Internasional Journal of Integrative Sciences (IJIS)
Vol.2, No.7, 2023: 971-978

Mikrotik Login Security with Port-Knocking and Brute Force Firewall at PT. Time Excelindo

Iwan Giri Waluyo[1*], Dedy Kurniawan[2]
Pamulang University
Corresponding Author: Iwan Giri Waluyo d02370@unpam.ac.id

A R T I C L E I N F O

Keywords: MikroTik Router, Security, Port-Knocking, Firewall, Brute force

Received : 15 May
Revised : 19 June
Accepted: 18 July

A B S T R A C T

In today's digital era, the use of MikroTik routers is increasingly common in companies, including PT Time Excelindo. However, attacks on MikroTik router logins are a frequent problem, and the company has a need to have a cheap and simple security system. This thesisaims to implement login security techniques using Port-Knocking and brute force firewalls on MikroTik routers at PT Time Excelindo, with the aim of providing solutions that are affordableand easy to implement. This study focuses on identifying the problems faced by PT Time Excelindo, namely repeated attacks against MikroTik router logins. The proposed solution involves implementing a Port- Knocking technique which will hide the login port on the router, so that only legitimate accesswill be allowed after a series of specific requests are made to certain ports. In addition, the firewall will also be activated to block brute force attacks by limiting the number of failed login attempts

DOI: https://doi.org/10.55927/ijis.v2i7.4782
ISSN-E: 2985-9050
https://journal.formosapublisher.org/index.php/ijis

INTRODUCTION

Along with the times, cases of hacking, especially on network devices, are increasingly widespread. The attack on the proxy router is a security problem for IT companies at the ISP service of PT. Time Excelindo. Network security is important in maintaining data integrity and confidentiality in this era of rapid technology. The company experienced a hack on most of the Mikrotik routers used to service customers. This encourages researchers to conduct in-depth studies and implement a more effective Mikrotik login security system using Port-Knocking techniques and BruteForce Firewalls. This research focuses on the implementation of the Mikrotik login security system at PT. Time Excelindo. It is hoped that this research can strengthen network security company and prevent costly attacks.

METHODOLOGY

Study Area

Case studies conducted at PT. Time Excelindo BSD branch, Serpong, South Tangerang, Banten. Is an IT-based company that has been established since 2003, with various business fields ranging from network infrastructure, software development and internet service providers. With quite heterogeneous clients ranging from individual clients, private companies, schools, or government agencies.

Research Methodology

In this study, it was carried out in a descriptive manner, namely research conducted to solve an existing problem. Based on the data collected, the analysis carried out, and interpretation so that the steps carried out in detail include :

Observation Method

The observation method is an activity carried out by directly observing various activities and activities carried out on the object of research carried out at PT. Time Excelindo.

Library Studies

Methods of data collection by collecting and studying reference books and sources related to the research topic.

Interview Method

Interview is a data collection technique through a one-way question and answer process, meaning that the questions come from the interviewee and the answers are given by the interviewer.

Discussion Conclusion

By following several business aspects for the company. The conclusions from the discussions and interviews resulted in findings of problems with the Mikrotik router network security system which is often used to experience repeated hacking incidents time. Therefore, I propose a safe and simple router security system following the results of this interview and discussion. In the form of a port-knocking firewall and brute-force firewall. And it is well-received by the parties concerned to cooperate in the process of implementing this security system that I propose.

RESULT AND DISCUSSION

Flow Design

The network security flow design that will be implemented is as shown in the following activity diagram:

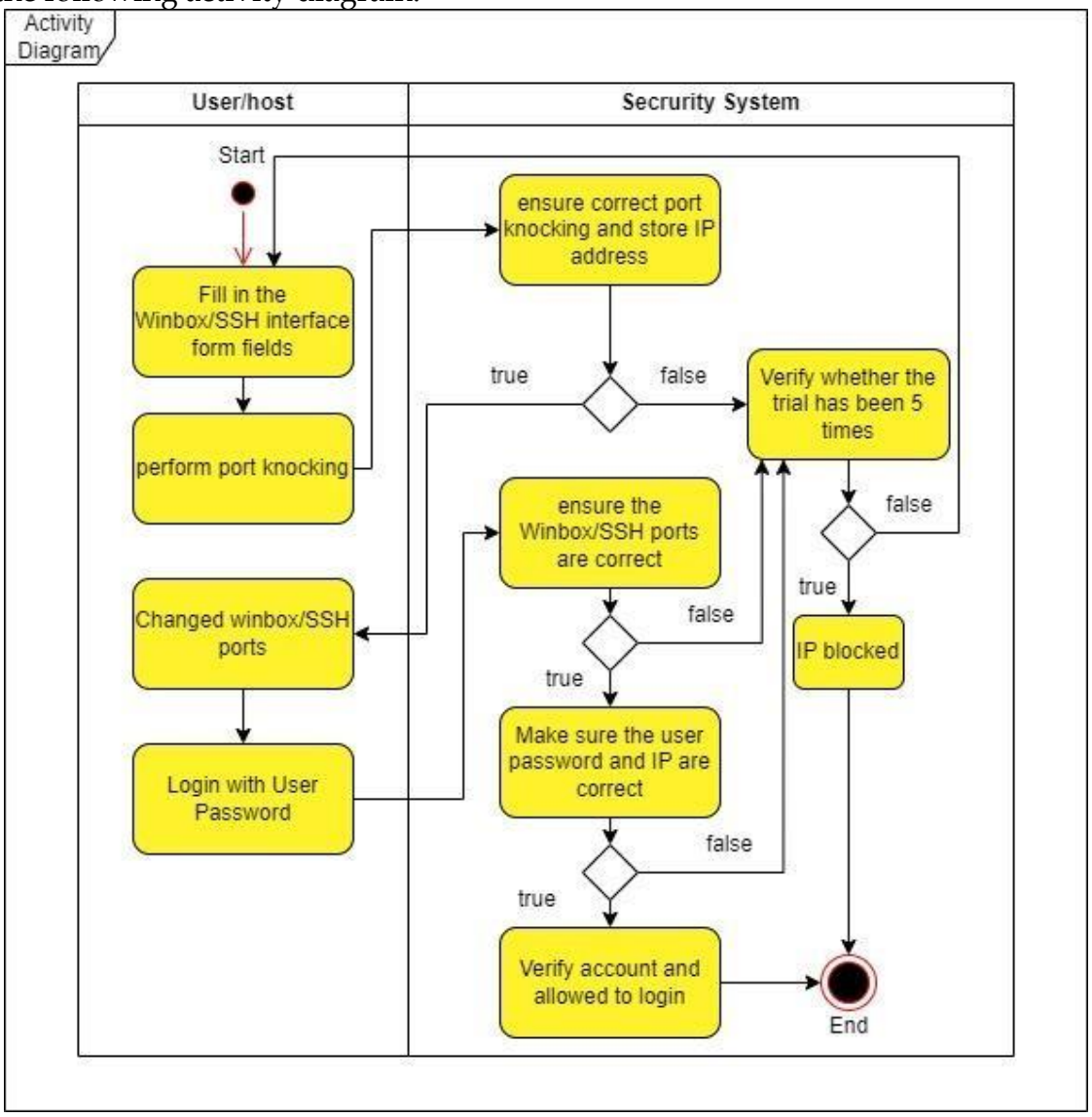

Figure 1. Activity Diagram

Security Flow Scenario

The security flow scenario describes the order in which the login security system is executed. in the form

1) Filter Hosts based on ip access list
2) The host performs port-knocking using certain services.
3) Host enters the destination IP service
4) Input the user password with a certain maximum trial limit

Implementation

In carrying out the implementation the author configures the routerboard and routerOS where the author sets several configurations following from the results of the discussion at the beginning in the form of:

1. Modify the access port on Mikrotik and disable unused ports
   To minimize attacks, the author turns off incoming access ports that are not used in the service list along with changing the port used so that it does not become the default port.
2. Set IPs that are allowed to enter with the Mikrotik system access list
   In this configuration the author determines which IP is allowed to access the proxy device login account
3. Create a Port Knocking configuration
   Configure firewall rule port knocking with specific ports that have been discussed with the team in this study.
4. Disable login access via Mac Address
   Turn off the proxy system feature in the form of a mac-server so that the port-locking system can easily be bypassed.
5. Firewall Login Bruteforce The maximum configuration of attempted access to a certain port that has been determined according to the agreement on the results of the discussion.

Testing

In testing the authors conducted several experiments as shown in the table below;

Table 1. Testing

No.	Test Components	Result	information
1	Login with default winbox port (8291)	failed	success
2	Tried logging in with the changed port without port-knocking	failed	success
3	Tried logging in after port-knocking and the host doesn't match the account access list	failed	success
4	Log in after port knocking by going to the port that matches the IP host listed on the account access list	done	success

Implementation Results

From the results of the implementation, several findings were obtained in the form of a decrease in the access test attack into the Mikrotik routerboard. And also after a series of requirements for access into the router which is considered quite complicated. This makes the router's defense more secure with only people with access and understanding how it works can access the router.

CONCLUSIONS AND RECOMMENDATIONS

The conclusions obtained from the results of this implementation include:

1) The implementation results are sufficient to influence a good security system for Mikrotik routerboard devices.
2) The Mikrotik router security implementation system uses a method that is quite simple to reduce costs and considerable effort.
3) The results of logs and login attempts are enough to prove that this implementation system is an effective preventive measure to prevent Mikrotik router hackers from taking the same action continuously.

The advice obtained from the results of this implementation include:

1. When configuring, it is highly recommended to back up the existing router configuration first.
2. Experiment with unused devices or with vmware emulation. Application to a running routerboard. Ensuring the confidentiality of all vital aspects of router security.
3. In the implementation and development it is expected to pay attention to the basic principles of network security
4. Ensure that the firewall rule sequence is appropriate.

FURTHER STUDY

Routers

According to (Basorudin, et al., 2021) Routers are almost the same as bridges but have advantages, routers will find the best path to send a message based on the destination address and origin address.

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two main functions: it manages traffic between these networks by forwarding data packets to the intended IP address, and it allows multiple devices to use the same Internet connection. There are several types of routers, but most routers pass data between a LAN (local area network) and WAN (wide area network). LAN is a group of connected devices that are limited to a specific geographic area. LAN usually requires one router. In contrast, a WAN is a large network that is spread over a geographical area wide. Large organizations and enterprises operating in multiple locations across the country, for example, would need a separate LAN for each location, which would then connect to other LANs to form a WAN. Because a WAN is distributed over a large area, it often requires multiple routers and switches.

Knocking Ports

According to (Amirudin, 2018) Port-knocking is the concept of hiding remote services in a firewall that allows access to the port only to find out the service after the client has successfully authenticated to the firewall. This can help prevent scanners from knowing what services are currently available on the host and also serve as a defense against zero-day attacks.

Port knocking is a surreptitious method of opening ports externally which, by default, firewalls keep closed. It works by requesting connection attempts to a predefined set of closed ports. With the simple port knocking method, when the correct sequence of port "knocks" (connection attempts) is received, the firewall opens certain ports to allow connections.

Firewalls

According to (Erwin, Ridwansyah, Mugi, 2023) Firewalls are implemented to prevent unauthorized access coming from both within the organization and from outside the organization.

A firewall is a network security system that functions to protect the network from unauthorized access or malware. The firewall monitors and controls data traffic entering and leaving the network based on predetermined security rules.

Firewalls work by managing network traffic, namely checking data packets that pass through the network and checking whether the data packets comply with predetermined security rules or not. If the data packet does not comply with the security rules, the Firewall will block or deny access to the data packet.

Brute Force

According to (Aji R. P., et al., 2023) the loopholes used by hackers are brute force or forced entry by trying every combination of the existing User and Administrator Password.

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. This is a simple but reliable tactic to earn unauthorized access to individual accounts and organizational systems and networks. Hackers try several usernames and passwords, often using computers to test various combinations, until they find the correct login information. The name “brute force” comes from an attacker using very forceful attempts to gain access to a user's account. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic among hackers.

REFERENCES

Aji, R. P., Prayudi, Y., & Luthfi, A. (2023). Analysis of Brute Force Attack Logs toward Nginx Web Server on Dashboard: Improved Log Logging System Using Forensic Investigation Method, 39-48.

Amarudin, A., & Ulum, F. (2018). Network Security Design on Mikrotik Router OS Using the Port Knocking Method.

Amarudin. (2018). Analysis and Implementation of Network Security on Mikrotik Router OS Using the Port Knocking Method

Amarudin. (2018). Analysis and Implementation of Network Security on Mikrotik Router OS Using the Port Knocking Method. (Unpublished thesis). [Name of Univers Rahmatillah, A., Firdaus, A., & Laila, E. (2021). Implementation of Intrusion Prevention System (IPS) on Network Security with Telegram-Based Notifications in Computer Engineering Department. ity/Institution], [Location].

Basorudin, B., Rouza, E., Yanto, B., & Mustafa, S. R. (2021). Design and Implementation of Configuration of Wifi Routers and Wireless Networks with Rb951ui-2nd.

Fran, Afrian. (2019) The Importance of Computer Security.
Mulyanto, Y., Julkarnain, M., & Afahar, A.
J. (2021). Implementation of Port Knocking for Network Security at SMKN 1 Sumbawa Besar.

Setiawan D, Erwin, Ridwansyah, and Raharjo M. 2023. "Next-Generation Firewall Network Security Design Using Routers,

Fortinet At PT. Alodokter Technology Solutions". Integrated Informatics Journal 9 (1):34-39.