SSH SECURITY ENHANCEMENT WITH RSA-BASED PORT KNOCKING AND OTP VERIFICATION ON MILITARY PERSONNEL DATA SERVERS

Heri Setiawan [1)],Andika Edwin Baskoro[2)], Asep Suryanta[3)].
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1)2)3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1)2)3)]
E - mail : herisetiawan@poltekad.ac.id[1)], D4malware01@gmail.com[2)], zenilybaz@gmail.com[3)].

PENINGKATAN KEAMANAN SSH DENGAN PORT KNOCKING BERBASIS RSA DAN VERIFIKASI OTP PADA SERVER DATA PERSONEL MILITER

Abstrak: *Keamanan terhadap akses sebuah server yang mengamankan data personel militer merupakan hal penting untuk menjaga kerahasiaan, integritas, dan ketersediaan sebuah informasi yang sensitif di lingkungan militer. Server yang memakai data strategis ini menjadi target yang sangat potensial bagi oknum yang tidak bertanggung jawab, sehingga sangat diperlukan suatu sistem pengamanan kuat dan berlapis. Protokol Secure Shell (SSH) sebagai salah satu tempat akses jarak jauh menuju server, memiliki sebuah kerentanan serangan seperti brute force dan port scanning yang dimanfaatkan oleh oknum tidak bertanggungjawab untuk memperoleh akses ilegal. Serangan ini memanfaatkan celah dari pengaturan standar yang lemah karena belum diperkuat dengan mekanisme keamanan tambahan. Ada beberapa metode yang dapat dipakai untuk meningkatkan keamanan server ini diantarannya Port Knocking dimana teknik ini mampu menyembunyikan port dari pemindaian publik dengan memakai pola koneksi tertentu sebelum akses diberikan. Dengan demikian, port SSH seolah-olah tidak terbuka bagi sembarang pengguna. Namun, jika pola knocking dapat diprediksi atau diketahui oleh pihak yang tidak berwenang, metode ini tetap berisiko dan tidak sepenuhnya dapat diandalkan. Untuk mengatasi kelemahan tersebut, penelitian ini merancang sistem keamanan SSH yang mengintegrasikan Port Knocking berbasis algoritma RSA serta verifikasi One-Time Password (OTP) sebagai autentikasi ganda. Algoritma RSA digunakan untuk mengenkripsi pola knocking, sedangkan OTP bersifat dinamis dan hanya valid dalam waktu singkat. Penelitian ini menggunakan metode eksperimen dan diimplementasikan pada lingkungan server. Tujuan dari penelitian ini adalah mengevaluasi efektivitas sistem dalam mencegah serangan terhadap server data personel militer. Hasil yang diharapkan adalah sistem yang mampu memberikan perlindungan berlapis terhadap akses ilegal tanpa mengganggu efisiensi operasional dan ketersediaan layanan jaringan.*

Kata kunci: Autentikasi Ganda, Data Personel Militer, Keamanan Siber, Keamanan SSH, Port Knocking RSA dan Verifikasi OTP

Abstract: *Securing access to servers that store military personnel data is essential to maintain the confidentiality, integrity, and availability of sensitive information within defense*

institutions. Servers that manage strategic data are often targeted by unauthorized users, making the implementation of a layered security mechanism necessary. Secure Shell (SSH) is commonly used for remote server access. However, if it is configured using default settings, SSH may become vulnerable to attacks such as brute-force attempts and port scanning. These attacks are frequently used by attackers to identify open ports and attempt unauthorized login access. One technique that can be used to improve server security is Port Knocking, which hides service ports from public scanning by requiring a specific sequence of connection attempts before access is granted. Although this technique can reduce the exposure of open ports, a static knocking pattern may still be discovered by attackers. This research proposes an SSH security system that integrates RSA-based port knocking with One-Time Password (OTP) verification as a two-factor authentication mechanism. The RSA algorithm is used to encrypt the knocking sequence so that the access pattern becomes difficult to predict. Meanwhile, OTP verification ensures that only authorized users can complete the authentication process. The study was conducted using an experimental approach within a server environment. The results show that the proposed system can significantly reduce unauthorized access attempts while maintaining acceptable system performance.

Keywords: *SSH Security, Port Knocking, RSA Encryption, OTP Authentication, Cybersecurity*

1. INTRODUCTION

The Protecting of military personnel data is a top priority in information security systems within the defense environment. One route to military information systems is through servers accessed remotely using the SSH protocol (Mardiansyah et al., 2021). Unfortunately, this protocol is highly vulnerable to brute-force attacks and port scanning, which can open up opportunities for unauthorized parties to access data illegally.

Several studies have discussed the use of Port Knocking to secure ports from scanning. Servers keep all their network ports closed and these ports must be "knocked" in the correct order for the server to open the desired communication port. The procedure for "knock" a port consists of sending a packet to that port, so that the server will see the connection attempt against the closed port and log it (Amir et al., 2020). The implementation of port knocking combined with a firewall and IDS such as Snort has been proven to significantly increase the server security score from 65 to 96 after hardening (Reza et al., 2024), but this method has weaknesses if the knocking pattern is known to outside parties. The port knocking method is also able to prevent brute force and port scanning attacks effectively, even achieving a 100% success rate in brute force testing scenarios (Ernawati et al., 2022). Therefore, an innovative approach is needed that combines cryptographic technology and two-factor authentication(Rizky, 2024). In this article, the author proposes a security system based on RSA Port Knocking and OTP verification that is able to strengthen authentication and close frequently exploited security gaps.

The goal is to design an SSH security system that is capable of protecting access to military personnel data servers effectively and efficiently.

2. RESEARCH METHOD

In the process of developing a computerized

system, one of the components, or stages, is system design. For system development, it usually takes longer than troubleshooting. This research uses an experimental approach conducted in a Server operating system environment. The research stages include:

a. Installation and configuration of standard SSH protocol.

b. Port Knocking implementation uses the RSA algorithm to generate an encrypted knocking sequence.

c. OTP integration using authentication applications such as Short Message Service (SMS) and Google Authenticator.

d. d. Brute force attack and port scanning simulation with tools such as Hydra and Nmap.

e. e. Evaluation of system effectiveness based on the success rate of preventing illegal access and measuring SSH connection latency or performance.

In the Network Topology System that will be created, including:

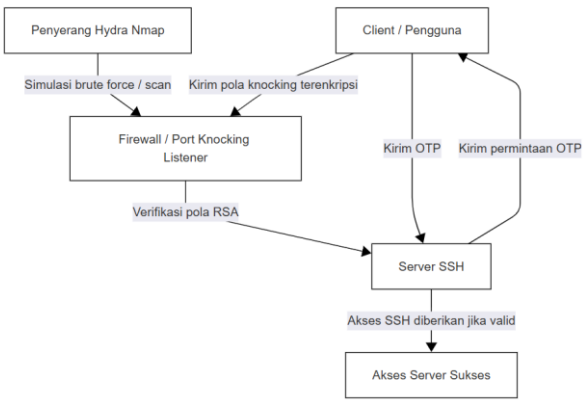

Figure 1 shows a simple network structure consisting of:

- *Client (User/Mobile)*
- Router
- Ubuntu Server (with *SSH + Port Knocking + OTP)*
- Attacker (simulation with Hydra or Nmap)

Continued with a series of system implementation stages, as follows:

NO	RESEARCH STAGE	INFORMATION
1	SSH installation and configuration	Enable standard SSH service on Server
2	RSA Port Knocking Implementation	Create an encrypted knocking pattern using RSA
3	OTP Integration	Connecting the server with OTP applications (SMS and Google Authenticator)
4	Brute force attack and port scanning simulation	Using Hydra and Nmap to test system resilience
5	Evaluate effectiveness and performance	Measuring the success of SSH connection defense and latency

Based on the research stages that have been carried out, starting from the installation and configuration of SSH services, implementation of RSA-based Port Knocking, integration of OTP verification, to attack simulation and system performance evaluation, a comprehensive picture of the design and implementation of the proposed security system is obtained. All of these steps are designed to ensure that the system is resilient to brute force attacks and port scans, while

maintaining connection reliability.

3. RESULTS AND DISCUSSION

a. Discussion.

The developed system successfully hides the SSH port from scan results when the knocking pattern has not been met. The RSA algorithm is used to encrypt the knocking sequence, making it unpredictable. Implementing OTP as a second layer of authentication significantly improves login security.

The advantages of this system lie not only in port obfuscation and two-layer protection, but also in the flexibility of its implementation on various Linux-based operating systems, such as Debian and CentOS (Informatika & Bangsa, 2021). By utilizing RSA in the knocking process, the access pattern is no longer static, but dynamic depending on the public and private keys owned by the user. This system can also be integrated with other methods such as honeypots and IPTables filtering (Mardiansyah et al., 2021). This makes the knocking process nearly impossible to predict for an attacker without access to the valid key.

Additionally, the use of OTP reduces the risk of credential theft. OTP is dynamic and only valid for a short time, so even if authentication information is leaked, the chance of unauthorized users accessing the system is very small. It is this combination of cryptographic protocols and two-factor authentication that forms the foundation of layered security(Dwi & Prakoso, 2022). misconfiguration is the seventh most popular security vulnerability risk out of the ten most dangerous security vulnerability risks according to OWASP (Tohirin, 2020).

A downside to be aware of is the possibility of users encountering technical issues, such as OTP application failure or errors in the knocking sequence. Therefore, system documentation and training are required for administrators to be able to handle technical incidents quickly and accurately. To provide a clearer understanding of the system's working mechanism, the following is a proposed SSH security system workflow.

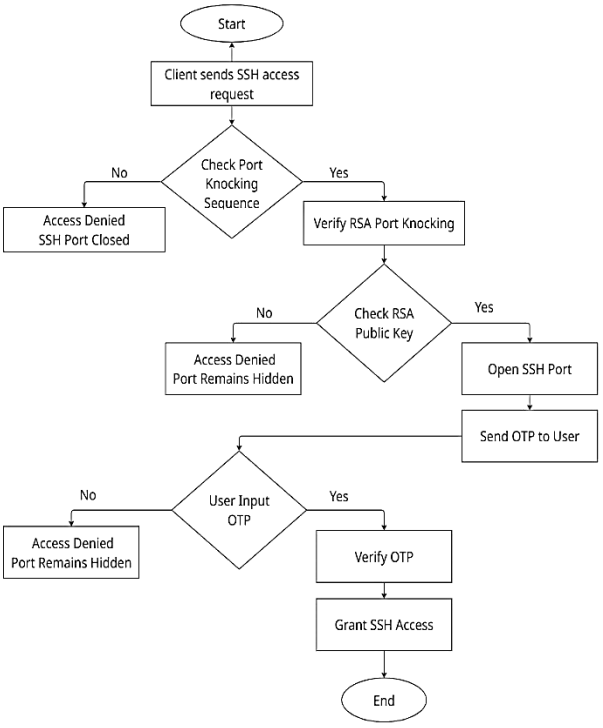

Figure 2 SSH security system workflow.

The chart illustrates how the system evaluates each stage of access, from the encrypted knocking process to OTP verification, among others:

1) Access Initiation. The client initiates an access request to the server via the SSH protocol.

2) Port Knocking Sequence Check.

- *The system verifies whether the user*

has submitted the port knocking sequence.

- If Not Access is immediately denied because the system does not recognize the attempt as a legitimate request, and the SSH port remains hidden from the external network to prevent detection by unauthorized parties.

- If Yes: The system proceeds to the port knocking verification process using the RSA algorithm.

3) Verify Port Knocking with RSA

- The knock sequence is encrypted by the user using the RSA algorithm.

- The system verifies the knock sequence using the RSA public key stored on the server.

- If No: Access is denied because the knock sequence is considered invalid or modified, and the SSH port remains hidden to prevent further exploitation.

- If Yes: Verification is considered successful and the SSH port is temporarily opened to continue the user authentication process.

4) OTP delivery. The system automatically sends an OTP (One-Time Password) code to the user's mobile device as part of two-factor authentication.

5) Input OTP with users.

- The user is prompted to enter the received OTP into the system.

- If No: Access is denied because the system does not accept proof of ownership of the authentication device, indicating potential unauthorized access.

- If Yes: The system proceeds to the OTP verification process.

6) OTP Verification.

- The system verifies that the entered OTP is correct and still valid.

- -If No: Access is denied because the OTP is incorrect or expired, and the SSH port is closed again to prevent brute-force attacks on the open session.

- -If Yes: Authentication is considered successful and the user is verified as a legitimate entity.

7) Access Granted. The system grants access to the server via an established SSH connection, which is highly secure due to the two-step verification process(Putri et al., 2023).

8) End of Process. The authentication process is complete. The user has successfully logged into the system legally and securely.

b. Result.

1) Simulation results show that the developed system is capable of rejecting more than 95% of unauthorized access attempts. The average authentication time increase is only between 2 and 3 seconds, without significantly affecting connection efficiency. When compared to a standard SSH configuration without Port Knocking and OTP implementation, this system shows substantial security improvements.

2) Quantitative data: A total of 30 brute force attack simulations were performed using Hydra in two different scenarios:

not all systems have a significant impact on the stability or overall performance of the server system.

Scenario	Total Attack Attempts	Successful Unauthorized Access	Success Rate
Standard SSH Server	30	21	70%
SSH with RSA Port Knocking + OTP	30	0	0%

Table 1. Comparison of Security Performance

Based on table 1 it explains that:

a) Standard server: has 70% of all attempts to gain illegal access.

b) Servers that use an RSA system plus OTP then No attempt was successful to gain server access (0%).

3) Connection delay.

a) The average time used as a standard server connection is 0.8 seconds recorded in the system.

b) The average connection time to the system using RSA plus OTP increased to 3.2 seconds due to the additional authentication process. This increase is still within the reasonable range, considering the additional layer of security.

4) Resource consumption.

a) There was a spike in CPU usage of around 5% since the OTP process with RSA decryption was implemented.

b) Although these improvements do not have a significant impact on the stability or overall performance of the server system,

5) The comparison of the findings that have been carried out is in accordance with research conducted by Kurniawan (2021), which states that a combination of using the port knocking method and OTP authentication can reduce the risk of exploitation by up to 90% on a system with open ports.

4. CONCLUSION.

The use of RSA-based Port Knocking combined with OTP verification has proven to be more effective in increasing SSH security access, especially on a server that can store a lot of military personnel data. This system can prevent port scanning and brute force attacks and can maintain connection effectiveness. For further research, my suggestion is that the system can be further developed by integrating an anomaly detection system or using AI to strengthen a server's security mechanism.

5. CLOSING

This research demonstrates that integrating RSA-based port knocking with OTP verification is a highly effective solution for enhancing SSH access security, particularly on servers handling critical data such as military personnel. This system has been shown to prevent unauthorized access without significantly impacting server performance.

In this way, cybersecurity on servers, particularly military personnel data, can be strengthened through relatively simple yet highly efficient methods and technological applications. Future developments in this system could include the use of biometric authentication, the application

of AI to detect suspicious access patterns, or the integration of logs and real-time monitoring to strengthen server access systems.

REFERENCES

Amir, Z., Syaifuddin, S., & Risqiwati, D. (2020). Implementasi Asymmetric Encryption Rsa Pada Port Knocking Ubuntu Server Menggunakan Knockd Dan Python. *Jurnal Repositor*, *2*(6), 787. https://doi.org/10.22219/repositor.v2i6.270

Dwi, R., & Prakoso, Y. (2022). *IMPLEMENTASI LOW INTERACTION HONEYPOT DAN PORT KNOCKING UNTUK MENINGKATKAN*. *02*(01), 16–23.

Ernawati, R., Ruslianto, I., Bahri, S., Rekayasa, J., & Komputer, S. (2022). Implementasi Metode Port Knocking Pada Sistem Keamanan. *Jurnal Komputer Dan Aplikasi*, *10*(01), 158–169. https://jurnal.untan.ac.id/index.php/jcskommipa/article/download/54226/75676593086

Force, B. (2024). *Arus Jurnal Sains dan Teknologi (AJST) Optimalisasi Sistem Keamanan SSH dari Serangan Brute Force*.

Informatika, J. T., & Bangsa, S. A. (2021). *Optimalisasi Keamanan Jaringan Menggunakan Metode Port Knocking Pada LAZIS Wahdah Jakarta*. *VII*(1), 40–48.

Mardiansyah, A. Z., Abdussyakur, Y. M., & Jatmika, A. H. (2021). Optimasi Port Knocking dan Honeypot Menggunakan IPTables Sebagai Keamanan Jaringan pada Server. *JTIKA (Jurnal Teknologi Informasi, Komputer, Dan Aplikasinya)*, *3*(2), 189–199. https://jtika.if.unram.ac.id/index.php/JTIKA/article/view/144

Putri, I., Agita, A., & Soim, S. (2023). *Implementasi Port Knocking , Port Blocking Pada Keamanan Jaringan Komputer Berbasis Mikrotik*. *6*(3), 125–130.

Reza, M., Cobantoro, A. F., Zulkarnain, I. A., Studi, P., Informatika, T., Teknik, F., Muhammadiyah, U., & Ponorogo, K. (2024). *KNOCKING PADA SISTEM PROGRAM STUDI*. *29*(3), 298–315.

Tohirin, T. (2020). Penerapan Keamanan Remote Server Melalui Ssh Dengan Kombinasi Kriptografi Asimetris Dan Autentikasi Dua Langkah. *Jurnal Teknologi Informasi*, *4*(1), 133–138. https://doi.org/10.36294/jurti.v4i1.1262