Implementation of Port Knocking with Telegram Notifications to Protect Against Scanner Vulnerabilities

Husain , I Putu Hariyadi , Kurniadin Abd. Latif , Galih Tri Aditya
Universitas Bumigora, Mataram, Indonesia

Article Info

Article history:

Received October 11, 2023
Revised November 18, 2023
Accepted November 28, 2023

Keywords:

Mikrotik Router
Port Knocking
Telegram Notification
Vulnerability

ABSTRACT

The opening of the service port on the Mikrotik router provides an opening for hackers to enter the Mikrotik service to access the router illegally. This research aimed to close certain ports that are gaps for hackers and uses port knocking and telegram bots. The Telegram bot was used as a message notification to managers in real-time to provide information that occurs when the vulnerability scanning process is carried out to find and map weaknesses in the network system. Searching for weaknesses also includes looking for open router service ports such as ports 22, 23, 80, and 8291. This research used the Network Development Life Cycle method, which started from analysis design and prototype simulation to implementation. The research results after testing were able to secure local network service ports against vulnerability scanners on routers using the port knocking method, and testing attack schemes carried out from each scheme could run well on the router's local network and obtain notifications via telegram bots in real time to administrators. This research contributes to administrators' ability to secure networks so irresponsible people do not easily infiltrate them.

Corresponding Author:

Husain, +6281805745587
Faculty of Engineering and Computer Science Study Program,
Universitas Bumigora, Mataram, Indonesia,
Email: husain@universitasbumigora.ac.id

How to Cite:
H. Husain, I. P. Hariyadi, K. Latif, and G. Aditya, ”Implementation of Port Knocking with Telegram Notifications to Protect Against Scanner Vulnerabilities”, *MATRIK: Jurnal Managemen,Teknik Informatika, dan Rekayasa Komputer*, Vol. 23, No. 1, pp. 215-228, Nov, 2023.

1. INTRODUCTION

The current development of computer network technology can be seen very rapidly [1]. Along with the speed of technological development, several things must be considered in a system, both in system management and security [2]. This also applies to the computer network management sector, namely the monitoring process and the computer network's security so that it is protected from irresponsible attacks [3]. Statistics show that, based on a report from Check Point Research, global cyberattacks increased by 38% in 2022 compared to 2021, with 83% of organizations experiencing at least one data breach in that year [4, 5]. From national data, based on reports from the National Cyber and Crypto Agency (BSSN), in 2022, there will be a total of 399 alleged cyber incidents, with the highest number of alleged incidents being data breaches [6], including cyber-attacks that have attracted attention. , one of which is the data breach uncovered by hacker Bjorka. Cyber attacks occur due to weaknesses in application security that can be exploited to commit criminal acts [7]. Security is a major challenge in computer network infrastructure because of potential threats from internal or external parties who intend to damage, steal, or change data on the system that we have built [8]. These threats can be viruses, malware, hacker attacks, or information leaks from irresponsible people [9].

Some recent works related to previous research are as follows: I Pali and R Amin [10] titled PortSec: Securing Port Knocking System using Sequence Mechanism in SDN Environment. This research describes a port knock sequence-based communication protocol in a software-defined network (SDN). The results of this research provide better management by separating the control plane and the data plane. What makes our research different is using Mikrotik, Vulnerability Scanner, and Telegram notifications. R, Rosihan Muin, Yasir 2022 [11] with the title MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method. This research produces network security on MikroTik Router devices that can prevent threats and attacks. What differs from our research is that it uses Knolng Port and Telegram notifications. Mursyidah, Husaini, et.al [12] with the title Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS. What makes our research different is that it uses a Vulnerability Scanner and Telegram notifications. This research is important to carry out. Apart from being able to contribute to society by overcoming threats or attacks on computer network systems and contributing scientifically by referring to previous research, no one has implemented network security, which includes using proxies, vulnerability scanners, port knocking, and telegram notifications.

A router is a network device that connects users to the internet [13, 14]. The completeness of a router's features does not rule out the possibility that someone seeking personal gain can infiltrate the network through open ports on the service used [15, 16].

Implementation of a computer network security system using the port knocking method using a development research method using a 4D model development approach (four-D model) [17, 18]. The result is a network security system that secures a Mikrotik router using the port-knocking method. It functions as an alternative for maintaining security in a computer network, preventing attackers from accessing the Mikrotik router and allowing administrators to determine who they are. Only those who have access rights can enter certain ports [19]. Telegram serves as a notification tool accessible from any location, facilitating administrators in promptly detecting and responding to potential attacks [20]. When an attack occurs, the mechanism for an attack on Telegram notifications is that the router's firewall rule will close service ports 22, 23, 80, and 8291. Then, the on-event feature on the router will send notifications via the Telegram bot so administrators can easily monitor network security and anticipate attacks happening even worse [21]. The use of port knocking minimizes server attacks [22, 23]. The port security carried out was on ports 22, 23, 80, and 8291. The results obtained were differences without knocking and access using knocking, and it was found that the port security successfully opened ports that were closed on the firewall. As a liaison between the administrator and the router, notification is needed so that the administrator can find out if a scanner vulnerability occurs [24, 25].

The mechanism used in port knocking is that when an attack occurs, if the rules created on the firewall do not comply with the provisions, the firewall will automatically block/blacklist the attacker's Internet Protocol (IP) address. To open access, the service port must be opened again following the provisions made in the firewall rules. This process is called port knocking [26]. The mechanism for an attack on Telegram notifications when an attack occurs is that the rules on the router's firewall will close service ports 22, 23, 80, and 8291. Then, the on-event feature on the router will send notifications via the Telegram bot so administrators can easily monitor network security and anticipate an even worse attack.

Network security using port-knocking and telegram notifications as information that the administrator more easily knows is a suggested solution for securing Mikrotik routers, monitoring networks when vulnerability scanner attacks occur, and limiting access to ports on the network. Port scanning detection is implemented so that the network being built can detect and avoid dangerous vulnerability scanner attacks on the network and immediately provide a warning to the administrator. The use of port knocking is done to open access to ports that have been closed by firewalls on network devices, which is done by sending packets in the form of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP). If the connection sent by the host complies with the knocking rules that have been applied, the rules on the firewall will provide access to the port that has been blocked [6]. Using bots in the Telegram application conveys information that will be sent from the router during an attack and then sent to Telegram. A simple mechanism/scheme when an attack occurs when a vulnerability scanner occurs, the firewall will close ports 22, 23, 80, and 8291, then the telegram bot will send specific notifications such as the name of the router device, Internet Protocol Address (IP Address), and the time the vulnerability scanner occurred. After receiving notification of an attack, the administrator will open closed ports on the firewall by implementing port knocking. This mechanism and solution are expected to reduce the level of risk for malicious elements, especially on networks that want to start committing crimes by scanning open ports via Mikrotik devices. With this solution, network administrators will know more quickly through notifications from telegram bots and port knocking that is configured and implemented.

2. RESEARCH METHOD

In this research, the methodology applied in the work process refers to the Network Development Life Cycle (NDLC) method. NDLC is a method used to design or develop a computer network and allows monitoring of the system being created or developed [7]. The NDLC method has six stages, which will serve as a guide in implementing NDLC. The six stages are Analysis, Design, Prototype, Implementation, Monitoring, and Management. This research only reached the implementation stage. The stages involved in the NDLC method are shown in Figure 1.

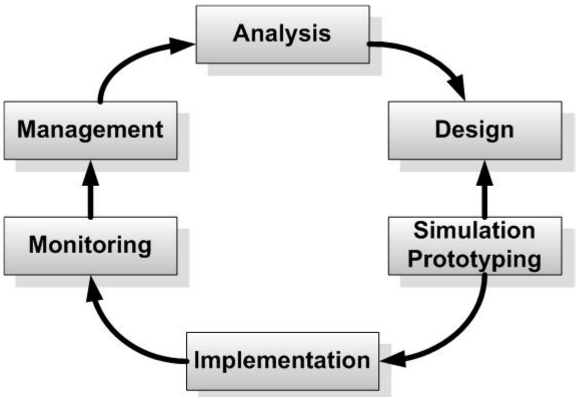


Figure 1. Stages of the network development life cycle method

Activities at each stage of the research are in the analysis stage. The analysis stage is carried out to analyze needs for problems that arise, devices to be used, and software. Design Stage: Design can take the form of designing network topology structures, designing data access, and designing wiring layouts. Simulation Stage: In the simulation stage, a design will be carried out as a simulation with the help of special tools such as Visio or Packet Tracer. This is intended to create an initial picture of the research that will be built. At this stage, an attack scheme will also be created using 3 schemes, namely not activating telegram notifications and port knocking as a safeguard for ports 22, 23, 80, and 8291 in the event of a scanner vulnerability, activating telegram notifications in the event of a scanner vulnerability but not implementing port knocking and activate telegram notifications and port knocking if a scanner vulnerability occurs. Implementation Stage: In the Implementation stage, everything planned will be implemented starting from the design stage, and implementation is the stage that will determine the success/failure of the research to be carried out. At this stage, the author will implement an action plan by configuring the Mikrotik router device on the local network using the port knocking method and port scanning detection on the Mikrotik router. The tools and software used include laptops, Winbox applications, Putty applications, and Nmap tools.

3. RESULT AND ANALYSIS

At the analysis stage, preliminary study analysis, literature study, data analysis stage, observation, problem formulation related to network hardware requirements such as routers, access points, and laptops, and several network software requirements are carried out.

3.1. Device Requirements Analysis

The hardware requirements used during this research are as follows:

Table 1. Router Hardware

No	Description	Specification
1	Category	Hap
2	Code	RB-941-2nD
3	Processor	650Mhz
4	Port Fast Ethernet	4
5	Wireless	2.4Ghz (802.11b/g/n)
6	Antenna	Internal Dual-Chain 2 x 1.dbi
7	Memory	32MB
8	Storage	16MB
9	Operating system	RouterOS

Table 1 shows the router device specifications, including category code, processor, fast port, internet, wireless, antenna, memory, and storage.

Table 2. Access Point Hardware

No	Description	Specification
1	Device Name	TP-Link
2	Version Code	TL-WR840N
3	WiFi Speed	300 Mbps
4	Power	9 V = 0.6 A
5	Wireless	2.4Ghz (802.11n)
6	Antenna	Dual Antena
7	Port	4 Port LAN + 1 Port WAN

Table 2 shows the Access Point specifications used by administrators to develop local network security, such as Device Name, Version Code, WiFi Speed, Power, Wireless, Antenna, and Port.

Table 3. Software Specifications

No	Description	Fungsi
1	Telegram	Software to receive notifications when a scanner vulnerability occurs
2	Winbox 3.31	Software for accessing Mikrotik Router configuration
3	Nmap 7.70	Software for vulnerability scanners
4	PuTTY 0.77	Software for port knocking

Table 3 shows the software requirements used during the research process, with each different function such as Telegram, Winbox 3.31, Nmap 7.70, PuTTY 0.77.

3.2. Topology Design and Internet Protocol Address (IP Address)

A vulnerability scanner simulation that approaches the problem and appropriate characteristics then applies the existing network topology in one case at the Sunset House Gili Meno hotel on the island of Gili Meno. By applying the topology at that location, it is hoped that it can be used for its application so that The running network does not experience network security problems and can make things easier for network administrators who work at the hotel and can make visitors secure in their privacy. The internet source used is the ISP provided by I-Connet. The topology involves one router device, one wireless distribution device (access point), a UTP RJ-45 cable, and two laptops (as a simulation of an attacker and administrator). Flow chart of the research carried outsimulation/scheme to be carried out for the attack and implementation of the attack solution.

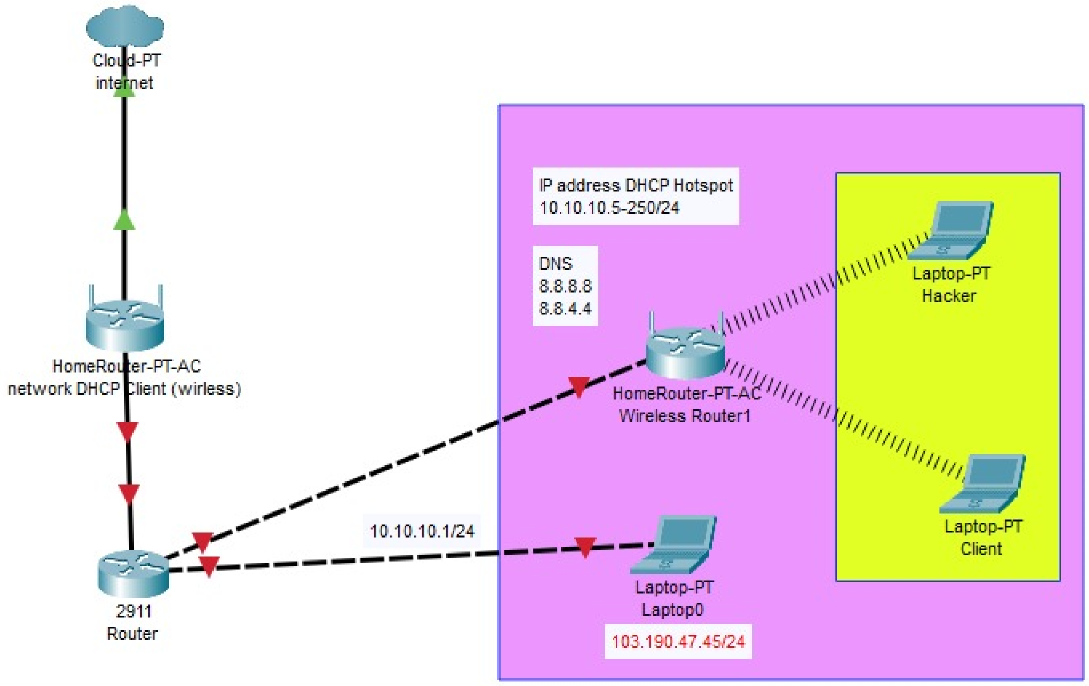


Figure 2. Network topology design

In the network topology design, the internet network will be taken from a modem connected directly to a fiber-optic cable provided by the Internet Service Provider (ISP) I-Connet. The IP address for network connections uses an IP address with Dynamic Host Configuration Protocol (DHCP) client mode on the router used via the IP address obtained with DHCP client mode. After the router gets an IP address for internet access, then an IP address on Ether3 for the laptop/device which is used as a port for configuration, the IP address set for Ether3 is 103.190.47.45/24, then create a DHCP server mode with the range 103.190.47.46.

Table 4. Network Addressing Design

No	Perangkat	Interface	Ip Address	Gateway	DHCP
1	Router	Ether1	10.0.2.0/24	-	YES
		Ether2	10.10.10.1/24	-	YES
		Ether3	103.190.47.45/24	-	YES
2	Access Point	Ether1	10.10.10.253/24	10.10.10.1	YES
3	Laptop Administrator	Ethernet	103.190.47.46/24	103.190.47.45	YES
4	Laptop Attacker	Ethernet	10.10.10.254/24	10.10.10.1	YES
6	Laptop Client	Ethernet	10.10.10.94/24	10.10.10.1	YES

Table 4 shows the network addressing used on the device, including the IP address, gateway, and status of whether the interface uses Dynamic Host Configuration Protocol (DHCP) Server/Client addressing.

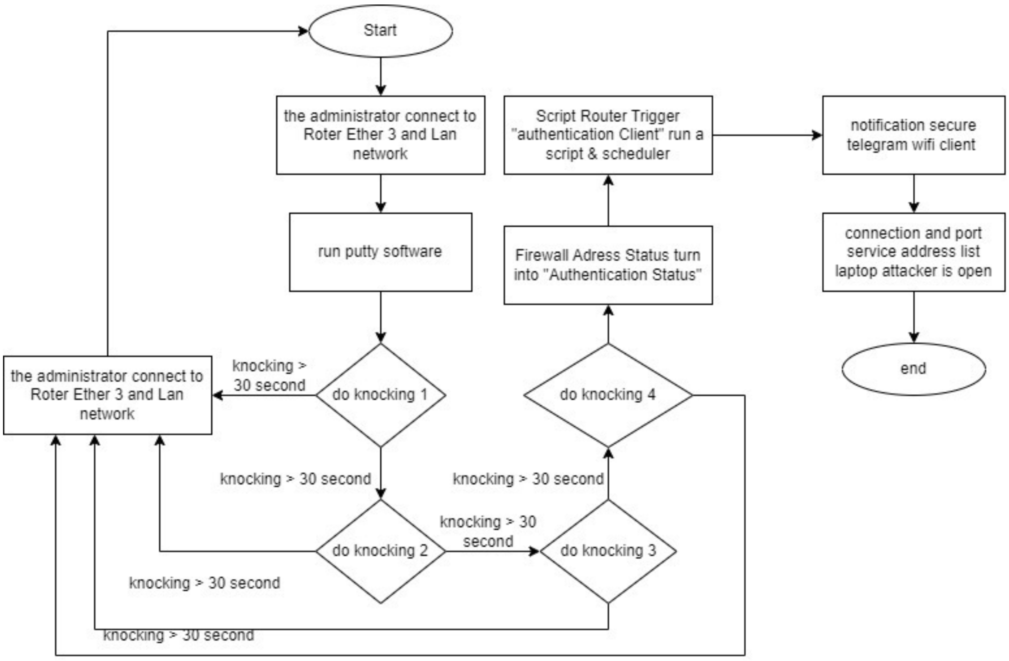

Start
the administrator connect to Roter Ether 3 and Lan network
run putty software
do knocking 1
knocking > 30 second
the administrator connect to Roter Ether 3 and Lan network
knocking > 30 second
do knocking 2
knocking > 30 second
knocking > 30 second
do knocking 3
knocking > 30 second
knocking > 30 second
do knocking 4
Firewall Adress Status turn into "Authentication Status"
Script Router Trigger "authentication Client" run a script & scheduler
notification secure telegram wifi client
connection and port service address list laptop attacker is open
end

Figure 3. Port knocking system design

Figure 3 above shows how the port-knocking process system works. When there is a ”port scanner” address list, the internet connection and service port on that IP address will automatically be closed, which is triggered because of the vulnerability scanner process in accordance with the configured firewall rules. To open closed connections and service ports, a port-knocking process is required. The administrator will use PuTTY software to perform knocking in 4 steps with a time interval of 30 seconds for each knocking stage. The first knock will be carried out on port 1000. If the knock 1 process takes more than 30 seconds, then the knock 1 address list will be reset, and there will only be a ”port scanner” address list. If knock 1 is successful in less than 30 seconds, then you can continue the knock 2 process, and so on, until the fourth knocking process is successful. After the fourth knocking process is successful, the ”authenticated client” address list will appear, and when the address list appears, it will be a trigger for the script and Scheduler features to run; when the script is running there is a command to send notification information that the WiFi client is safe to Telegram via BOT Token according to the Chat ID entered, that way the Scheduler will run the script, and the script will execute the command. When the ”authenticated client” address list is triggered, the firewall will automatically open the internet connection and the service ports previously closed in the ”port scanner” address list.

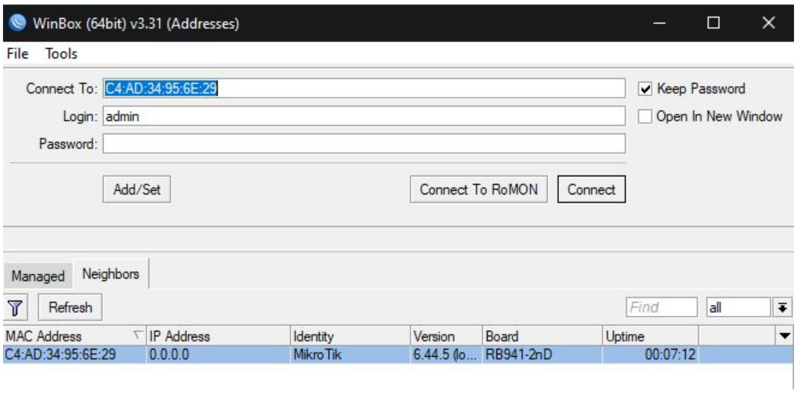
3.3. Implementation Stage

Implementation stage: everything planned will be implemented starting from the design stage. Implementation is the stage that will determine the success/failure of the research to be carried out. At this stage, the author will implement an action plan by configuring the Mikrotik router device on the local network using the port knocking method and port scanning detection on the Mikrotik router. The tools and software used include laptops, Winbox applications, Putty applications, and Nmap tools with the following process:

Connecting a laptop with a Mikrotik router device. Connect the RJ-45 cable to the proxy router, which the ISP connects to an internet connection. Configure the IP address of the Mikrotik router with the Winbox application. Check open service ports (Winbox, Ssh, Telnet, and Webfig) before carrying out port scanning detection and port knockingimplementing port scanning detection and firewall configuration for sending notifications to Telegram bots. Create a Telegram bot so it can connect to the Mikrotik router. Check open service ports (Winbox, Ssh, Telnet, and Webfig) after carrying out port scanning detection and port knockingimplementation of port knocking and closing ports and notifications on Telegram by creating rules on the firewall. Carry out authentication tests on the configured firewall. Validate the port that will be tapped. If the port tapped is correct, you can access existing services; if it is wrong, the process will be repeated (9). Perform data analysis.

1. Installation and Configuration Results

This section discusses the results of the installation and configuration of the hardware and software used, configuration verification, and several test scenarios. The test scenarios carried out include carrying out port knocking to the Mikrotik router to access services that were initially closed and carrying out attacks related to vulnerability scanners. These two test scenarios will trigger a notification message to the specified Telegram group if the client has successfully carried out port knocking and when an attack is detected in the form of port scanning.



Connect To: C4:AD:34:95:6E:29
Login: admin
Password:
☑ Keep Password
□ Open In New Window
all

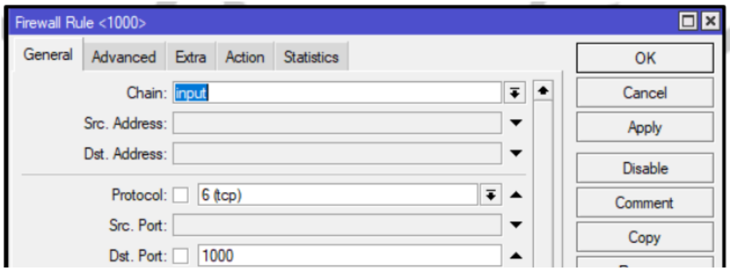
MAC Address	IP Address	Identity	Version	Board	Uptime
C4:AD:34:95:6E:29	0.0.0.0	MikroTik	6.44.5 (lo...	RB941-2nD	00:07:12

Figure 4. Login using winbox

Figure 4 shows the Winbox interface to enter the Mikrotik interface using the MAC address number, obtained automatically when the computer device is physically connected to the Mikrotik router. The following is the configuration contained in the Winbox interface. Connect To = Enter the Router IP or MAC Address of the Router we want, Login = Enter your login username and password to your router (default = admin),Password = Enter the password for the router you want to connect to (default not filled in),Add/Set = To save information, change Router IP/MAC, Login, and Password to the Managed menu so that when you connect to the router in the future, you do not need to type it again,Connect = To connect to our router,Managed = Results of the saved Router IP/MAC list, Login, Password,Neighbors = A list of routers directly connected to our router will appear.

2. Firewall Configuration

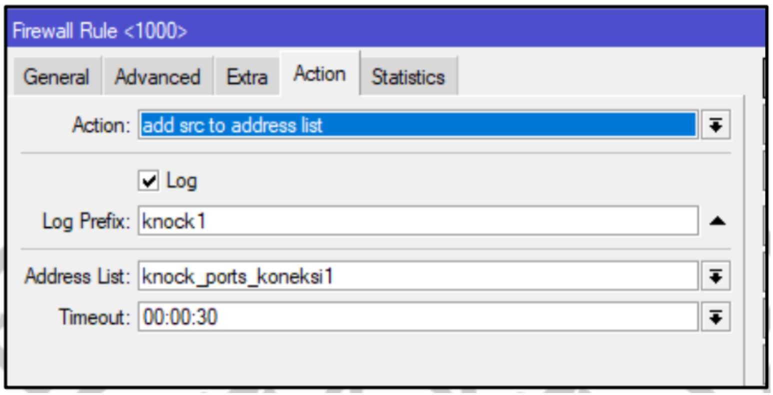
There are 2 (two) types of rules on the IP Firewall Filter from the MikroTik router: rules for carrying out port knocking to open closed connections or services and rules for blocking vulnerability scanners such as port scanners. The port knocking rule to open closed connections or services on the MikroTik router is made with the provision that the client must knock 5 (five) destination port numbers in sequence, namely 1000, 1500, 3000, 4000, and 5000, with the destination transport protocol ”6 (TCP)”, as seen in Figure 5.



Chain: input
Src. Address:
Dst. Address:
Protocol: □ 6 (tcp)
Src. Port:
Dst. Port: □ 1000

Figure 5. Firewall rule for port knocking general tab

On the General tab of the IP Firewall Rule, several parameters are set, including Chain with the value ”input” to filter traffic entering the MikroTik router, Protocol with the value ”6 Transmission Control Protocol/Internet Protocol (TCP)” to determine the transport method to be filtered, namely Transmission Control Protocol (TCP), etc. Port is used to filter ports with a destination number, for example, 1000. Meanwhile, on the Action tab, set the Action parameter with the value ”add src to address list” to add the source IP address of the client to a new Address List with the name ”knock_ports_koneksi1” with a timeout time of 30 seconds, as seen in Figure 6.


Firewall Rule <1000>

Action: add src to address list

☑ Log

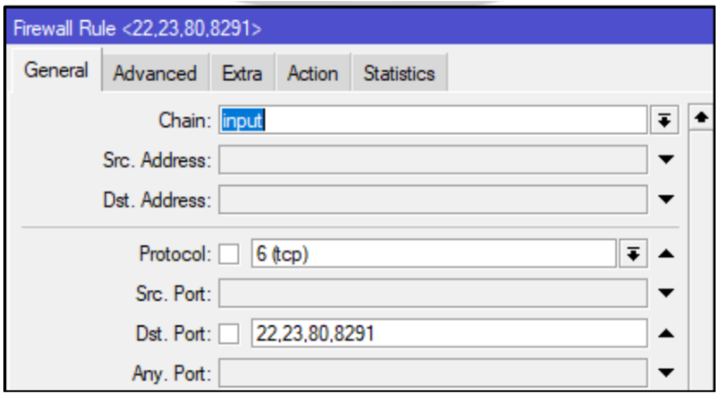
Log Prefix: knock1

Address List: knock_ports_koneksi1

Timeout: 00:00:30

Figure 6. Firewall for port knocking tab action

Apart from that, this tab also activates the Log feature to record this activity in the router log and sets the Log Prefix parameter with the value ”knock1” to mark the saved log, making it easier to search the log. Finally, set the rule’s Comment with the value ”Port Knocking Connection: Step 1” to differentiate it from other rule entries. Meanwhile, the IP Firewall Filter rules from the MikroTik router close ports 22, 23, 80, and 8291 when port scanning is detected, as shown in Figure 7.


Firewall Rule <22,23,80,8291>

Chain: input

Src. Address:

Dst. Address:

Protocol: □ 6 (tcp)

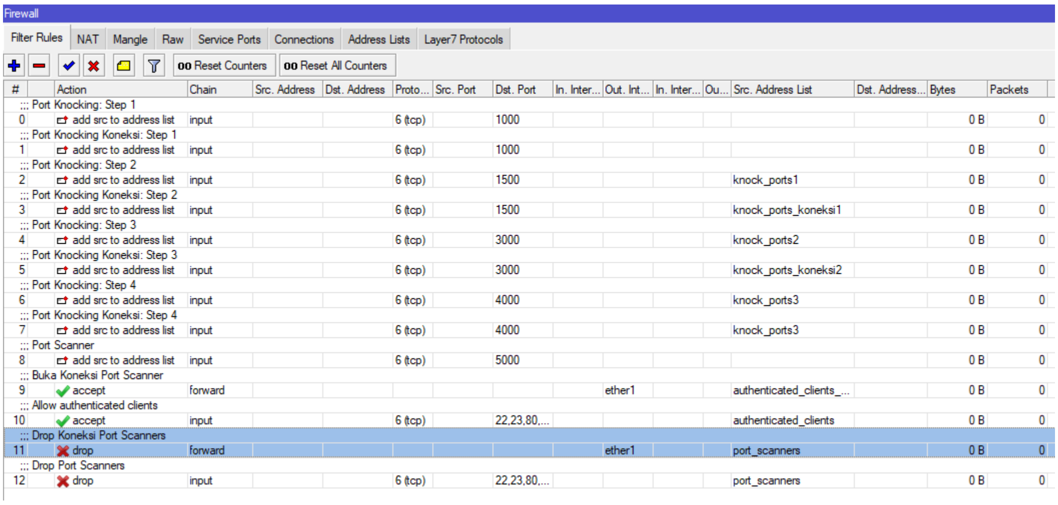
Src. Port:

Dst. Port: □ 22,23,80,8291

Any. Port:

Figure 7. Firewall rule to block port scanning

On the General tab of the IP Firewall Rule, several parameters are set, including Chain with the value ”input” to filter traffic entering the MikroTik router, Protocol with the value ”6 (TCP)” to determine the transport method to be filtered, namely Transmission Control Protocol (TCP), etc. Port is used to filter ports with destination numbers 22, 23, 80 8291. Meanwhile, settings are made for the Src parameter on the Advanced tab. Address List has the value ”port_scanners” so that when a client performs port scanning, the IP address of that client will be added to the Address List with that name. On the other hand, on the Action tab, set the Action parameter with the value ”drop” to reject connections from the client’s source IP address and activate the Log feature to record this activity in the router log. Apart from that, you can also set the Log Prefix parameter with the value ”Port Scanning Blocked:” to mark the saved logs, making it easier to search the logs and send notification messages to Telegram. Finally, set the rule’s Comment with the value ”Drop Connection Port Scanners” to differentiate it from other rule entries. The results of the overall firewall rules settings are shown in Figure 8.



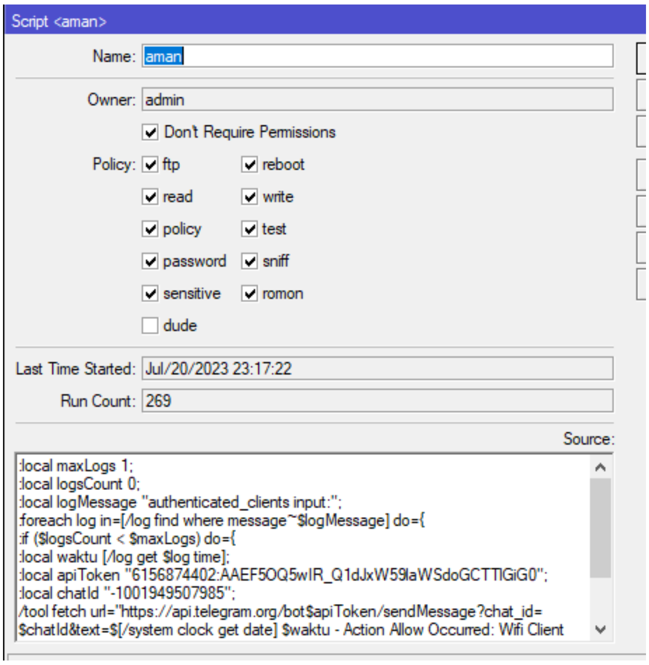
#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Ou...	Src. Address List	Dst. Address...	Bytes	Packets
;;; Port Knocking: Step 1																
0		add src to address list	input			6 (tcp)		1000							0 B	0
;;; Port Knocking Koneksi: Step 1																
1		add src to address list	input			6 (tcp)		1000							0 B	0
;;; Port Knocking: Step 2																
2		add src to address list	input			6 (tcp)		1500					knock_ports1		0 B	0
;;; Port Knocking Koneksi: Step 2																
3		add src to address list	input			6 (tcp)		1500					knock_ports_koneksi1		0 B	0
;;; Port Knocking: Step 3																
4		add src to address list	input			6 (tcp)		3000					knock_ports2		0 B	0
;;; Port Knocking Koneksi: Step 3																
5		add src to address list	input			6 (tcp)		3000					knock_ports_koneksi2		0 B	0
;;; Port Knocking: Step 4																
6		add src to address list	input			6 (tcp)		4000					knock_ports3		0 B	0
;;; Port Knocking Koneksi: Step 4																
7		add src to address list	input			6 (tcp)		4000					knock_ports3		0 B	0
;;; Port Scanner																
8		add src to address list	input			6 (tcp)		5000							0 B	0
;;; Buka Koneksi Port Scanner																
9		✓ accept	forward							ether1			authenticated_clients_...		0 B	0
;;; Allow authenticated clients																
10		✓ accept	input			6 (tcp)		22,23,80,...					authenticated_clients		0 B	0
;;; Drop Koneksi Port Scanners																
11		✖ drop	forward							ether1			port_scanners		0 B	0
;;; Drop Port Scanners																
12		✖ drop	input			6 (tcp)		22,23,80,...					port_scanners		0 B	0

Figure 8. Firewall rules results

It can be seen that there are 13 (thirteen) rules created, including rules related to port knocking with ID (♯) 0 to 7, rules for adding the client's IP address to the Address List, which carries out port scanning with ID 8, rules for opening a port scanner connection for the client those authenticated with ID 9, rules to allow access to ports 22, 23, 80 and 8291 for clients authenticated with ID 10. Meanwhile, rules with IDs 11 and 12 are used to block or deny connections from clients who carry out vulnerability scanners or port scanning.

3. Script

There are 2 (two) scripts created to send notifications from the MikroTik router to Telegram, namely a script with the name "safe" when the client has carried out port knocking so that it can access network services and a script with the name "unsafe" when an attack occurs in the form of a vulnerability scannera snippet of the results from creating a "safe" script, as shown in Figure 9.



Name: aman

Owner: admin

☑ Dont Require Permissions

Policy: ☑ ftp ☑ reboot
☑ read ☑ write
☑ policy ☑ test
☑ password ☑ sniff
☑ sensitive ☑ romon
☐ dude

Last Time Started: Jul/20/2023 23:17:22

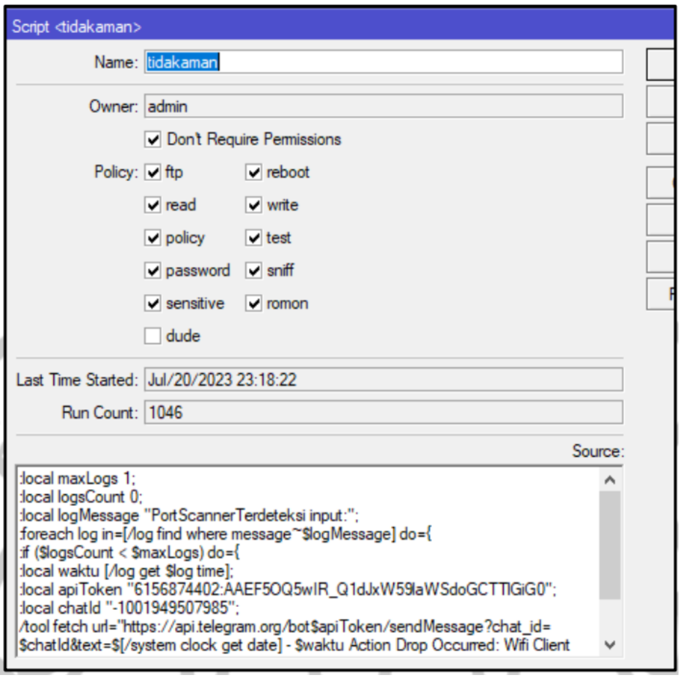
Run Count: 269

Source:

```
:local maxLogs 1;
:local logsCount 0;
:local logMessage "authenticated_clients input:";
:foreach log in=[/log find where message~$logMessage] do={
:if ($logsCount < $maxLogs) do={
:local waktu [/log get $log time];
:local apiToken "6156874402:AAEF5OQ5wIR_Q1dJxW59laWSdoGCTTlGiG0";
:local chatId "-1001949507985";
/tool fetch url="https://api.telegram.org/bot$apiToken/sendMessage?chat_id=
$chatId&text=$[/system clock get date] $waktu - Action Allow Occurred: Wifi Client
```

Figure 9. Secure script snippet

The value in the Source: parameter of this script is used to retrieve and process logs from the MikroTik router containing the prefix ”authenticated_clients input:” and send them to Telegram. To be sent, notification messages require an API Token and chatId from the Telegram group to which the message is sent. Sending messages from the MikroTik router can be done by executing the /tool fetch command with a URL parameter containing the Telegram API address to send the message. The content of the message sent to the chat group contains the time from the system, the time from the log, and the notification text ”Action Allow Occurred” WiFi Client is Secure [Authenticated Clients].” Meanwhile, a snippet of the results from creating an ”unsafe” script, as shown in Figure 10. The value in the Source: parameter from this script is used to retrieve and process logs from the MikroTik router containing the prefix ”PortScannerDetected input:” when a scanner vulnerability occurs and send them to Telegram. To be sent, notification messages require an API Token and chatId from the Telegram group to which the message is sent.



Name: tidakaman

Owner: admin

☑ Don't Require Permissions

Policy: ☑ ftp ☑ reboot
☑ read ☑ write
☑ policy ☑ test
☑ password ☑ sniff
☑ sensitive ☑ romon
☐ dude

Last Time Started: Jul/20/2023 23:18:22

Run Count: 1046

Source:

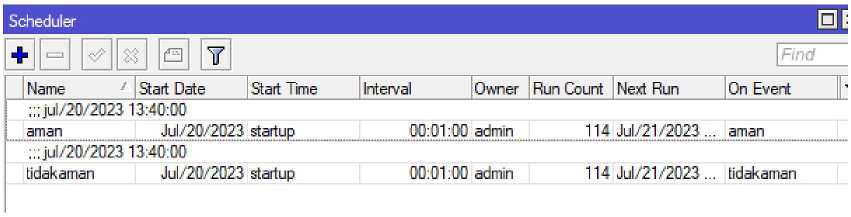
```
:local maxLogs 1;
:local logsCount 0;
:local logMessage "PortScannerTerdeteksi input:";
:foreach log in=[/log find where message~$logMessage] do={
:if ($logsCount < $maxLogs) do={
:local waktu [/log get $log time];
:local apiToken "6156874402:AAEF5OQ5wIR_Q1dJxW59laWSdoGCTTlGiG0";
:local chatId "-1001949507985";
/tool fetch url="https://api.telegram.org/bot$apiToken/sendMessage?chat_id=
$chatId&text=$[/system clock get date] - $waktu Action Drop Occurred: Wifi Client
```

Figure 10. Insecure script snippet

Sending messages from the MikroTik router is also done by executing the /tool fetch command with a URL parameter containing the Telegram API address for sending messages. The content of the message sent to the chat group contains the time from the system, the time from the log, and the notification text ”Action Drop Occurred” WiFi Client Is Unsafe [Port Scanning].”

4. Scheduler

The results of creating a scheduler on the MikroTik router to schedule the execution of ”safe” and ”unsafe” scripts are shown in Figure 11.



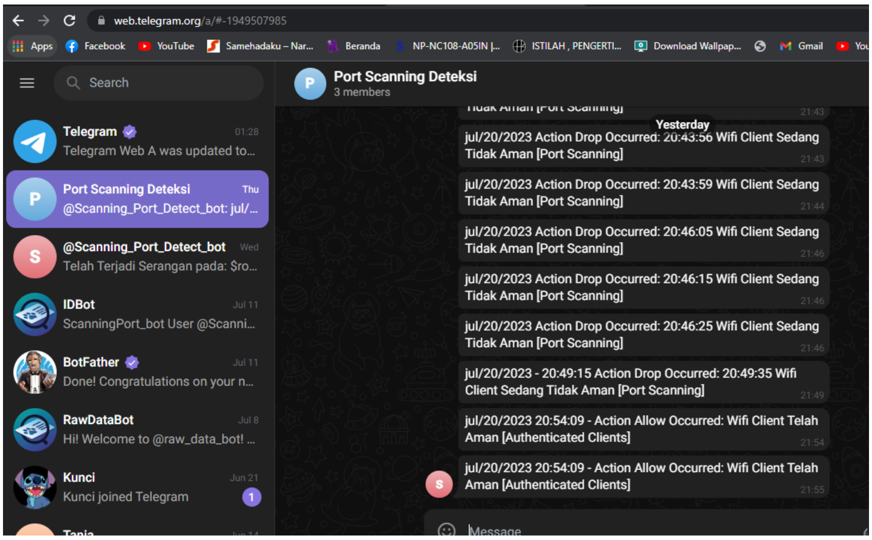
Name	Start Date	Start Time	Interval	Owner	Run Count	Next Run	On Event
;;; jul/20/2023 13:40:00							
aman	Jul/20/2023	startup	00:01:00	admin	114	Jul/21/2023 ...	aman
;;; jul/20/2023 13:40:00							
tidakaman	Jul/20/2023	startup	00:01:00	admin	114	Jul/21/2023 ...	tidakaman

Figure 11. Scheduler results

It can be seen that there are 2 (two) schedulers created, namely with the name ”safe” to trigger the execution of scripts with the name ”safe” regarding secure connections and with the name ”unsafe” to trigger the execution of scripts with the name ”unsafe” regarding unsafe connections according to the value of the On Event parameter. Both schedulers start to be triggered at startup according to the value of the Start Time parameter and are executed every minute as indicated by the value of the Interval parameter, which is 1 minute.

5. Telegram Notifications

The administrator received notification messages on Telegram when testing an attack on the MikroTik router, as shown in Figure 12.



Telegram 01:28
Telegram Web A was updated to...

Port Scanning Deteksi Thu
@Scanning_Port_Detect_bot: jul/...

@Scanning_Port_Detect_bot Wed
Telah Terjadi Serangan pada: $ro...

IDBot Jul 11
ScanningPort_bot User @Scanni...

BotFather Jul 11
Done! Congratulations on your n...

RawDataBot Jul 8
Hi! Welcome to @raw_data_bot! ...

Kunci Jun 21
Kunci joined Telegram

jul/20/2023 Action Drop Occurred: 20:43:56 Wifi Client Sedang Tidak Aman [Port Scanning] 21:43

jul/20/2023 Action Drop Occurred: 20:43:59 Wifi Client Sedang Tidak Aman [Port Scanning] 21:44

jul/20/2023 Action Drop Occurred: 20:46:05 Wifi Client Sedang Tidak Aman [Port Scanning] 21:46

jul/20/2023 Action Drop Occurred: 20:46:15 Wifi Client Sedang Tidak Aman [Port Scanning] 21:46

jul/20/2023 Action Drop Occurred: 20:46:25 Wifi Client Sedang Tidak Aman [Port Scanning] 21:46

jul/20/2023 - 20:49:15 Action Drop Occurred: 20:49:35 Wifi Client Sedang Tidak Aman [Port Scanning] 21:49

jul/20/2023 20:54:09 - Action Allow Occurred: Wifi Client Telah Aman [Authenticated Clients] 21:54

jul/20/2023 20:54:09 - Action Allow Occurred: Wifi Client Telah Aman [Authenticated Clients] 21:55

Figure 12. Telegram notification results

The notification message contains information including the time and actions taken, both drop and allow. One of the notification messages received in the Telegram group showed that port scanning activity had occurred and was dropped on July 20 2023, at 20:43:56, marked with the message ”Action Drop Occurred”. On the other hand, port knocking activity occurred by a validly authenticated client on July 20, 2023, at 20:54:09, marked with the message ”Action Allow Occured.”

3.4. Test Result Indicators

The test results indicators can be summarized based on the trials carried out, as shown in Table 12.

Table 5. Test Result Indicators

No	Indicator	Result
1	Nmap Attack.	Known by administrators via Telegram Notifications and via Logs.
2	Activity log	Record Log Prefix goes into the system log.
3	Scanner vulnerability gaps	The port appears open and then is closed by the firewall.
4	Open closed connections and ports with PuTTY knocking ports	Closed connections and ports were successfully reopened at the attacker’s IP address.
5	Notifications on Telegram against attacks	It was well received.
6	Notification: The router is safe against attacks.	It was well received.
7	Port knocking sequence.	Success must be in sequence from knocking port 1000 to 4000, with time limits according to the provisions.
8	Attempt 25 consecutive attacks.	The Scheduler and Script worked well, and Telegram managed to receive all attack notifications.

Based on Table 5, information can be obtained that there are 8 (eight) test indicators, and the overall test results for each indicator went well. The system detected 25 (twenty-five) consecutive attacks and recorded them in the log, and the administrator received notification regarding the attack via Telegram. This indicates that the system developed has worked as expected.

4. CONCLUSION

This research concludes that the implementation of port knocking on the MikroTik router firewall feature and attack monitoring can run well based on attack test results indicators. Testing is carried out by testing attacks with several indicators, such as attacks from Nmap. Administrators can find this information through Telegram notifications and system logs. The firewall detects attacks and closes ports 22, 23, 80, and 8291. On the Vulnerability Gap indicator, the port scanner appears open, then closed by the firewall. Next, on the Open connection and close port indicator with PuTTY knocking port, the result is that the closed connection and port have been successfully reopened at the attacker's IP address. Next, it will automatically drop the IP Address on the ether2 router, and to open it, you need to tap ports 1000, 1500, 3000, and 4000, with a time limit of 30 seconds. The administrator receives a telegram notification regarding attack information and contains information about whether the device is safe/unsafe on its network (port scan), including the time and date of the attack. The attack testing carried out 25 times for notification testing has gone well, without a single missed notification. Monitoring with Scheduler and Telegram can help network administrators monitor if an attack occurs without having to log into the local network. The test results show that notifications are sent to Telegram when an attacker's port scan on a router contains information about secure network devices/unsecure networks and the time and date of the attack or secure network. This research has implications for improving network security and contributing to network management in overcoming interference from irresponsible people who can damage computer network systems. For further research, trials need to be conducted using router devices from vendors such as Cisco or others.

5. ACKNOWLEDGEMENTS

I would like to thank all parties who have helped in this research, including the research team, translators, and reviewers.

6. DECLARATIONS

AUTHOR CONTIBUTION

The author compiled this research, which was divided into their respective tasks. Husain determined the research topic, compiled and analyzed the methods used, and I Putu Haryadi studied the theory of design, configuration, and testing. Kurniadin Abd. Latif carried out theoretical studies and method comparisons, as well as an analysis of the results, and Galih Tri Aditya carried out system design, configuration, and testing.

FUNDING STATEMENT

This research did not receive grants from anywhere, including the public, commercial, or non-profit sectors.

COMPETING INTEREST

This study has no reserves related to competing financial, public, or institutional interests.

REFERENCES

[1] L. Grinin and A. Grinin, "Technologies: Limitless possibilities and effective control," in *Reconsidering the Limits to Growth: A Report to the Russian Association of the Club of Rome*. Springer, 2023, pp. 139–154.

[2] Y. Edan, G. Adamides, and R. Oberti, "Agriculture automation," *Springer Handbook of Automation*, pp. 1055–1078, 2023.

[3] H. Husain, A. Anggrawan, H. Santoso, H. T. Sihotang, D. Pyanto, and F. R. Hidayat, "Pengaturan Bandwidth Management Dan Time Limitation Berbasis User Manajer Mikrotik," *Jurnal Mantik Penusa*, vol. 2, no. 2, 2018.

[4] A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, "A security awareness and competency evaluation in the energy sector," *Computers & Security*, vol. 129, p. 103199, 2023.

[5] V. Mahendra and B. Soewito, "Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber," *Techno. Com*, vol. 22, no. 3, pp. 527–538, 2023.

[6] B. S. Prawiraharjo, F. X. Priyono, and N. Trihastuti, "The Jurisprudence Regarding the Protection of Personal Data for the Communities and Business Actors in Indonesia," in *Proceedings of the 1st International Workshop on Law, Economics and Governance, IWLEG 2022, 27 July 2022, Semarang, Indonesia*, 2023.

[7] T. Sutikno and D. Stiawan, "Cyberattacks and data breaches in Indonesia by Bjorka: hacker or data collector?" *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 6, pp. 2989–2994, 2022.

[8] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International journal of critical infrastructure protection*, vol. 25, pp. 36–49, 2019.

[9] R. Adrian, T. Widiasari, M. A. R. Somardani, and A. J. Okke, "Malware Clustering System using Moth-Flame Optimization as IoT Security Strengthening," in *2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE)*. IEEE, 2023, pp. 279–283.

[10] I. Pali and R. Amin, "PortSec: Securing Port Knocking System using Sequence Mechanism in SDN Environment," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2022, pp. 1009–1014.

[11] R. R and Y. Muin, "MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method," *International Journal of Computer Applications*, vol. 183, no. 47, pp. 33–37, 2022.

[12] A. Mursyidah, Husaini, Atthariq, Muhammad Arhami, Hari Toha Hidayat and Ramadhona, "Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS," *IOP Conference Series: Materials Science and Engineering*, vol. 536, no. 1, 2019.

[13] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: A survey on application potential," *Applied Energy*, vol. 257, p. 113972, 2020.

[14] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future generation computer systems*, vol. 108, pp. 909–920, 2020.

[15] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," *Journal of King Saud University-Computer and Information Sciences*, 2022.

[16] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, "Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 281–292, 2023.

[17] L. Wu, A. Jaiprakash, A. K. Pandey, D. Fontanarosa, Y. Jonmohamadi, M. Antico, M. Strydom, A. Razjigaev, F. Sasazawa, and J. Roberts, "Robotic and image-guided knee arthroscopy," in *Handbook of robotic and image-guided surgery*. Elsevier, 2020, pp. 493–514.

[18] A. Shekargoftar, H. Taghaddos, A. Azodi, A. Nekouvaght Tak, and K. Ghorab, "An integrated framework for operation and maintenance of gas utility pipeline using BIM, GIS, and AR," *Journal of Performance of Constructed Facilities*, vol. 36, no. 3, p. 4022023, 2022.

[19] A. Blaise, M. Bouet, V. Conan, and S. Secci, "Detection of zero-day attacks: An unsupervised port-based approach," *Computer Networks*, vol. 180, p. 107391, 2020.

[20] R. Muwardi, H. Gao, H. U. Ghifarsyam, M. Yunita, A. Arrizki, and J. Andika, "Network security monitoring system via notification alert," *Journal of Integrated and Advanced Engineering (JIAE)*, vol. 1, no. 2, pp. 113–122, 2021.

[21] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.

[22] N. S. Chahal, P. Bali, and P. K. Khosla, "A Proactive Approach to assess web application security through the integration of security tools in a Security Orchestration Platform," *Computers & Security*, vol. 122, p. 102886, 2022.

[23] W. Major, W. J. Buchanan, and J. Ahmad, "An authentication protocol based on chaos and zero knowledge proof," *Nonlinear Dynamics*, vol. 99, pp. 3065–3087, 2020.

[24] Y. Huang, F. Zhu, L. Liu, W. Meng, S. Hu, R. Ye, and T. Lv, “WNV-Detector: automated and scalable detection of wireless network vulnerabilities,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, pp. 1–21, 2021.

[25] G. Chalhoub and A. Martin, “But is it exploitable? Exploring how router vendors manage and patch security vulnerabilities in consumer-grade routers,” 2023.

[26] A. AlSabeh, J. Khoury, E. Kfoury, J. Crichigno, and E. Bou-Harb, “A survey on security applications of P4 programmable switches and a STRIDE-based vulnerability assessment,” *Computer Networks*, vol. 207, p. 108800, 2022.