JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 9 Number 1 | June 2024: 41-51
DOI: 10.15575/join.v9i1.1254

Case Study In Network Security System Using Random Port Knocking Method On The Principles Of Availability, Confidentiality And Integrity

Tati Ernawati[1], Idham Kholid[2], Dahlan[3], Dini Rohmayani[4]
[1,2,3,4]Informatics Engineering Study Program, TEDC Bandung Polytechnic, Indonesia

Article Info

Article history:

Received December 20, 2023
Revised March 08, 2024
Accepted March 21, 2024
Available Online April 23, 2024

Keywords:

Availability
Confidentiality
Integrity
Network Security
Random Port Knocking

ABSTRACT

Preventing unidentified individuals from misusing their access to information is a major concern when it comes to data security. Network administrators are charged with working harder to be able to secure the computer network they manage. The utilization of right method is a challenge for network administrators to protect computer network from intruders. The RPK method is one of solution to overcome this problem. This research aims to implement RPK method on the principles of availability, confidentiality, and integrity which have not been explored by previous studies. The network system configuration stage involved installing Debian 9, NMAP, Hydra, RPK, cloud server, remote admin, and attacker. The network security system's performance was tested, revealing a 99.97% availability rate and 100% confidentiality. The system's integrity was assessed, with an average response time of 0.22 seconds and 100% blocking accuracy. The test results indicate that the system's network security performance, using the RPK method, capable of protecting server attacks and effectively upholding security stability.

Corresponding Author:

Tati Ernawati,
Informatics Engineering Study Program, TEDC Bandung Polytechnic, Indonesia
Jl.Pasantren KM 2 Cimahi, Jawa Barat, Indonesia
Email: tatiernawati@poltektedc.ac.id

1. INTRODUCTION

The rapid development of information technology is significantly impacting the Internet industry, making it more accessible and creating increased challenges in terms of security [1]. In 2023, survey reports from the Association of Indonesian Internet Service Providers show that the internet user penetration rate reached 78.19%, including around 215,626,156 individuals out of the total population of 275,773,901, which marked a 1.17% increase compared to 2022 [2]. While computer network and the internet provide convenience for human work, system also introduces problems, particularly in the form of cyber network security attacks, and addressing these threats has become a significant challenge [3][4]. Statistical data shows a simultaneous increase in cyber security incidents with the growing use of networks and technology [5]. The evolution of computer networking has seen the transition to virtualization. Since cloud computing offers a new method of supplying and financing computer and network resources, it is seen as revolutionary [6]. Meanwhile, the use of cloud technology such as virtual servers will be vulnerable to cyber attacks.

In an August 2023 report, the National Cyber and Cryptography Agency documented irregular traffic of 78,464,385, with 8,134,901 instances of information leakage irregularities due to unauthorized access which represents a significant 91.18% increase compared to July. Recorded cyber security incidents totaled 54, with the highest number being 43 cases of data breach, an event where hackers

gain unauthorized access to sensitive information. Additionally, 290,556 instances of data exposure, including credential information, were discovered on the darknet [7].

The increasing frequency of cyber-attack signifies the critical importance of security controls and evaluations [8]. However, this practice shows personal data to potential misuse by users lacking proper access or authorization [9]. A system that ignores security considerations can have a damaging impact on total efficiency, performance, and user convenience [10]. Protecting privacy becomes important for users, given the susceptibility of a large amount of user data to theft in an untrustworthy internet environment [11]. The issue developing from cyber threats includes internet users sharing personal data or information to support work activities. [6] stated that Information is stored on computer hardware, manipulated by software, and transmitted through communications, requiring protection in each area. Information security aims to implement protective measures to ward off attacks, prevent system collapse, and recover quickly. According to [6] three protections must be implemented over information i.e. availability, confidentiality and integrity.

Network administrators face the challenge of preventing unknown individuals from abusing access to information, the problem is they require the use of effective methods to protect their computer networks from intruders. One of method that can be used as an alternative solution for computer network security is Random Port Knocking (RPK) method which has ability to identify authorized users entering system, thereby improving security against attack. Using pseudo random port generator, generating random numbers using an application that will later serve as a port sequence in the knocked application [12], port knocking security layer strengthens the network's existing security mechanisms [13]. Port Knocking is a method to unlock access to a particular port that has been blocked by a firewall on a network device by sending a particular package or connection [14].

Several research explored RPK method, including [14], which used RPK to improve network security. Tests were conducted on various login processes, showing the effectiveness of the method. Additionally, [15] joined Rivest-Shamir-Adleman (RSA) encryption random sequence into port knocking to safeguard system during online collective access. Test results on Secure Shell (SSH) services, using major authentication on port 22/TCP, recommended that devices could be effectively secured by secreting port from internet scanners and malware. Meanwhile, [16] analyzed the performance of Secure Random Port List Generator (SRPLG) method in securing the Secure Shell (SSH) server. The results showed the efficacy of the process in securing the transmitted port list information, and successfully encrypting the communication path to prevent attacks such as sniffing. Another research was implemented of a pseudo random number generator in port knocking aims to enhance the authentication process for client computers connecting to the server system. The results showed the authentication process is excellent in validating the client computer that will be connected to the server system [12].

This research aims to implement RPK method to a Virtual Private Server (VPS)-based computer network security system. It is driven by three main principles of network security: availability, confidentiality, and integrity. This research have not been examined in prior research which only focused on restricts unauthorized access to the system (confidentiality). VPS is selected for the saving costs [17] and virtual servers can be made available fast [6].

2. METHOD

This research aims to implement RPK method to meet the principles of availability, confidentiality, and integrity based on VPS. The flow diagram for the system design utilized in this study is depicted in Figure 1.

2.1 Literature Review

The initial phase of the research involves conducting a literature review of various studies on network security for RPK method and other relevant materials correlated with this study, understanding the topic's fundamental ideas is another purpose of this stage.

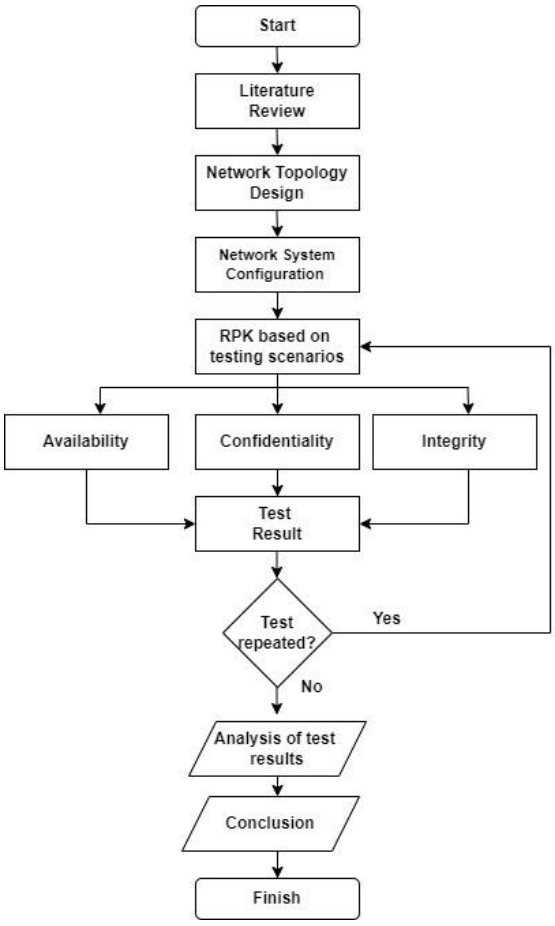

Figure 1. Research Method Flowchart

2.2 Network Topology Design

The second stage, the proposed network topology design was created between the server and attacker, referencing the current operational topology. The current topology showed TEDC Polytechnic network conditions in Figure 2, security system on the server was only protected by a firewall configured through a router, with packets analyzed using rules matching the firewall. Data was collected through observations and interviews with network administrators.

Furthermore, in Figure 3, the built topology proposed added Debian 9-based cloud server configured with RPK. Attacker connected to the server through internet access using SSH protocol and when successful, the server sent IP data and access time to the connected PC/Laptop through Telegram application.

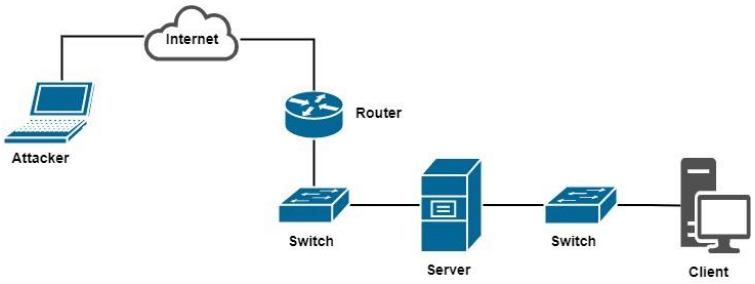

Figure 2. Network Topology Existing

p-ISSN: 2528-1682
e-ISSN: 2527-9165

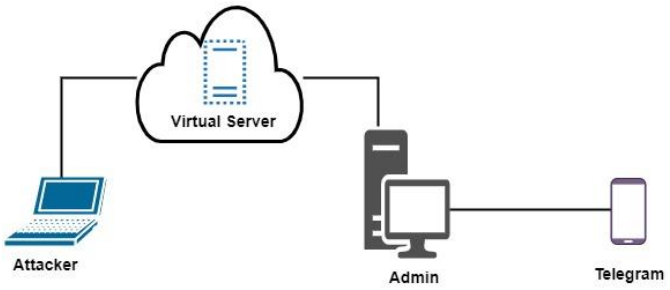

Figure 3. Network Topology Proposed

2.3 Network System Configuration

The third stage included creating the initial network performance using Virtualbox simulation tools and the results served as the foundation for the direct installation process on VPS. The network system configuration stage included installing and applying all configurations into VPS, including the installation of the operating system (Debian 9) and supporting applications (NMAP, Hydra), RPK configuration, system configuration on the cloud server, remote admin, and attacker, as well as Internet Protocol (IP) address configuration.

IP address configuration was completed only on the virtual server (149.28.154.xxx) with a subnet mask of 255.255.255.0. PC admin and PC attacker were not configured because both devices had to change IP when accessing the server or connecting to network. System configuration was conducted on the server, remote admin, and attacker. Server configuration included two stages namely first, creating virtual machines using Virtualbox application, and second, installing the server, including Debian 9 installation, RPK configuration using the knock application, creating a firewall to close connections from port 22, and configuring Telegram by creating Telegram bot and finding user identity data (bot token and user token) to be input into Debian 9 configuration. Remote admin configuration used the knock-knock application to input sequences obtained from Telegram, and Putty application connected to the server through SSH (port 22). Attacker configuration included two types of attacks which were brute force using Hydra and port scanning using NMAP.

2.4 RPK Based on Testing Scenario

The testing stage included continuous observation during the experiment, assessing the performance of the RPK based on testing scenarios. In addition, test parameters included availability, confidentiality, and integrity, with response time and blocking accuracy tested for brute force attack and port scanning. Network security testing is detailed in Table 1.

Table 1. Types, Scenarios, and Success Rates of Testing

Test Types	Test Scenarios	Success Level
1. Availability System	Testing how long system could be active again after being attacked. The cause of failure was an unstable network when logging into the server.	System availability percentage, the higher the better it becomes.
2. Confidentiality System	System performance testing: a. Hid the original SSH port, b. Blocked access for users without access rights, c. Able to view network traffic on the server, d. Showed user login notifications to the server on Telegram, e. Showed notifications of random sequence port changes when the user successfully logged into the server.	Five test scenario parameters were fulfilled.
3. Integrity System	a. *Response Time* Testing the time it used for the knocked application to open access to users with access rights to the server in seconds for each sequence. b. Blocking Accuracy Testing attacks entering system.	The shorter the duration, the better. Could block all attacks that occur in system.

2.5 Analysis Test Result

The complete test was conducted in 8 days (D1-D8), the integrity system for response time test was conducted 5 times (P1-P5) in 8 days, in the meantime, 40 simulations were run for each of the blocking accuracy tests for port scanning and brute force attacks.

2.5.1 Availability

Availability principle signifies the recovery time of system after an attack based on the uptime of the method [6]. The results of the availability test were calculated using the following formula (1)

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF+MTTR}} \text{ x } 100 \quad (1)$$

MTBF = *Mean Time Between Fault*, average uptime.
MTTR = Mea*n Time to Repair*, the average time required to restore service.
The total value (days 1-8) was calculated by averaging the Availability/day values.

2.5.2 Confidentiality

Confidentiality principle restricts access to system from unauthorized users [6][18]. The success of confidentiality test was fulfilled five test scenario parameters (Table 2)

Table 2. Confidentiality Scenarios Test and Success Rates of Testing

Test Scenarios	Success Level
1. System was able to hide the original SSH port	RPK system with a firewall using IP Tables successfully hid SSH port (22), the user should enter port sequence.
2. System was able to block access to users who did not have access rights	Users without sequence port input cannot access the server.
3. System could monitor network traffic on the server.	Users who joined the port sequence and successfully accessed system through SSH port (22) were detected on system through the syslog file in the var/log folder.
4. A user login notification to the server on Telegram appeared	Telegram sent a notification to Telegram admin containing the IP address, time, and location of users who had successfully joined system
5. Random port sequence changed notification would appear when the user successfully logged in to the server	Port sequence changed randomly when the user successfully joined the server. When the user closed system, the operator could not enter again and might enter a different port sequence. Port sequence changed message appeared in the knocked application in the form of the changed time and sequence number sent through telegram

2.5.3 Integrity

Integrity principle is used to determine the accuracy or speed of system in handling attack [6][19]. Two parameters were using for integrity test, namey respon time and blocking accuracy.

a. Respon times

The total response time value was calculated using the formula (2)

$$\bar{R} = \frac{RDi}{\text{Dn}} \quad (2)$$

$\bar{R}$ = Average total response time
RDi = Average response time/day $_i$
Dn = Total days

b. Blocking Accuracy

Experimental testing was performed at TEDC Polytechnic campus using simulated brute force attack and port scanning. The results of blocking accuracy test for brute force attack and port scanning, performed with 40 simulations each, were 100%, meaning system successfully handled all attacks (no incoming attacks). Brute force attack includes using applications to attempt random usernames and passwords, creating a danger where unauthorized users can gain access to system [6]. Port scanning checks for active ports on the server and is risky when open, allowing unrestricted access by users without permission to access system through those ports [19].

2.6 Conclusion

Following the completion of the analysis, conclusions were made. The authors draw conclusions based on the analysis of the results of research related to the problem of network security by reference to the formulation of the problem and the purpose of the research.

3. RESULT AND DISCUSSION

3.1. Result

The achieved result was computer network security system using RPK method that fulfilled the principles of availability, confidentiality, and integrity. System was used and tested on the internal network of TEDC Polytechnic in Bandung.

3.1.1 Availability

The total value (days 1-8) was calculated by averaging the Availability/day values, the test result data in Table 3.

Table 3. Average Availability Value

Day i (Di)/ Downtime (WIB)	MTBF (Minutes)	MTTR (Minutes)	Availability (%)
D1/19:33	6223.58	5.16	99.92
D2/08:16	6997.54	3.61	99.95
D3/12:52	8742.47	2.28	99.97
D4/19:33	10555.8	2.3	99.98
D5/19:29	16322.3	4.2	99.97
D6/19:30	17739.1	0.9	99.99
D7/14:31	28955.1	1.9	99.99
D8/20:15	32200.6	2.2	99.99
	Average Availability Value		*99.97*

3.1.2 Confidentiality

The five test scenario conditions were met, and the confidentiality test result was 100%. The test result data in Table 4.

Table 4. Confidentiality Test Results

Test Scenarios	Test results	Day i (Di)/Test Time (WIB)							
		D1	D2	D3	D4	D5	D6	D7	D8
		19:33	08:16	12:52	19:33	19:29	19:30	14:31	20.15
1. System was able to hide the original SSH port	RPK system with a firewall using IP Tables successfully hid SSH port (22), the user should enter port sequence.	√	√	√	√	√	√	√	√
2. System was able to block access to users who did not have access rights	Users without sequence port input cannot access the server.	√	√	√	√	√	√	√	√
3. System could monitor network traffic on the server.	Users who joined the port sequence and successfully accessed system through SSH port (22) were detected on system through the syslog file in the var/log folder.	√	√	√	√	√	√	√	√
4. A user login notification to the server on Telegram appeared	Telegram sent a notification to Telegram admin containing the IP address, time, and location of users who had successfully joined system (Figure 4).	√	√	√	√	√	√	√	√
5. Random port sequence changed notification would appear when the user successfully logged in to the server	Port sequence changed randomly when the user successfully joined the server. When the user closed system, the operator could not enter again and might enter a different port sequence. Port sequence changed message appeared in the knocked application in the form of the changed time and sequence number sent through telegram (Figure 4).	√	√	√	√	√	√	√	√

Note: √ = Successful

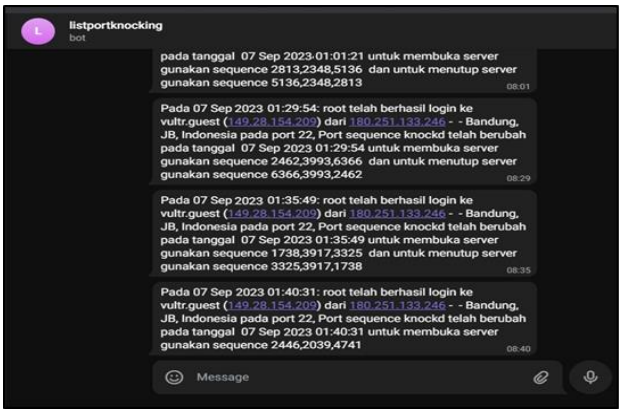

Figure 4. Login Notification and Port Sequence Changes on Telegram

3.1.3. Integrity

a. Response Time

The complete response time test results were shown in Table 4 in which the test was conducted 5 times (P1-P5) in 8 days (D1-D8). The average value per day was shown in Figure 5 and the total response time value:

$$\bar{R} = \frac{RDi}{8} = \frac{0.23+0.21+0.22+0.21+0.22+0.23+0.21+0.24}{8} = 0.22 \text{ second}$$

Table 4. Response Time Test Results

Test (P)	Day i (Di)/Test Time (WIB)/Response Time (Second)							
	D1	D2	D3	D4	D5	D6	D7	D8
	19:33	08:16	12:52	19:33	19:29	19:30	14:31	20.15
P1	0.219	0.219	0.228	0.224	0.224	0.224	0.224	0.167
P2	0.228	0.228	0.228	0.224	0.224	0.274	0.225	0.280
P3	0.228	0.168	0.219	0.224	0.224	0.224	0.225	0.170
P4	0.228	0.228	0.219	0.168	0.224	0.224	0.225	0.337
P5	0.228	0.225	0.219	0.225	0.224	0.225	0.168	0.225

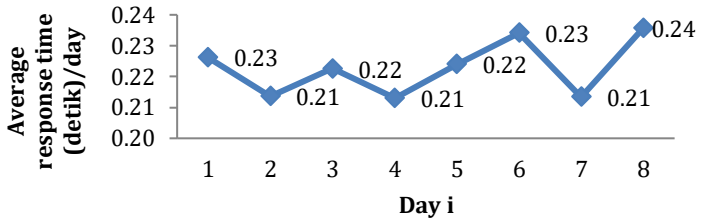

Figure 5. Graph of Average Response Time Per Day

b. Blocking Accuracy

The system effectively handled every attack (no inbound attacks) as evidenced by the 100% blocking accuracy test results for both port scanning and brute force attacks, each with 40 simulations. Figures 6-12 showed the capture results of blocking accuracy test using Hydra NMAP tool.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

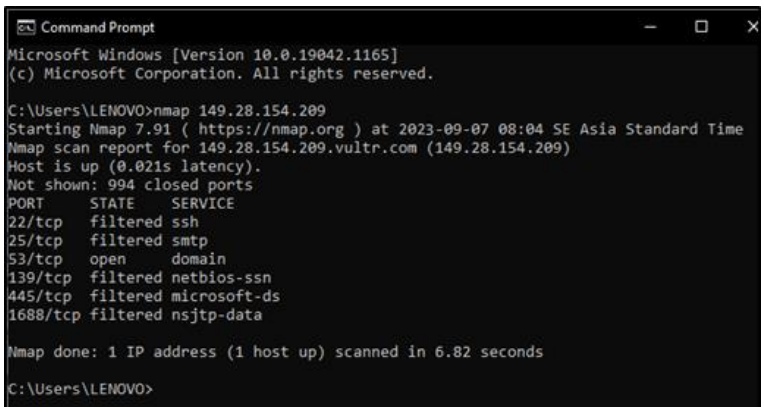

Figure 6. Blocking Port Scanning Attack on All Ports

Figure 6 shows the results of scanning all ports on the server with an open state (port: 53/tcp-service: domain), showing accessible ports, others were filtered (22/tcp-ssh, 25/tcp-smtp, 139/tcp-netbios-ssn, 445/tcp-miscrosoft-ds, and 1688/tcp-nsjtp-data), unable to be accessed due to the firewall, while the command used was nmap 149.28.154.209.

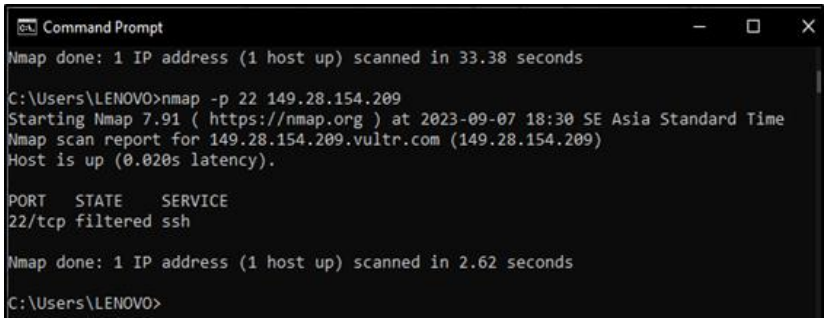

Figure 7. Blocking Port Scanning Attacks on SSH Port (22)

Figure 7 shows port 22 (SSH), and the outcome showed that it was filtered when the command nmap -p 22 149.28.154.209 was performed.

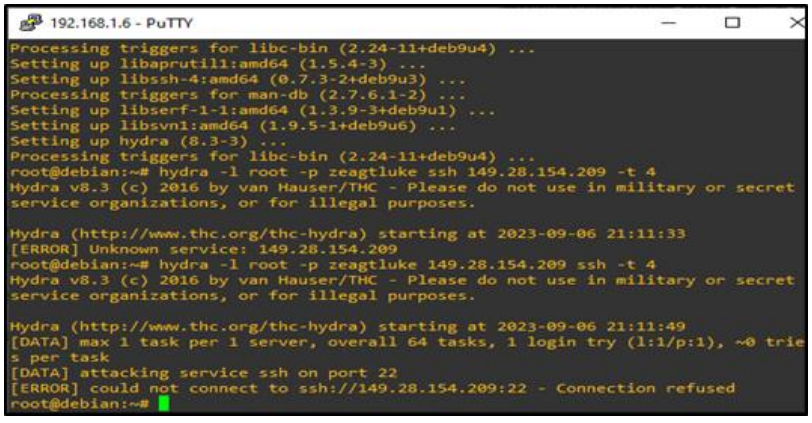

Figure 8. Blocking Brute Force Attack Single Username and Single Password

Figure 8 shows brute force attack using the username root and password zeagtluke with the command hydra -l root -p zeagtluke ssh 149.28.154.209 -t 4, leading to connection refusal, implying an unsuccessful attack.

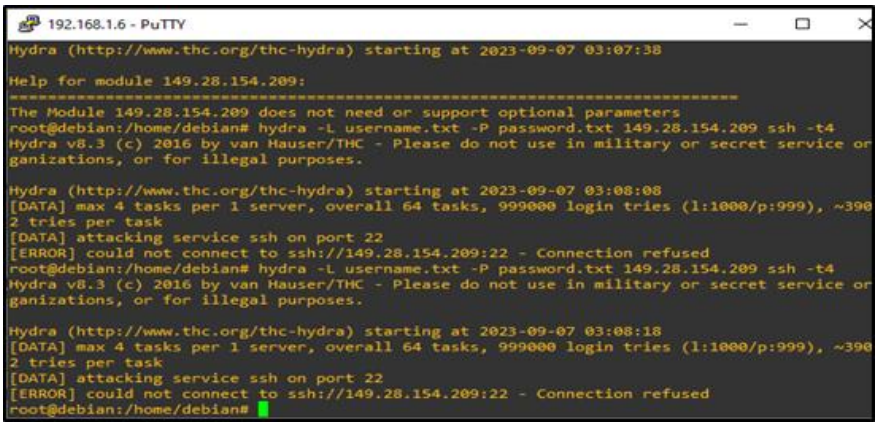

Figure 9. Blocking Brute Force Attack Multiple Username and Multiple Password

Figure 9 shows a brute force attack using data files username.txt and password.txt, leading to a connection refusal, showing an unsuccessful attack. The testing command was hydra -L username.txt -P password.txt ssh 149.28.154.209 -t 4.

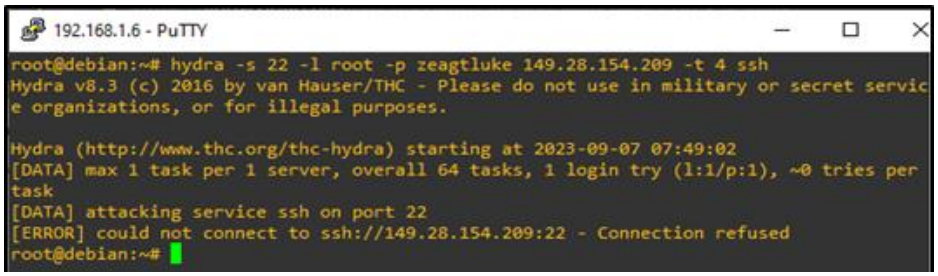

Figure 10. Blocking Brute Force Attack Single Username and Single Password on SSH Port (22)

Figure 10 shows brute force attack using the username root and password zeagtluke, adding port 22 (SSH) with the command hydra -s 22 -l root -p zeagtluke 149.28.154.209 -t 4 ssh, leading to a connection refusal, presenting an unsuccessful attack.

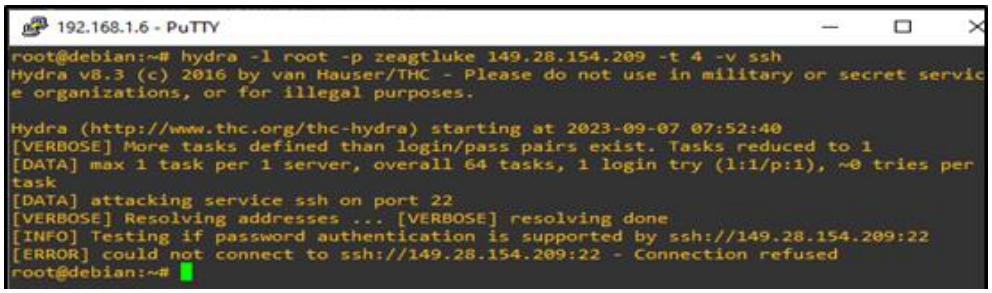

Figure 11. Blocking Brute Force Attack Single Username and Single Password with Different Verbose

Figure 11 shows a brute force attack using the username root and password zeagtluke with the command hydra -l root -p zeagtluke 149.28.154.209 -t 4 -v ssh, leading to a connection refusal, presenting an unsuccessful attack.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

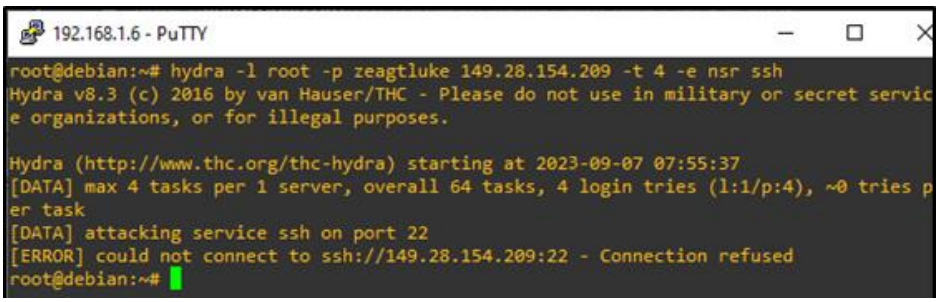

Figure 12. Blocking Brute Force Attack Single Username and Single Password with Additional Options

Figure 12 shows brute force attack using the username root and password zeagtluke, leading to a connection refusal. The command used was hydra -l root -p zeagtluke 149.28.154.209 -t 4 -e nsr ssh, with additional options including -e with -n for system using empty passwords, -s for system through the same password, and -r for the reverse brute force attack method.

3.2. Discussion

The RPK method in computer network security achieved a total performance result with 99.97% availability, 100% confidentiality, and successful integrity tests (average response time of 0.22 seconds and 100% blocking accuracy). RPK could anticipate port scanning and brute force attack on the server, leading to a good security system performance.

Similar results were obtained by several previous research observing the performance of RPK. The results of [14] proved that RPK method could handle security in the login process, automatically changing ports when login attempts failed more than three times, automatically blocking IP, and preventing network attack, therefore, improving network security stability. The use of the Secure Random Port List Generator to secure SSH servers effectively safeguarded against port scanning attacks, with no usable vulnerabilities identified in any of the shown port information [16]. The results [20] concluded that the performance of RPK could address brute force attack on the server by closing port and only users with access could knock on the designated port.

The added value of this study is the addition of two security principles namely availability and integrity in addition to confidentiality, while previous studies [14,16,20] focused only on confidentiality.

4. CONCLUSION

In conclusion, RPK showed effective performance in the network security system, making it a practical option for administrators or other users pursuing to use of this method in network security systems. This was evidenced by the test results of availability rate was 99.97%, confidentiality was 100%, and integrity system parameters, response time with an average speed of 0.22 second, and blocking accuracy was at 100%., which showed good performance. RPK could be relied upon to prevent brute force attack and port scanning. Different from previous studies [14,16,20] RPK focuses on the confidentiality principle, in particular the study restricts access to system from unauthorized users does not study avaibility and integrity.

The performance testing parameters for RPK were currently limited to three parameters and did not include all five network security principles. The parameters showed a deficiency in the current findings, and future research could improve by considering additional factors such as Authentication and Access control. Consequently, further development should be performed by adding ports such as Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP), while for types of attacks, Denial of Service Attack, Man in the Middle Attack, and DNS Poisoning could be included.

REFERENCES

[1] H. Chen, X. Han and Y. Zhang, "Endogenous Security Formal Definition, Innovation Mechanisms, and Experiment Research in Industrial Internet", *Tsinghua Science and Technology*, *IEEE Access* , vol. 29, no. 2, pp. 492-505, 2023, doi: 10.26599/TST.2023.9010034.

[2] APJII, *"Survei APJII pengguna internet di Indonesia tembus 215 juta orang"*, Available https://apjii.or.id/ berita/ d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang, 2023

[3] J.Sun, "Computer Network Security Technology and Prevention Strategy Analysis", *Proceedings of The 7th International Conference on Intelligent, Interactive Systems and Applications, Elsevier: ScienceDirect*, vol. 208, pp 570-576, 2022, https://doi.org/10.1016/j.procs.2022.10.079

[4] Y. Kai, H. Qiang and M. Yixuan, "Construction of Network Security Perception System Using Elman Neural Network", *2021 2nd International Conference on Computer Communication and Network Security (CCNS), Xining, China, IEEE Access* , pp. 187-190, 2021, doi: 10.1109/CCNS53852.2021.00042

[5] I.K.Sokolowska, and W. Caputa, "Awareness of Network Security and Customer Value-The Company and Customer Perspective", *Elsevier: ScienceDirect*, vol.190, pp 1-15, 2023, https://doi.org/10.1016/ j.techfore. 2023. 122430

[6] M.Ciampa, "*Comp TIA Security+ Guide to Network Security Fundamentals (7th edition)"*, Boston: Cengage Learning, Inc., 2020

[7] Direktorat Operasi Keamanan Siber BSSN (Badan Siber dan Sandi Negara), "*Laporan Bulanan Publik Agustus 2023*", 2023

[8] D. Jung, J. Shin, C. Lee, K. Kwon and J. T. Seo, "Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology", *IEEE Access,* vol. 11, pp. 15229-15241, 2023, doi: 10.1109/ACCESS.2023.3244991.

[9] X.Wang, and L.Shi, " Desing of Computer Network Security Storage System Based on Cloud Computing Technology", *IOP J. Phys.: Conf. Ser.*, vol.2083, 2021, doi:10.1088/1742-6596/2083/4/042084

[10] J. Y. Yu, E. Lee, S. -R. Oh, Y. -D. Seo and Y. -G. Kim, "A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security", *IEEE Access*, vol. 8, pp. 45304-45324, 2020, doi: 10.1109/ACCESS. 2020.2977778.

[11] Y. He, M. Zhang, X. Yang, J. Luo and Y. Chen, "A Survey of Privacy Protection and Network Security in User On-Demand Anonymous Communication", *IEEE Access*, vol. 8, pp. 54856-54871, 2020, doi: 10.1109/ ACCESS.2020.2981517.

[12] M. A. Verdiana, I. M. A. D. Suarjaya, and A. A. K. A. C. Wiranatha, "Implementasi Algoritma PRNG pada Aplikasi Port Knocking Sebagai Perlindungan Server", *Jurnal Ilmiah Merpati*, vol. 8, no. 3, pp. 232-243, 2020, doi: https://doi.org/10.24843/JIM.2020.v08.i03.p08

[13] I. Pali and R. Amin, "PortSec: Securing Port Knocking System using Sequence Mechanism in SDN Environment," *2022 International Wireless Communications and Mobile Computing (IWCMC)*, Dubrovnik, Croatia, 2022, pp. 1009-1014, doi: 10.1109/IWCMC55113.2022.9824343.

[14] I.R.P. Jeinever, A.Rasyid and N.Suharto, "Penerapan Sistem Keamanan Jaringan Menggunakan Random Port Knocking Berbasis Raspberry Pi Yang Dikirm Melewati Telegram", *Jurnal JARTEL*, vol.7, no.2, p.61-67, 2018, doi: https://doi.org/10.33795/jartel.v7i2.213

[15] M.Z.A.Mahmud, Saifuddin and D. Risqiwati, "Implementasi Asymmetric Encryption RSA Pada Port Knocking Ubuntu Server Menggunakan Knockd Dan Python", *Jurnal Repositor*, vol.2 no.6, pp.787-794, 2020, doi:10.22219/REPOSITOR.V2I6.270

[16] S. A. Rauf, M. Faiqurahman, and D. R. Akbi, "Secure Random Port List Generator pada Mekanisme Autentikasi Dengan Menggunakan Port Knocking dan Secure Socket Layer",Register: *Jurnal Ilmiah Teknologi Sistem Informasi,* vol. 4, no. 2, pp. 103-113, 2018, https://doi.org/10.26594/register.v4i2.1162

[17] B.A.Nday, G.P. Kusuma, and R.Fredyan," Serverless Utilization In Microservice E-Learning Platform", *7th International Conference on Computer Science and Computational Intellegence 2022, Elsevier: ScienceDirect,* pp.204-212, 2023, doi: https://doi.org/10.1016/j.procs.2022.12.128.

[18] S. O. Oruma and S. Petrovic, "Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey", *IEEE Access,* vol. 11, pp. 63205-63237, 2023, doi: 10.1109/ACCESS.2023.3288338.

[19] R.R.Singh and D.S. Tomar, "Scanning Attack Analysis with Dempster-Shafer Evidence Theory*", International Journal of Applied Engineering Research*, vol.12, no.16, p.5900-5904, 2017, ISSN 0973-4562

[20] R.Ernawati, I.Ruslianto, and S.Bahri, "Implementasi Metode Port Knocking Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring", *Jurnal Komputer dan Aplikasi*, vol.10, no.01, p. 158-169, 2022, doi: http://dx.doi.org/10.26418/coding.v10i01.54226