

# IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN PORT KNOCKING

Yuniaman Mendrofa<sup>1</sup>, Rahmat Fauzi<sup>2</sup>

<sup>1</sup>Mahasiswa Program Studi Teknik Informatika, Universitas Putera Batam

<sup>2</sup>Dosen Program Studi Teknik Informatika, Universitas Putera Batam  
*email:pb190210054@upbatam.ac.id*

### ABSTRACT

*Technological advancements continue to progress rapidly, allowing experts to enhance their knowledge across various industries, including health, network security, and others. PT Air Batam Hulu is a water company situated at Building A-WTP Moya Muka Kuning Jl. Letjend Supranto in Batam, responsible for managing the security of drinking water. However, the company's existing system is susceptible to data security breaches due to unauthorized hacking attempts. In addition, computer network systems face both physical and logical threats, such as Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Cracker, and more. Among the current successful hacking attempts, UML sites, Malware, Trojans, Viruses, and port scanning are commonly encountered. To address security concerns, the company implements a security system called "port knocking," which involves opening or closing access to specific ports through the use of a firewall on network devices. This system works by sending certain packets or connections, including TCP, UDP, and ICMP protocols. To gain access to restricted ports, users are required to perform a "knocking" action by inputting the necessary rule beforehand. This ensures that only authorized users can access and use specific ports, enhancing data security and reducing the risk of unauthorized infiltration.*

**Keywords** Network; Security; Port Knocking

### PENDAHULUAN

Perkembangan teknologi dari hari kehari semakin meningkat, dimana para ahli mengembangkan ilmu pengetahuannya baik dalam bidang industri, kesehatan, keamanan jaringan dan lainnya. Semakin meluasnya perkembangan pembangunan terhadap teknologi semakin banyak juga pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan, oleh sebab itu maka aplikasi yang digunakan oleh pengguna yang terhubung secara langsung dengan internet harus mewaspadain terjadinya

penyusupan oleh pihak yang tidak berwenang, karena pada saat sekarang ada banyak pengguna internet menjadi korban penyusupan. Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML*, *Malwere*, *Trojan*, *Virus*, dan pemindaian *port*. Menggunakan jaringan, pemindaian port adalah sebuah metode untuk menemukan *port* komputer yang terbuka.

PT Air Batam Hulu adalah sebuah perusahaan yang beralamat Gedung A-WTP Moya Muka Kuning Jl.Letjend Supranto merupakan perusahaan air dibatam yang menjaga keamanan

pengelolaan air minum. Namun pada sistem yang digunakan oleh perusahaan masih terdapat Pihak-pihak yang tidak berwenang melakukan peretasan. Oleh karena itu, keamanan data menjadi rawan terhadap upaya penyusupan. Dalam konteks suatu sistem jaringan komputer, terdapat variasi ancaman baik dari sisi fisik maupun logika, seperti *Sniffer*, *Spoofing*, *Breaking*, *Remote Attack*, *Hole*, *Hacker*, *Cracker*, dan ancaman lainnya. Saat ini, sering terjadi kasus berhasil diretas yang menyebabkan penyusupan, misalnya pada situs UML, *Malware*, Trojan, Virus, dan juga pemindaian *port*.

Jaringan komputer merupakan kumpulan atau kelompok dari dua komputer atau lebih yang saling terhubung dengan tujuan untuk memungkinkan berbagi informasi dan data dengan akurat. Keamanan jaringan komputer, yang dikenal sebagai *Network Security*, memiliki hubungan yang erat dengan keamanan data. Oleh karena itu, keamanan jaringan memainkan peran yang sangat penting dalam melindungi data dari akses oleh pihak-pihak yang tidak berwenang. Serangan dapat ditujukan kepada berbagai jenis instansi, perusahaan, atau lembaga tertentu.

*Port knocking* adalah sebuah mekanisme keamanan yang bertujuan untuk mengontrol akses ke *port* tertentu dengan menggunakan *firewall* pada perangkat jaringan. Caranya adalah dengan mengirimkan paket atau koneksi tertentu dalam bentuk protokol TCP, UDP, maupun ICMP. Sebelum pengguna dapat mengakses dan menggunakan akses ke port yang telah dibatasi, mereka harus melakukan tindakan "mengetuk" terlebih dahulu dengan memasukkan aturan (*rule*) yang telah ditentukan sebelumnya. Aturan ini hanya diketahui

oleh pihak penyedia jaringan (administrator jaringan).

## KAJIAN TEORI

### 2.1 Jaringan

Jaringan komputer merupakan kumpulan atau kelompok terminal komunikasi yang terdiri dari dua komputer atau lebih, yang terhubung satu sama lain dengan tujuan untuk berbagi informasi dan data secara akurat. Selain itu, peran jaringan komputer juga penting dalam mengintegrasikan data antar komputer-komputer klien agar mendapatkan data yang relevan. Namun, dalam sistem jaringan komputer, terdapat berbagai bentuk ancaman baik dari sisi fisik maupun logika, seperti *Sniffer*, *Spoofing*, *Breaking*, *Remote Attack*, *Hole*, *Hacker*, *Cracker*, dan lainnya. (Amien et al., 2020).

### 2.2 Firewall

Sistem *Firewall* adalah suatu sistem yang terpasang pada perangkat keras dan perangkat lunak untuk tujuan melindungi, membatasi, memfilter, atau bahkan menolak aktivitas dari segmen jaringan lokal menuju jaringan eksternal yang berada di luar cakupannya. Tujuan utama dari Firewall adalah memastikan bahwa tidak ada akses yang diizinkan dan telah ditetapkan di luar rentang yang telah ditetapkan. (Riska et al., 2018)

sebagai router jaringan..



**Gambar 1 Firewall**

Sumber: (Santoso et al., 2022)



**Gambar 2 Mikrotik**

Sumber: (Ontoseno et al., 2017)

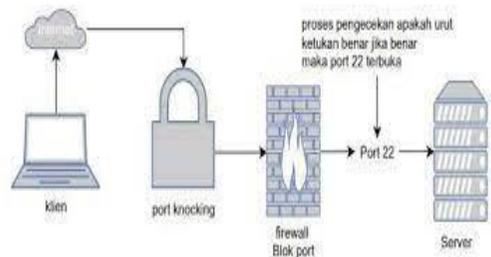
### 2.3 Mikrotik

Berlandaskan pada penelitian (Frado Pattipeilohy, 2016), diketahui bahwa MikroTik adalah sistem operasi berbasis Linux yang dirancang khusus sebagai *router* jaringan. Tujuan utamanya adalah memberikan kemudahan bagi pengguna dalam melakukan administrasi, dan hal ini dapat dilakukan melalui media PC.

Sementara berlandaskan pada penelitian (Asep & Dedi, 2020) Pada awalnya, MikroTik merupakan perusahaan kecil yang berbasis di Riga, Latvia, sebuah negara di Eropa. Perusahaan ini didirikan oleh John Trully dan Arnis Riekstins pada tahun 1995. Awalnya, banyak orang mengenal MikroTik sebagai perangkat router daripada sebagai perusahaan. Sementara itu, menurut (Ontoseno et al., 2017), MikroTik adalah sistem operasi komputer dan perangkat lunak yang digunakan untuk mengubah komputer biasa menjadi router. Sistem operasi MikroTik berbasis Linux dan digunakan

### 2.4 Port Knocking

*Port knocking* adalah sebuah mekanisme keamanan yang bertujuan untuk mengatur akses ke port tertentu dengan menggunakan firewall pada perangkat jaringan. Caranya adalah dengan mengirimkan paket atau koneksi spesifik dalam bentuk protokol TCP, UDP, atau ICMP. Dengan demikian, untuk mendapatkan akses ke port yang dibatasi, pengguna harus "mengetuk" terlebih dahulu dengan memasukkan aturan (rule) yang telah ditentukan sebelumnya. Aturan ini hanya diketahui oleh pihak penyedia jaringan (administrator jaringan). Dalam implementasinya, sistem harus mencapai keseimbangan yang baik antara tingkat keamanan dan fleksibilitas yang diberikan (Sembiring et al., n.d.)



**Gambar 3 Port Knocking**

Sumber : (Ontoseno et al., 2017)

## 2.5 Tools/Software Pendukung

### 1. modem

Modem, merupakan sebuah perangkat yang berfungsi untuk menyambungkan perangkat komputer, laptop dan smartphone ke jaringan internet.



**Gambar 4** Modem

Sumber: (Riska et al., 2018)

### 2. Winbox

Winbox adalah aplikasi manajemen jarak jauh yang dikembangkan oleh MikroTik, dan aplikasi ini dirancang untuk memberikan antarmuka grafis (GUI) yang intuitif untuk mengatur dan mengelola perangkat MikroTik RouterOS. Landasan teori Winbox terutama berfokus pada cara pengguna berinteraksi dengan perangkat MikroTik melalui GUI yang mudah digunakan. Dengan adanya antarmuka grafis, pengguna yang tidak terlalu terampil dalam *command-line interface* (CLI) dapat dengan mudah melakukan konfigurasi dan mengelola perangkat MikroTik.

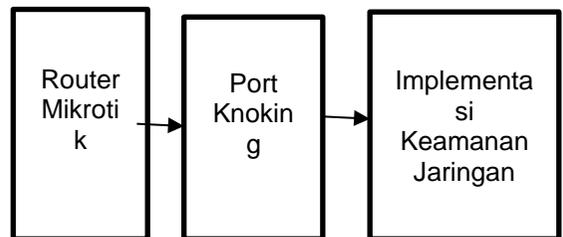


**Gambar 5** Winbox

Sumber: (Riska et al., 2018)

## 2.6 Kerangka Pemikiran

kerangka pemikiran adalah dasar atau konsep-konsep yang menjadi landasan atau pijakan untuk merancang atau mengembangkan sebuah penelitian atau proyek. Kerangka pemikiran berfungsi sebagai panduan dalam mengidentifikasi masalah penelitian, merumuskan hipotesis atau tujuan, serta merencanakan metode atau pendekatan yang akan digunakan dalam penelitian. Dalam penelitian ini kerangka pemikiran yang digunakan adalah sebagai berikut.



**Gambar 6** Kerangka Pemikiran

Sumber Data penelitian 2023.

Sistem keamanan jaringan untuk melindungi router mikrotik dengan menggunakan port knocking dalam mengimplementasi keamanan

jaringan informasi mencegah penyerang mengakses router mikrotik.

**Sumber:** Data Penelitian 2023

## METODE PENELITIAN

### 3.1 Desain Penelitian

Langkah berikutnya bagi seorang peneliti adalah merancang desain penelitiannya dan membentuk struktur atau tahapan yang menggambarkan jalannya penelitian. Hal ini dapat dilakukan dengan membuat bagan atau skema agar penelitian lebih terfokus pada tujuan yang ingin dicapai..



**Gambar 7** Desain Penelitian

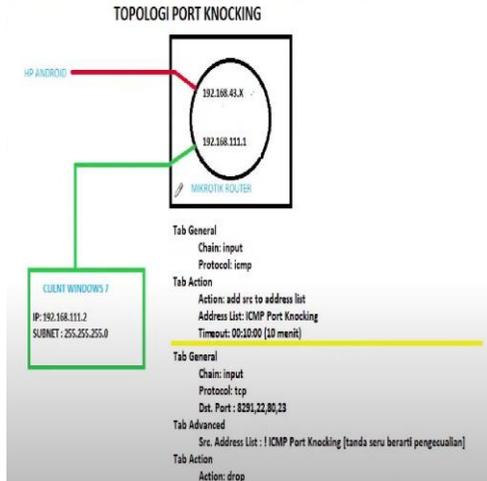
### 3.3 Tahap Desain

### 3.2 Tahap Analisis

Tahap ini bertujuan untuk menganalisis kebutuhan masalah yang timbul, menganalisis preferensi pengguna, serta mengevaluasi topologi jaringan yang telah ada saat ini. Metode yang diterapkan dalam tahap ini adalah sebagai berikut:

- a. Wawancara, Dilakukan interaksi wawancara dengan pihak terkait, yaitu PT Air Batam Hulu, untuk membahas mengenai situasi manajemen yang sedang berlangsung saat ini serta aspirasi dan harapan yang diinginkan..
- b. Observasi, melakukan pengamatan Langsung melakukan interaksi dengan PT Air Batam Hulu untuk memperoleh hasil yang lebih valid, yang kemudian akan digunakan sebagai bagian dari analisis atau penelitian lebih lanjut.

Merupakan tahap dilakukannya desain pada pembuatan port knocking.



**Gambar 8** Tahap Desain  
Sumber: Data Penelitian 2023



**Gambar 8** Instal Microtic OS  
Sumber: Data Penelitian 2023

## HASIL DAN PEMBAHASAN

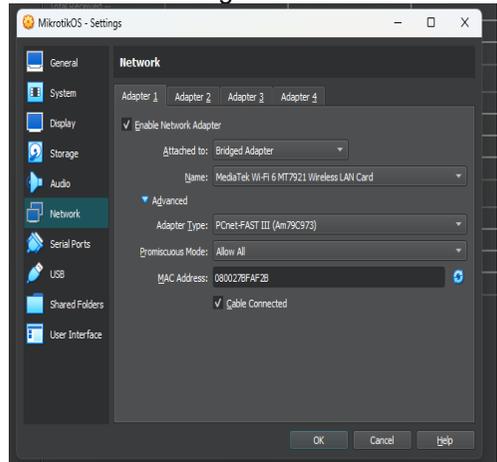
### 4.1 Tahap simulasi

Pada langkah ini, dilakukan simulasi dari desain jaringan yang telah dibuat dengan menggunakan simulator GNS3 dan melakukan konfigurasi pada router untuk menerapkan *port knocking* sebagai langkah untuk mengamankan jaringan. Selain itu, pada tahap ini juga dilakukan simulasi pengujian sistem. Berikut adalah langkah-langkah yang digunakan:

#### 1. Instal Mikrotic OS

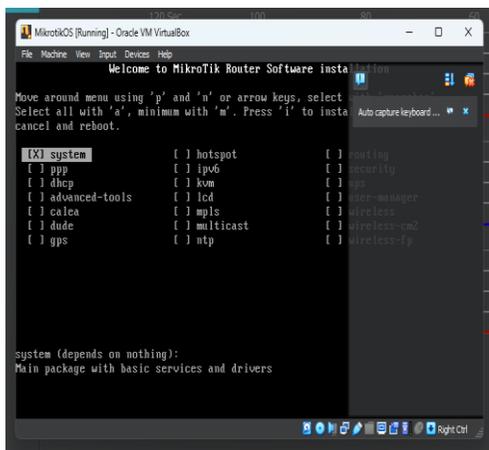
Instal Microtic OS seperti langkah dibawah ini yaitu dengan klik New-Next Hingga Finish.

### 2. Lakukan setting Microsoft OS



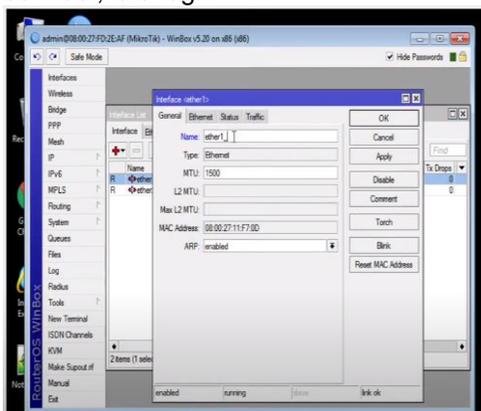
**Gambar 9** Instal Microtic OS  
Sumber: Data Penelitian 2023

Tekan terus dan tunggu hingga selesai terus tekan enter reboot.



**Gambar 10** Instal Microtic OS  
Sumber: Data Penelitian 2023

Pilih atas sendiri yg 192. Terus klik connect, lalu login

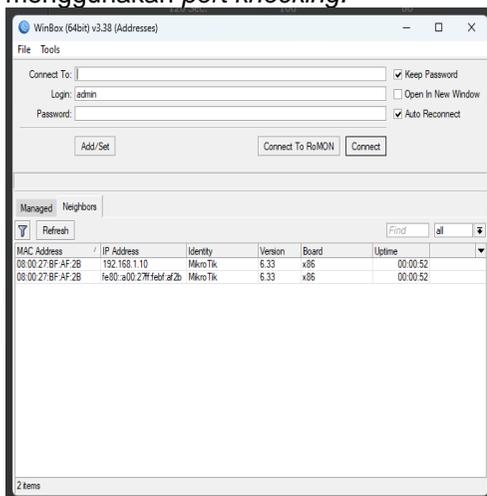


**Gambar 12** winbox  
Sumber: Data Penelitian 2023

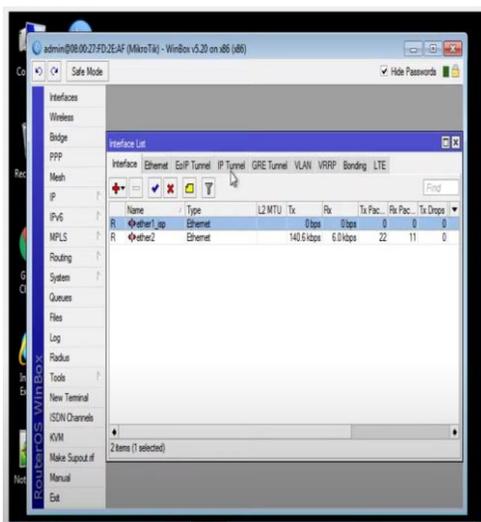
### 3. Simulasi dan prototype

Dalam tahap simulasi ini, winbox dipilih sebagai simulator penelitian karena menyajikan berbagai fitur yang memudahkan dalam perencanaan dan pengaturan keamanan jaringan menggunakan *port knocking*.

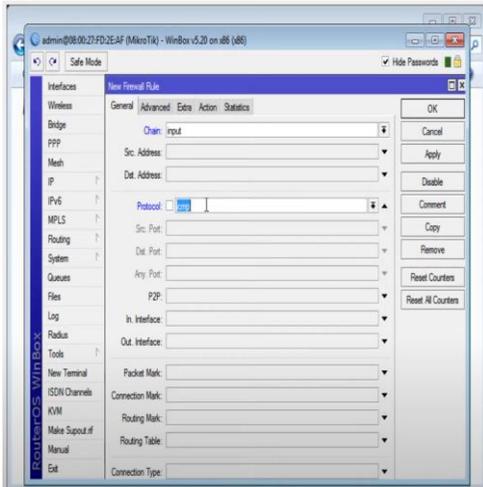
Gambar di atas merupakan antarmuka utama winbox, yang mencakup kolom *login* dan *password*. Untuk mengakses MikroTik, pengguna diharuskan mengisi kolom login dan password yang terdapat pada gambar..



**Gambar 11** winbox  
Sumber: Data Penelitian 2023



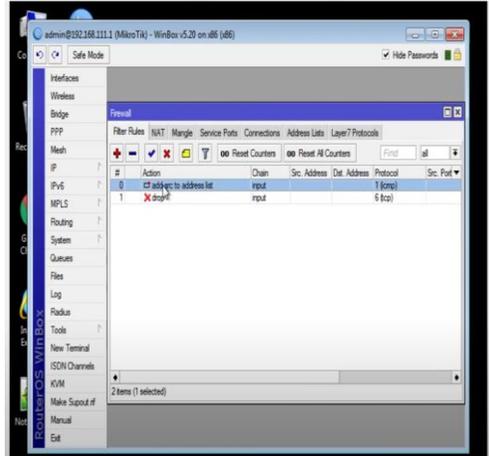
**Gambar 13** winbox  
Sumber: Data Penelitian 2023



**Gambar 13** winbox

Sumber: Data Penelitian 2023

Merupakan tampilan setelah login winbox untuk melakukan konfigurasi dengan mengklik pada menu IP dan menunjukkan pada menu Firewall



**Gambar 15** winbox

Sumber: Data Penelitian 2023

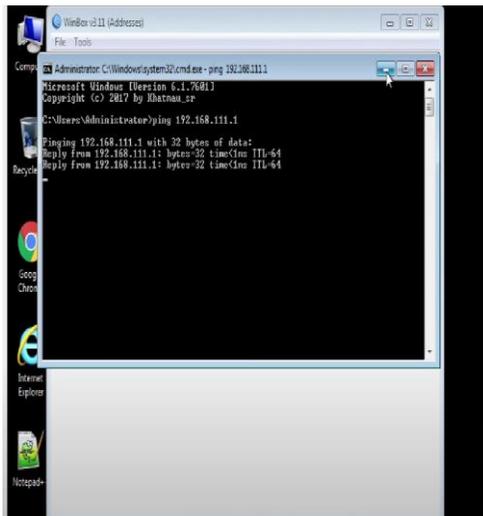
Pada gambar di atas, dilakukan pengujian berbagai konfigurasi port knocking menggunakan perangkat MikroTik. Semua konfigurasi port knocking diuji untuk mengevaluasi kerjanya.

**SIMPULAN**

**Kesimpulan**

Berdasarkan penerapan implementasi metode port knocking untuk keamanan jaringan, dapat diambil kesimpulan sebagai berikut:

1. Dengan menggunakan port knocking dapat membantu port mana yang dapat diakses client, dan jika client tersebut tidak memiliki akses maka tidak dapat berbagi file dan komunikasi dengan server.
2. Sistem yang telah di rancang mampu memberikan penambahan keamanan dalam proses autentifikasi karena port tidak terbuka secara bebas atau public.
3. Tingkat penggunaan sumber daya oleh server lebih stabil sehinggakerja pada server tidak terganggu.



**Gambar 14** winbox

Sumber: Data Penelitian 2023

**DAFTAR PUSTAKA**

Asep, S., & Dedi, S. (2020). Pemanfaatan Mikrotik Untuk Jaringan Hotspot Dengan Sistem Voucher Pada Desa Ujanmas Kota Pagar Alam. *JIRE (Jurnal Informatika & Rekayasa Elektronika)*, 3(2), 4–14.

Frado Pattipeilohy, W. (2016). Analisis dan Perancangan User Manager pada Mikrotik Router dengan Sistem Pembelian Kredit Voucher. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, 5(1), 64. <https://doi.org/10.32736/sisfokom.v5i1.30>

Jurnal, J., & Teknologi, I. (2021). *IMPLEMENTASI PORT KNOCKING UNTUK KEAMANAN JARINGAN SMKN 1*. 3(2), 326–335.

Ontoseno, R. D. H., Haqqi, M. N., & Hatta, M. (2017). Limitasi Pengguna Akses Internet Berdasarkan Kuota Waktu Dan Data Menggunakan Pc Router Os Mikrotik. *Teknika: Engineering and Sains Journal*, 1(2), 125. <https://doi.org/10.51804/tesj.v1i2.134>. 125-130

Riska, P., Sugiartawan, P., & Wiratama, I. (2018). *Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode Port Knocking*. 1(2), 53–64.

Ryansyah, M., & Maulana, M. S. (2018). *Malware Security Menggunakan Filtering Firewall dengan Metode Port Blocking pada Mikrotik RB 1100AHx*. 2. 6(3), 6–10.

Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). *Implementasi Keamanan Jaringan Menggunakan Port Knocking Network Security Implementation Using Port Knocking*. 2(2), 90–95. <https://doi.org/10.25008/janitra.v2i2.156>

. *Penerapan sistem pengamanan port pada layanan jaringan menggunakan port knocking*. 10(2), 45–50.

Ulum, F. (2018). *DESAIN KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS*. 12(2), 72–75.



**Yuniaman Mendrofa**

merupakan mahasiswa Prodi Teknik Informatika dari Universitas Putera Batam yang aktif dalam mendalami bidang teknologi dan informasi.



**Rahmat Fauzi**

merupakan Dosen Prodi Teknik Informatika dari Universitas Putera Batam. Aktif sebagai tenaga kerja dan peneliti.