JURNAL INFORMATIKA RESONAT ALGORITHM

https://jurnal.unipi.ac.id/index.php/ALGORITHMUS
ISSN ONLINE : ----------

IMPLEMENTASI DAN REKAYASA SISTEM KEAMANAN JARINGAN MENGGUNAKAN METODE PORT KNOCKING PADA MIKROTIK RB-941 SERIES (Studi kasus : Universitas Persatuan Islam)

Tasep Adi Nugraha[1], Errysa Shubekthi [2] ,

[1] Informatika, Universitas Persatuan Islam
[2,]Informatika, Universitas Persatuan Islam

Jl. Peta no. 154 Suka Asih, Bandung, Jawa Barat
tasepunipi@gmail.com , errysa@unipi.ac.id ,

Abstract

Port knocking is a security system that aims to open block acess to certain ports by using a firewall on network devices by sending certain packets or connections. In addintion, the purpose of having multiple conections is in the form of protocols such as TCP, UDP, and ICMP. By using this protocol, we can share information and data easily, quicly, and accurately. Port knocking works by closing all ports on the computer system and only the network administrator can acess a predetermined port, namely by tapping or knocking first. If the connection sent by the host complies with the knocking rules applied, the firewall will dynamically grant access to the port that has been denied.

Keywords: *Port knocking, TCP, UDP, ICMP, Firewall, Mikrotik, Winbox*

Abstrak

Port knocking adalah sistem keamanan yang mempunyai tujuan untuk membuka akses block ke port tertentu dengan menggunakan firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Selain itu tujuan dari adanya beberapa koneksinya berupa protokol seperti TCP, UDP, maupun ICMP. Dengan menggunakan protokol tersebut, berbagi informasi dan data dapat kita dapatkan dengan mudah, cepat, dan akurat. Port knocking bekerja dengan cara menutup semua port yang sudah ditolak.

Kata kunci: Port knocking, TCP, UDP, ICMP, Firewall, Mikrotik, Winbox

1. PENDAHULUAN

Universitas Persatuan Islam (UNIPI) merupakan institusi pendidikan yang berfokus pada bidang Tarbiyah dan Jami'yah, yang kini telah bertransformasi menjadi universitas berdasarkan SK Kemenristedikti Nomor 1271/KPT/1/2018. Seiring dengan perkembangan teknologi informasi, kebutuhan akan jaringan komputer yang stabil dan aman di lingkungan kampus menjadi prioritas utama. Local Area Network (LAN) digunakan di UNIPI untuk mengintegrasikan sumber daya perangkat keras dan perangkat lunak antar unit kerja. Namun, integrasi ini memunculkan tantangan besar dalam aspek keamanan jaringan, terutama pada perangkat router yang menjadi gerbang utama lalu lintas data.

Keamanan jaringan merupakan mekanisme krusial untuk melindungi aset data kampus dari ancaman eksternal maupun internal, seperti pencurian data dan akses ilegal terhadap sistem [1]. Saat ini, infrastruktur jaringan di UNIPI yang menggunakan MikroTik seri RB-941 masih memiliki celah kerentanan pada port layanan administratif seperti Winbox, SSH, dan Telnet. Kondisi port yang terbuka secara permanen memungkinkan pihak tidak berwenang melakukan upaya peretasan atau pengelolaan jaringan secara ilegal. Tanpa adanya proteksi tambahan, router sangat rentan terhadap serangan brute force yang menargetkan kredensial administrator.

Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan penerapan metode port knocking. Teknik ini bekerja dengan cara menutup seluruh port administratif dan

Diterima (tanggal), Direvisi (tanggal), Diterima untuk publikasi (tanggal)

hanya akan membukanya secara dinamis apabila sistem menerima urutan paket data atau "ketukan" khusus dari pengguna yang sah. Beberapa penelitian terdahulu telah membuktikan efektivitas metode ini. menyatakan bahwa port knocking mampu meningkatkan keamanan pada MikroTik RouterOS secara signifikan [2]. Penelitian lain mengombinasikan port blocking dan port knocking pada seri RB-941 untuk memperkuat pertahanan jaringan [3]. Selain itu, penggunaan IP Tables sebagai firewall pendukung juga telah dikaji oleh Al Amin guna mengoptimalkan penyaringan paket [4].

Meskipun penelitian mengenai port knocking telah banyak dilakukan, implementasi spesifik pada infrastruktur Universitas Persatuan Islam memiliki karakteristik unik terkait topologi dan kebutuhan akses administratifnya. Penelitian ini bertujuan untuk melakukan rekayasa sistem keamanan pada MikroTik RB-941 melalui metode port knocking guna menutup celah ilegal pada port layanan. Kebaruan dari penelitian ini terletak pada optimasi aturan firewall yang disesuaikan dengan kondisi realita di UNIPI untuk menciptakan sistem autentikasi sebelum akses port terbuka sepenuhnya.

2. TINJAUAN PUSTAKA

2.1 Rekayasa Perangkat Lunak (RPL)

Sistem biasanya terdiri dari sebuah program terpisah dan file konfigurasi yang digunakan untuk menyiapkan sebuah program. Ini mungkin termasuk dokumentasi sistem yang menggambarkan struktur sistem, dokumentasi pengguna, yang menjelaskan cara menggunakan sistem (Rachmad, 2022).

Dapat disimpulkan bahwa rekayasa perangkat lunak adalah sebuah bidang yang mendalami cara-cara mengembangkan sebuah perangkat lunak didalamnya termasuk manajemen, pemeliharaan, pembuatan dan pengembangan

2.2 Keamanan Jaringan

Keamanan komputer digunakan untuk mengontrol pengguna komputer dan keamanan komputer yang dimaksud adalah yang terhubung ke dalam sebuah jaringan (Etie Nur Hartiwati, 2021). Dapat disimpulkan bahwa keamanan jaringan terdiri dari kebijakan dan praktik yang diterapkan untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, modifikasi, atau penolakan jaringan komputer dan sumber daya yang dapat diakses.

2.3 Port Knocking

Port knocking memliki metode buka port kepada suatu client bila client meminta, dan tutup kembali bila client telah selesai. Untuk menjalankan metode ini, sebuah server haruslah memiliki firewall dan daemon untuk menjalankan metode port knocking yang berjalan di server tersebut (Rometdo Muzawi, 2016). Port knocking adalah sebuah metode sederhana untuk memberikan akses remote tanpa meninggalkan port dalam keadaan selalu terbuka. Dapat disimpulkan bahwa port knocking adalah suatu metode komunikasi dua arah yaitu antara client dan server dimana metode ini diterapkan dalam suatu sistem dengan port tertutup

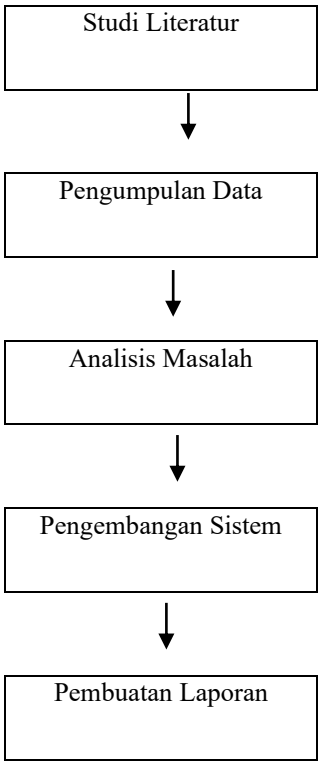
2.2 Penelitian Terdahulu

Penelitian terdahulu digunakan sebagai bahan referensi dan penguat dalam pelaksanaan penelitian ini. Adapun penelitian yang relevan adalah sebagai berikut: Analisis dan perencanaan system

A. Amarudin pada tahun 2018 mengawali kajian ini dengan melakukan analisis implementasi keamanan pada MikroTik Router OS, yang menyimpulkan bahwa metode port knocking secara signifikan mampu meminimalisir risiko serangan langsung pada port administratif [2]. Selanjutnya, Rizal dkk. (2020) mempersempit ruang lingkup penelitian dengan mengimplementasikan kombinasi port blocking dan port knocking khusus pada perangkat MikroTik seri RB-941. Hasil penelitian tersebut menunjukkan bahwa meskipun perangkat memiliki spesifikasi perangkat keras yang terbatas, metode ini tetap mampu memberikan perlindungan optimal tanpa membebani performa CPU router secara berlebihan [3].
B. pengembangan metode ini juga dilakukan melalui integrasi dengan sistem firewall lainnya. Al Amin (2020) meneliti penggunaan IP Tables sebagai firewall pendukung untuk mengoptimalkan mekanisme knocking, sehingga penyaringan paket data menjadi lebih selektif [4]. Relevansi penggunaan metode ini pada instansi pendidikan juga dibuktikan oleh Julkarnain dan Afahar (2021) melalui studi kasus di SMKN 1 Sumbawa Besar, yang menunjukkan bahwa port knocking menjadi solusi praktis bagi administrator jaringan sekolah dalam mengelola akses jarak jauh secara aman [5]. Terakhir, Mardiansyah dkk. (2021) melakukan optimasi lebih lanjut dengan menggabungkan port knocking dan sistem honeypot. Penelitian tersebut menekankan bahwa selain menutup akses, sistem juga dapat digunakan untuk menjebak penyusup yang mencoba melakukan pemindaian jaringan (port scanning) [6].

3. METODE PENELITIAN

Untuk memberikan paduan dalam penyusunan pendekatan ini, maka perlu adanya kerangka kerja (frame work) yang jelas tahapan-tahapannya. Kerangka kerja ini merupakan langkah-langkah yang akan dilakukan dalam penyelesaian masalah yang akan dibahas. Adapun kerangka kerja penelitian yang digunakan adalah sebagai berikut Pada



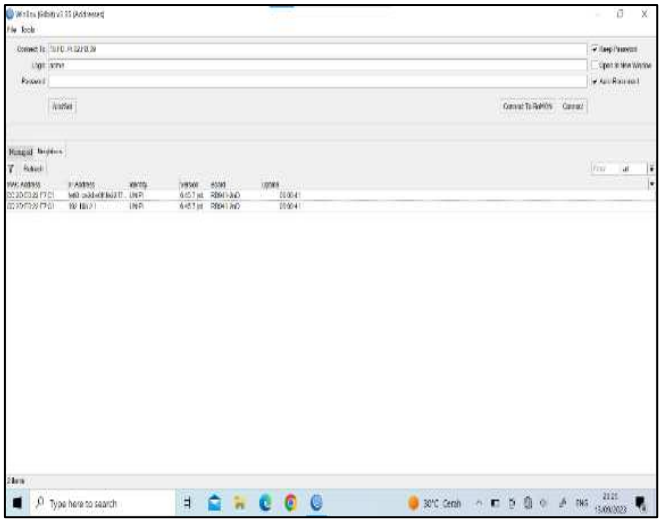
Gambar 3.1 Metode Penelitian

3.1 Metode Penelitian

Metodologi penelitian ini diawali dengan tahapan studi literatur untuk membangun landasan teoritis yang kuat melalui eksplorasi berbagai referensi ilmiah terkait keamanan jaringan. Proses pengumpulan data dilakukan secara komprehensif melalui empat teknik utama, yaitu observasi langsung terhadap infrastruktur jaringan lokal (LAN) di Universitas Persatuan Islam, wawancara mendalam dengan pihak pimpinan dan staf IT untuk mengidentifikasi kendala sistemik, serta dokumentasi seluruh rangkaian kegiatan penelitian. Selain itu, penyebaran angket kepada civitas akademika yang meliputi mahasiswa, dosen, dan staf BAK dilakukan untuk memperoleh perspektif pengguna sekaligus validasi dari para ahli mengenai kondisi riil keamanan jaringan di lingkungan kampus.

4. HASIL DAN PEMBAHASAN

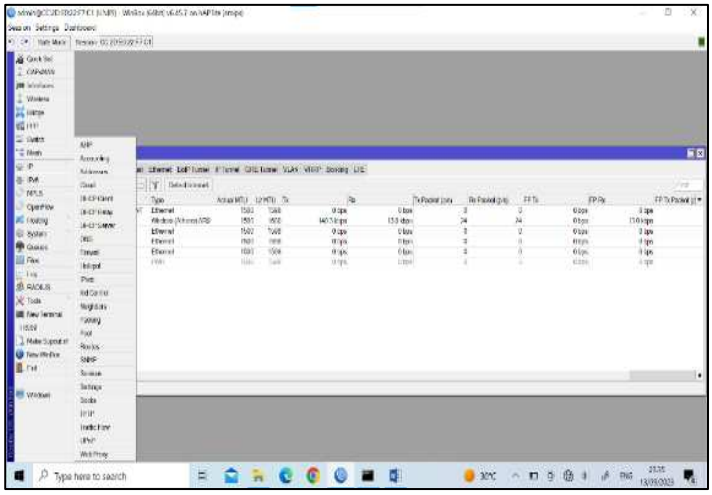
1) Tahapan Pengujian Akses Tanpa Melakukan Knocking



Gambar 4.1 Pengujian Akses Tanpa Melakukan Knocking

tahapan otentikasi awal untuk mengakses sistem manajemen jaringan dilakukan melalui antarmuka utama perangkat lunak konfigurasi. Prosedur akses ini melibatkan dua langkah krusial, yaitu pemilihan identitas perangkat target melalui klik pada alamat fisik (MAC Address) atau alamat logis (IP Address) yang terdeteksi, kemudian dilanjutkan dengan menekan tombol Connect untuk menginisiasi sesi komunikasi dengan router. Langkah ini merupakan pintu masuk utama bagi administrator sebelum dapat melakukan konfigurasi lebih lanjut, termasuk dalam menerapkan aturan firewall dan metode port knocking pada sistem.

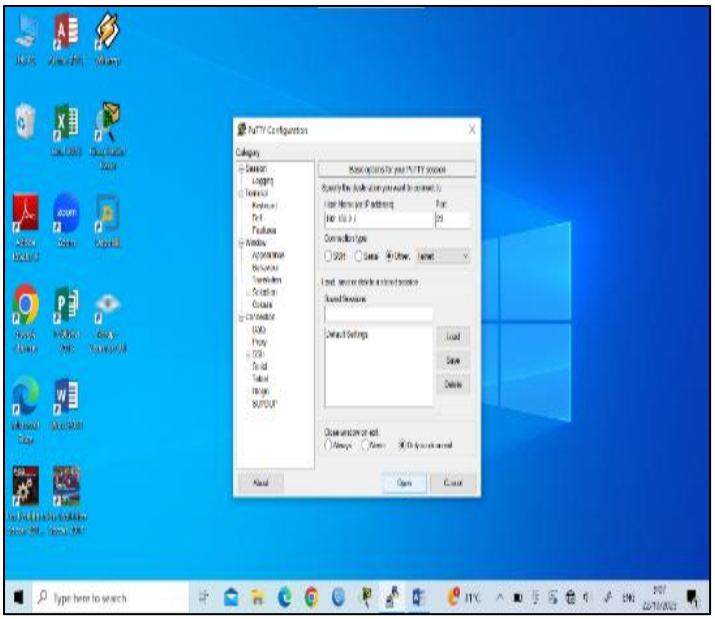
2) Interface mikrotik setelah login



Gambar 4.2 Pengujian Akses Tanpa Melakukan Knocking

Setelah proses autentikasi berhasil dilakukan, Gambar IV.2 menampilkan tampilan antarmuka utama (interface) sistem operasi MikroTik (RouterOS) yang menyediakan akses menyeluruh terhadap berbagai fitur manajemen jaringan. Pada jendela utama ini, administrator dapat memantau status perangkat secara real-time serta mengakses menu navigasi di sisi kiri untuk melakukan konfigurasi spesifik, seperti pengaturan IP Address, Interfaces, dan khususnya menu Firewall yang menjadi modul utama dalam pengimplementasian metode port knocking. Tampilan ini mengonfirmasi bahwa koneksi antara komputer administrator dan router RB-941 telah terjalin dengan stabil, sehingga rekayasa sistem keamanan pada port layanan dapat segera dilaksanakan.

3) Mengakses Port 23 (Telnet) menggunakan Knocking



Gambar 4.3 Koneksi Telnet melalui aplikasi Putty

Pada tahap ini, administrator diwajibkan melakukan pengujian konektivitas guna memastikan bahwa sesi komunikasi terjalin secara sempurna sebelum akses administratif diberikan sepenuhnya. Penggunaan aplikasi pihak ketiga seperti Putty ini berfungsi sebagai instrumen untuk memvalidasi apakah sistem keamanan yang sedang dirancang dapat mengenali permintaan koneksi pada port tertentu, yang menjadi bagian krusial dalam mekanisme autentikasi sebelum metode port knocking membuka akses secara dinamis.

5. KESIMPULAN

Penelitian ini merupakan penelitian kualitatif yang bertujuan untuk mendeskripsikan implementasi dan rekayasa sistem keamanan jaringan menggunakan metode port knocking pada mikrotik RB-941 series di kampus Universitas Persatuan Islam. Data diperoleh dengan melakukan observasi, wawancara langsung kepada pihak kampus, dokumentasi, mengambil sampel dari beberapa civitas akademika Universitas Persatuan Islam dan beberapa ahli dibidangnya.

Berdasarkan hasil penelitian, dapat disimpulkan bahwa penerapan sistem keamanan jaringan menggunakan metode port knocking untuk melindungi perangkat mikrotik dari berbagai ancaman dari luar cukup efektif. Ini dibuktikan dengan proses dan tahapan yang harus dilalui oleh user atau admin yang ingin masuk pada perangkat mikrotiknya cukup rumit. Proses yang dimaksud cukup rumit ialah beberapa tahapan yang harus dilalui sebelum dapat mengakses perangkat mikrotik yaitu menjalankan protokol ICMP, menjalakan Telnet, dan menjalankan SSH

DAFTAR PUSTAKA

[1] Mustofa Alif Tomy, Sutanta Edhy, Akbar Triyono Joko. “Perancangan dan Implementasi Sistem Monitoring Jaringan Wi-Fi Menggunakan Mikhom Online di Wisma Muslim Klitren Gondokusuman Yogyakarta”. Jurnal JARKOM Vol. 7, No. 2, Desember (2019) : 67..

[2] Amarudin, "Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," Jurnal Teknologi dan Sistem Informasi, vol. 4, no. 2, pp. 1-10, 2018.

[3] R. Rizal, Ruuhwan, and K. A. Nugraha, "Implementasi Keamanan Jaringan Menggunakan Port Blocking dan Port Knocking Pada Mikrotik RB-941," Jurnal Informatika, vol. 7, no. 1, pp. 45-52, 2020..

[4] J. Al Amin, "Implementasi Keamanan Jaringan dengan IP Tables Sebagai Firewall Menggunakan Metode Port Knocking," Jurnal Teknik Informatika, vol. 5, no. 2, 2020.

[5] M. Julkarnain and A. Afahar, "Implementasi Port Knocking Untuk Keamanan Jaringan SMKN 1 Sumbawa Besar," Jurnal Informatika dan Teknologi, vol. 4, no. 1, pp. 20-28, 2021.

[6] A. Z. Mardiansyah, Y. M. Abdusyakur, and A. H. Jatmika, "Optimasi Port Knocking Dan Honeypot Menggunakan IP Tables Sebagai Keamanan Jaringan Pada Server," Jurnal Komputer dan Informatika, vol. 9, no. 1, 2021

[7] D. Demira and R. Wiryadinata, "Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking," Jurnal Teknik Elektro dan Komputer, vol. 11, no. 3, 2022

[8] A. Wahyudin, E. Subkthi, C. Abbas, and Andriansyah, "Audit Keamanan Internet Service Provider Menggunakan Standar ISO 27001 : 2022 (Studi Kasus : Mini ISP Namnet SMKN 6 Garut)," Informatika, Universitas Persatuan Islam, 2025.

[9] Andriansyah, "Rancang Bangun Sistem Informasi Persediaan Barang Berbasis Web (Studi Kasus: SMA Negeri 19 Garut)," Informatika, Universitas Persatuan Islam, 2025.

[10] A. Safitri, E. Subkthi, D. Alamsyah, and Andriansyah, "Rancang Bangun Sistem Informasi Kepegawaian Berbasis Web (Studi Kasus: SMA Negeri 19 Garut)," Informatika, Universitas Persatuan Islam, 2025.

[11] N. Aisah, E. Subkthi, C. Abbas, and Andriansyah, "Rancang Bangun Sistem Informasi Pembayaran SPP Berbasis Web (Studi Kasus: SMA Negeri 19 Garut)," Informatika, Universitas Persatuan Islam, 2025.

[12] Aulia, E. Subkthi, C. Abbas, and Andriansyah, "Rancang Bangun Sistem Informasi Akademik Berbasis Web (Studi Kasus: SMA Negeri 19

Garut)," Informatika, Universitas Persatuan Islam, 2025.

[13] Hermawan, E. Subkthi, D. Alamsyah, and Andriansyah, "Rancang Bangun Sistem Manajemen Simpan Pinjam Koperasi Berbasis Web (Studi Kasus: SMPN 2 Cisurupan)," Informatika, Universitas Persatuan Islam, 2025.

[14] L. N. Wida, E. Subkthi, D. Alamsyah, and Andriansyah, "Sistem Informasi Geografis Pemetaan Lokasi UMKM Berbasis Web (Studi Kasus: Kelurahan Ciwalen)," Informatika, Universitas Persatuan Islam, 2025.

[15] P. Nurmansyah, E. Subkthi, C. Abbas, and Andriansyah, "Rancang Bangun Sistem Manajemen Inventaris Barang Berbasis Web (Studi Kasus: Kantor Kecamatan Karangpawitan)," Informatika, Universitas Persatuan Islam, 2025.