keys and cards, and protection against theft or physical damage.

Port knocking is a computer network security method used to hide normally open ports in a firewall. This method requires special steps to open those ports and allow access to protected.

The port knocking process usually involves the following steps:

a) **Setting up the firewall**: First, the firewall is configured to block all incoming connections to the ports you want to hide. Under normal conditions, these ports cannot be accessed directly from outside the network.
b) **Knocking pattern**: A user wishing to access hidden ports must make a series of connections to certain ports on the protected system in a certain order. This pattern is often a predetermined sequence known to authorized users.
c) **Opening ports**: After a series of connections are established according to the correct knocking pattern, the firewall will detect the sequence and open temporarily hidden ports. The knocking user can then connect to those ports for a set period of time.
d) **Access to the system**: After the ports are open, users who have passed the knocking process can access the system through these ports. Connections to these ports are considered valid by the firewall because they have passed the proper knocking steps.

The advantage of the port knocking method is to protect normally open ports from port scanning attacks by attackers. This method hides those ports effectively and requires knowledge of the correct knocking pattern to gain access to protected systems.

However, it is important to remember that port knocking is not a perfect security solution. This method is still vulnerable to attacks such as replay attacks, where the attack logs and plays back a series of knocking connections previously made by an authorized user. Therefore, the use of port knocking must be done with caution and in combination with other safety measures to achieve a higher level of security combined with other security measures to achieve a higher level of security.

METHODOLOGY

This research method uses descriptive method. At this stage, specifications are determined regarding the system that will be designed to meet the objectives of this research.

The stages of the research are shown by the flowchart in Figure 1.

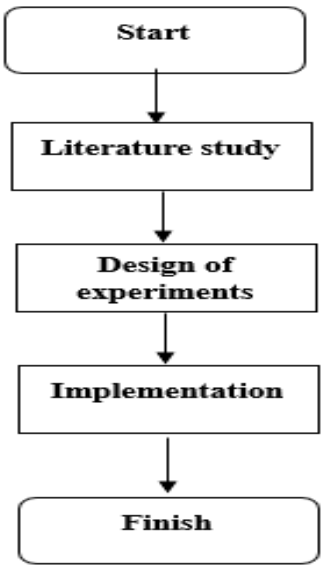


Figure 1. Flowchart of Research Stages

A. Study of literature

Search for references supporting sources that can be used as a reference in making this research as well as other basic theories regarding the design and implementation of the port knocking method.

B. Port knocking

Port knocking is tapping on the communication port in the data communication system. The function and workings of this system are not much different from the literal meaning**.**

These communication ports are usually the ports in the TCP or UDP protocol which are members of the Transportation layer in the OSI standard **.**

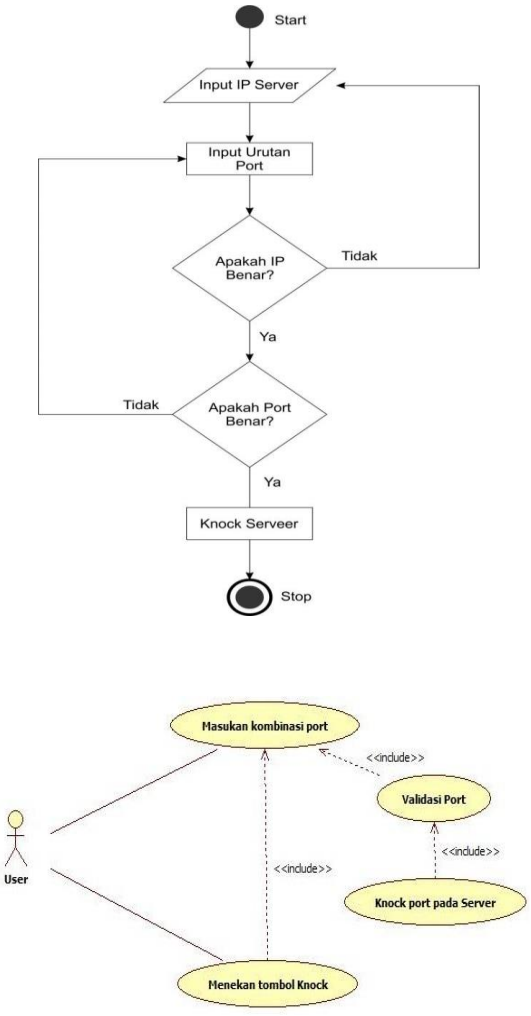
Through this communication port, the outside world can reach your device. Vice versa, you can also reach those who open certain communication ports. Communication can run smoothly, information exchange becomes easy and your computer convenience increases with the opening of these communication ports. However, sometimes this convenience is often abused by some people. These communication ports are often used as loopholes to enter illegally. The open ports are used as a path to the internal network or to the servers in it, then disrupt it**.**

RESULTS

Designing a system capable of connecting through closed ports using the port knocking method. The port knocking method is a technique for opening certain ports on a firewall by sending connection packets to a certain number of ports sequentially. Once the correct sequence is received, the firewall rules will change dynamically to allow access to the host that sent the packets.

This method is usually implemented by configuring a daemon that monitors firewall log files to look for connection attempts to certain points, and then modifying the firewall configuration accordingly. Port knocking can also be done at the kernel level by using a kernel-level packet filter such as iptables. Although port knocking can increase system security, it must be used with caution because this method can be intercepted by attackers and can lead to system compromises.

One way to mitigate this risk is to add additional security rules such as requesting the source of a packet from a known sender before opening a port. Port knocking can be used to secure SSH services on Linux by allowing access only to users who send certain packet sequences. Port knocking can also be used to hide services and ports from the system. Use case diagrams depict the processes that occur in the port knocking system.



Picture 3. Use Case System Design

Implementation

Port Knocking testing is done by accessing the Router admin from PC1. As for the test results :

Table 1. Port Knock Test

No	Test Components	Information
	First Test	
1	Login to Router	Failed
2	Ping to Router	Ping Replay
3	Ping to PC2	Ping Replay
4	Login to Router	Failed
	Second Test	
1	Ping to PC3	Ping Replay
2	Login to Router	Succeed

Based on the test results, it was found that the Router admin could not be accessed from PC1 because PC1 was only a Ping Request to PC2, so the Router Admin could not be accessed. The second test is carried out by accessing the Router admin from PC1 by Ping Request to PC3 first and then being able to log in to the Router admin. Thus the Router admin can only be accessed from PC1 if PC1 has made a Ping Request to PC3 first.

CONCLUSION

Testing the network security system with the Port Knocking method to secure the Router can be applied to Mikrotik routers by utilizing a firewall that functions to guard against illegal access and overcome problems caused by Attackers.

REFERENCES

A. Z. Mardiansyah, Y. M. Abdussyakur, and A. H. Jatmika, "*OPTIMASI PORT KNOCKING DAN HONEYPOT MENGGUNAKAN IPTABLES SEBAGAI KEAMANAN JARINGAN PADA SERVER (Port Knocking and Honeypot Optimization using IPTables for Serverrs Network Security)*," vol. 3, no. 2, 2021, [Online]. Available: http://jtika.if.unram.ac.id/index.php/JTIKA/

R. Damanik and P. Andika, "*TERHADAP SERANGAN CYBER WARFARE*".

A. Amarudin, "*Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking,*" *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.

T. Taslim, D. Toresa, and S. Syahtriatna, "Pengaruh Pengaplikasian E-learning Terhadap Hasil Belajar (Studi Kasus : Mahasiswa Keamanan Komputer Fasilkom Unilak)," *INOVTEK Polbeng - Seri Inform.*, vol. 2, no. 2, p. 182, 2017, doi: 10.35314/isi.v2i2.205.

R. Nurbahri and G. W. Nurcahyo, "Jurnal Sistim Informasi dan Teknologi Analisis Penggunaan Metode Port Knocking pada Sistem Keamanan Jaringan Komputer *(Studi Kasus di Universitas Baiturrahmah),*" vol. 5, pp. 102–108, 2023, doi: 10.37034/jsisfotek.v5i1.211.

P. Riska, P. Sugiartawan, and I. Wiratama, "Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking," *J. Sist. Inf. dan Komput. Terap. Indones.*, vol. 1, no. 2, pp. 53–64, 2018, doi: 10.33173/jsikti.12.

E. A. R. and B. L. P. Mehran, "PKT: Secure Port Knock-Tunneling, an enhanced port security authentication mechanism,"," in *IEEE Symposium on Computers & Informatics (ISCI)*, malaysia, 2012, pp. 145–149. doi: doi: 10.1109/ISCI.2012.6222683.