IMPLEMENTASI PORT KNOCKING UNTUK MENAMBAH KEAMANAN LAYANAN JARINGAN PADA ROUTER MIKROTIK

Sarmila Elvira[1], Aulia Syarif Aziz[2]

Pendidikan Teknologi Informasi, Tarbiyah & Keguruan,
Universitas Islam Negri Ar-Raniry

Jl. Syeikh Abdul Rauf Darussalam, Banda Aceh
Email: [1]200212010@student.ar-raniry.ac.id, [2]aulia.aziz@ar-raniry.ac.id

Abstak: Teknologi informasi saat ini berkembang begitu pesat, baik itu perkembangan pada perangkat keras maupun perangkat lunak, diikuti oleh perkembangan zaman dan kebutuhan manusia yang kian meningkat. Salah satu teknologi informasi yaitu jaringan. Jaringan merupakan salah satu faktor yang secara signifikan memengaruhi keberadaan manusia. Karena jaringan sudah menjadi salah satu komponen utama karena itu hal hal yang menyangkut keamanan tidak dapat diabaikan, oleh sebab itu maka diperlukannya peningkatan keamanan. Tujuan peningkatan keamanan jaringan adalah untuk menghentikan ancaman dari pengguna yang ceroboh melakukan kejahatan. Dari permasalahan tersebut maka diperlukannya sebuah metode keamanan layanan jaringan yang bertujuan untuk mengamankan data dan informasi serta mengurangi resiko penyerangan terhadap jaringan. Maka dari itu peneliti mengimplementasikan *Port Knocking* untuk menambah keamanan layanan jaringan ini menggunakan metode NDLC. Metode ini terdiri dari beberapa tahap yaitu, Anilisis, Desain, Simulasi *Prototype,* Implementasi, Monitoring, dan Manajemen. Dengan adanya project ini dapat meningkatkan keamanan layanan jaringan pada router mikrotik dengan mudah dan efesien. Hasil dari penelitian ini adalah Implementasi *Port Knocking* Untuk Menambah Keamanan Layanan Jaringan Pada Router Mikrotik dengan dibangunnya sistem ini dapat membantu operator Lab B PTI dalam mengelola keamanan layanan jaringan pada Lab tersebut.

Kata kunci: Keamanan, Jaringan, Mikrotik, NDLC, *Port Knocking*

Abstract: *Information technology is currently developing so rapidly, both in terms of hardware and software, followed by the development of the times and increasing human needs. One of the information technologies is the network. The network is one of the factors that significantly affects human existence. Because the network has become one of the main components, therefore, matters concerning security cannot be ignored, therefore, increased security is needed. The purpose of increasing network security is to stop threats from careless users committing crimes. From these problems, a network service security method is needed that aims to secure data and information and reduce the risk of attacks on the network. Therefore, researchers implemented Port Knocking to increase the security of this network service using the NDLC method. This method consists of several stages, namely, Analysis, Design, Prototype Simulation, Implementation, Monitoring, and Management. With this project, it can increase the security of network services on Mikrotik routers easily and efficiently. The results of this study are the Implementation of Port Knocking to Increase Network Service Security on Mikrotik Routers with the construction of this system can help Lab B PTI operators in managing network service security in the Lab.*

Keywords: *Security, Network, Mikrotik, NDLC, Port Knocking*

PENDAHULUAN

Teknologi informasi saaat ini berkembang begitu pesat, baik itu perkembangan pada perangkat keras maupun perangkat lunak, diikuti oleh perkembangan zaman dan kebutuhan manusia yang kian meningkat. Oleh sebab itu maka diperlukannya peningkatan keamanan. Jaringan merupakan salah satu faktor yang secara signifikan memengaruhi keberadaan manusia. Karena jaringan sudah menjadi salah satu komponen utama karena itu hal hal yang menyangkut keamanan tidak dapat diabaikan, oleh sebab itu maka diperlukannya peningkatan keamanan. Tujuan peningkatan keamanan jaringan adalah untuk menghentikan ancaman dari pengguna yang ceroboh melakukan kejahatan. Dari permasalahan tersebut maka diperlukannya sebuah metode keamanan layanan jaringan yang bertujuan untuk mengamankan data dan informasi serta mengurangi resiko penyerangan terhadap jaringan. Maka dari itu peneliti mengimplementasikan *Port Knocking* untuk menambah keamanan layanan jaringan ini menggunakan metode NDLC. Tujuan keamanan jaringan adalah untuk menghentikan pengguna yang ceroboh melakukan kejahatan.

Untuk membuat interaksi pengguna menjadi lebih nyaman, desain jaringan harus di buat sesuai agar nyaman untuk digunakan dan memiliki kualitas keamanan yang kuat, salah satunya seperti pada jaringan komputer yang dapat di atur dengan baik, hal tersebut termasuk menggunakan perangkat lunak terbaru, menggunakan kata sandi yang kuat, dan menghindari terhubung pada jaringan yang tidak aman. Cara ini untuk mempertahankan keamanan jaringan dari bermacam jenis ancaman yang membahayakan.

Keamanan jaringan merupakan upaya proses pencegahan yang dilakukan untuk menghindari serangan yang terhubung kedalam jaringan komputer melewati akses yang tidak sah atau pengguna ceroboh yang mendapatkan keuntungan pribadi dari komputer dan jaringan. Secara garis besar keamanan jaringan mempunyai tujuan untuk meningkatkan kerahasiaan, integritas, dan ketersediaan jaringan.

Menurut Intan Ayu Agita (2023), peningkatan keamanan layanan jaringan yang menggunakan metode *port knocking* memiliki tujuan agar jaringan terhindar dari serangan ancaman yang dapat mengacaukan jaringan. *Port knocking* merupakan teknik yang meminta pengguna untuk melakukan serangkaian tindakan terkendali sebelum dapat mengakses jaringan.

Port knocking menjadi salah satu metode peningkatan keamana layanan jaringan yang terbilang sederhana dan efesien, metode *port knocking* merupakan metode yang berfungsi untuk memblokir akses yang tidak diinginkan, dengan kata lain, jika seseorang perlu mengakses server maka harus melakukan ketukan terlebih dahulu, dan *port* tersebut akan ditutup kembali setelah digunakan, untuk lasan ini diperlukan metode keamanan jaringan yang dapat mencegah ancaman serangan dan meminimalkan jumlah ancaman serangan yang dapat masuk ke sistem jaringan, secara harfiah, arti *port kocking* adalah metode yang membatasi user untuk mengakses router mikrotik..

KAJIAN PUSTAKA DAN LANDASAN TEORI

Keamanan Jaringan

Keamanan jaringan merupakan upaya proses pencegahan yang dilakukan untuk menghindari serangan yang terhubung kedalam jaringan komputer melewati akses yang tidak sah atau pengguna ceroboh yang mendapatkan keuntungan pribadi dari komputer dan jaringan. Secara garis besar keamanan jaringan mempunyai tujuan untuk meningkatkan kerahasiaan, integritas, dan ketersediaan jaringan.

Port Knocking

Port knocking merupakan konsep penting untuk mengamankan layanan yang disediakan oleh server, dengan mengurutkan *port knocking* yang telah diidentifikasikan apakah permintaan tersebut merupakan permintaan sah pada layanan. Pada dasarnya *port knocking* memiliki cara kerja dengan menutup semua *port* yang terbuka dan membatasi akses ke pengguna tertentu dengan mengetuknya terlebih dahulu. Hal ini berbeda dengan cara kerja *firewall*, yang menutup semua port

yang terbuka, terlepas dari apakah pengguna memiliki hak akses atau tidak. *Port knocking* memiliki kelebihan port tersebut dapat di akses oleh user yang memiliki hak meskipun *port* tersebut sudah tertutup.

Mikrotik

Mikrotik adalah perangkat hardware dan software pada jaringan komputer, yang dapat berfungsi sebagai alat Filtering, Router, atau Switc. Mikrotik adalah brand dari perangkat keras RouterBoard dengan sistem operasi RouterOS yang mereka ciptakan, mikrotik ini banyak digunakan karena kemudahan dalam penggunaan, mendapatkan spek yang sama dengan brand yang ladi denganharganya yang terbilang relatif lebih murah.

Winbox

Winbox adalah aplikasi yang digunakan untuk memanajemen mikrotik agar bisa mengkonfigurasi dan mengelola perangkat mikrotik secara grafis. Penggunaan aplikasi ini memberikan kemungkinan pengguna untuk melakukan pengontrolan *firewall*, mengatur jaringan, mengelola user dan password, juga bisa melakukan pemantauan pada perangkat Mikrotik.

METODE

Jenis Pendekatan Penelitian

Network Development Life Cycle (NDCL) didasarkan pada prosedur pengembangan sebelumnya seperti analisis distribusi data, siklus hidup pengembangan aplikasi, dan perencanaan strategi bisnis. Sistem informasi yang memenuhi tujuan pengembangan sistem akan dihasilkan jika teknologi jaringan berhasil diimplementasikan..

Metode NDLC yang memiliki beberapa fase merupakan teknik pengumpulan data yang digunakan dalam penelitian ini. Tahap-tahap tersebut adalah sebagai berikut::

1. Analisis sistem adalah untuk memeriksa isu terkini, preferensi pengguna, dan topologi jaringan. Wawancara, survei, tinjauan data, dan membaca manual atau rencana dokumentasi semuanya dilakukan pada tahap ini.
2. Desain, dikembangkan untuk topologi jaringan yang akan dibangun kemudian menggunakan data yang akan dibangun.
3. Simulasi prototype, Dengan menggunakan alat jaringan khusus seperti Boson, packet, Tracert, VMware, dan lain-lain, kembangkan bentuk simulasi. Ini bertujuan untuk menentukan kinerja awal jaringan serta persentase konten dan pembagian.
4. Implementasi, tahap ini memakan lebih banyak waktu dari pada tahap sebelumnya, ini adalah tahap menerapkan dan menjalankan semua yang telah direncanakan sebelumnya.
5. Monitoring, merupakan fase krusial yang berupaya menjamin bahwa komunikasi dan jaringan komputer dapat berfungsi sesuai dengan preferensi atau tujuan awal.
6. Manajemen merupakan aspek yang sangat penting. Kebijakan harus dibuat atau ditetapkan untuk memastikan bahwa sistem yang telah dibangun dapat berfungsi dengan baik, bertahan lama, dan mempertahankan faktor keandalan.

Teknik Pengumpulan Data

Dalam proses pengimplementasian *port knocking* untuk menambah keamanan jaringan pada router mikrotik ini, diperlukannya data yang akurat. Oleh karena itu, penulis melakukan pengumpulan data dengan beberapa cara yaitu:

1. Wawancara, adalah teknik dalam mengumpulkan data yang dilakukan dengan cara interaksi langsung antara peneliti dan partisipasi peneliti. Tergantung pada tingkat struktur yang telah ditentukan sebelumnya, wawancara dapat dilakukan dengan cara tidak terstruktur, semi terstruktur.
2. Observasi, adalah metode pengumpulan data yang melibatkan pengamatan langsung terhadap orang dan situasi yang terkait dengan topik yang diteliti. Peneliti dapat meneliti interaksi sosial, perilaku, dan lingkungan sekitar

yang berkaitan dengan subjek yang diteliti melalui observasi.

3. Penelitian kepustakaan atau studi pustaka merupakan pengumpulan informasi dari buku-buku dan bahan referensi lain yang berkaitan dengan masalah dan tujuan penelitian. Peneliti akan menganalisis dan mengolah sumber data yang diambil dari buku dan publikasi lainnya. Penelitian dilakukan dengan mengumpulkan sumber- sumber keputusan kepustakaan untuk memproleh informasi yang bersifat teoris.

Teknik Analisis Data

Analisis data merupakan sebuah usaha untuk mencari dan menyusun secara sistematis catatan hasil wawancara, observasi, dan studi pustaka untuk meningkatkan pemahaman peneliti terhadap kasus yang diteliti dan menyajikannya untuk orang lain.

Metode analisa data yang digunakan dalam penelitian ini yaitu kualitatif yang memberikan pengetahuan dan wawasan mendalam tentang konteks dan makna di balik kejadian yang sedang diamati.

Alat-Alat Yang Digunakan

Berikut adalah spesifikasi perangkat keras yang digunakan oleh penulis:

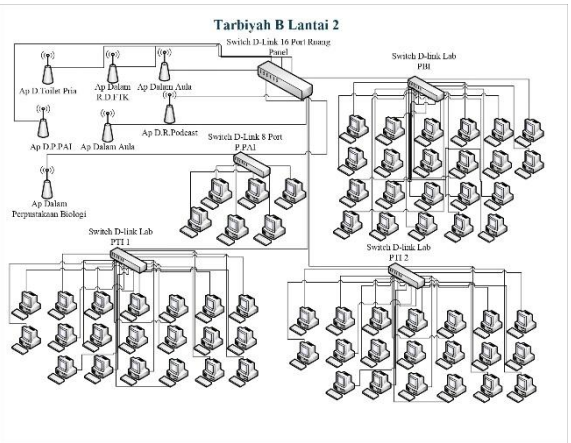
1. Laptop
2. Swich
3. Router Mikrotik
4. Kabel UTP (Cross / Starlight)

Dan berikut adalah spesifikasi perangkat lunak yang digunakan oleh penulis:

1. Winbox
2. Windows 11
3. Draw.io
4. PuTTy

Analisa Sistem Yang Sedang Berjalan

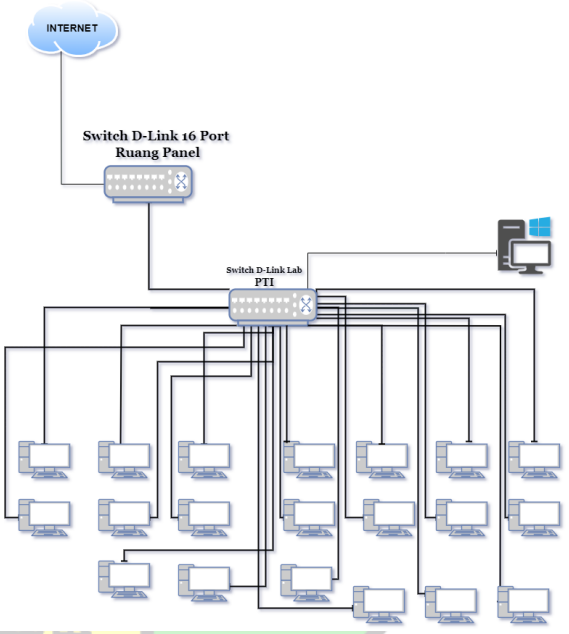
Sistem yang sedang berjalan saat ini, keamanan layanan jaringan gedung tabiyah B sendiri berpusat pada *Information and Comunication Tecnologies* (ICT). Yang dimana *client* mengakses router lalu dikirim ke *firewall fortigate* kemudian dikirim ke internet.



Gambar 1 Analisa Sistem Yang Sedang Berjalan

Topologi Jaringan Laboratorium PTI

Berikut adalah topologi jaringan pada Lab P



TI:

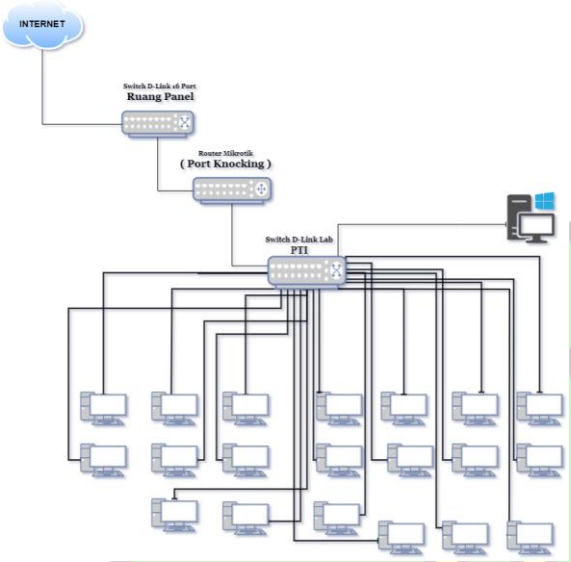
Gambar 2 Topologi Jaringan PTI

Rancangan Penelitian

Sesudah analisa sistem yang sedang berjalan diketahui maka akan lanjut ketahap berikutnya yaitu melakukan perancangan sistem dengan mempebaharui sistem yang lama yang terkomputerasasi. Untuk tahap ini, perlu adanya analisa sistem yang akan dibangun dengan mengidentifikasikan kebutuhan fungsional dan gambaran bagaimana suatu sistem dibentuk.

Rancangan Router Mikrotik Laboratorium PTI

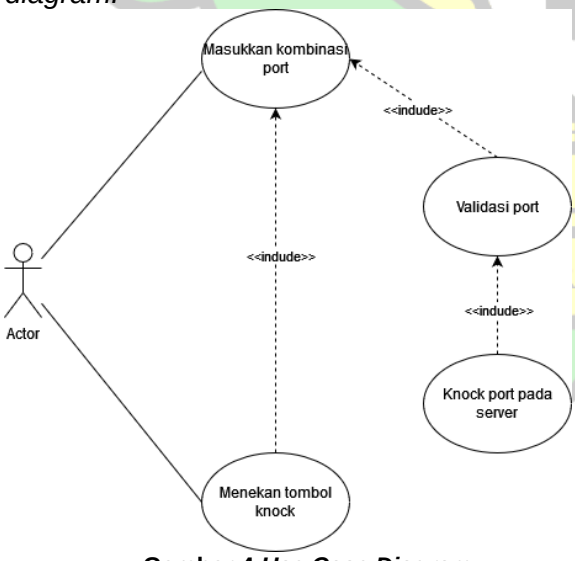
Berikut adalah rancangan router mikrotik Laboratorium PTI di gedung tarbiyah B:



Gambar 3 Rancangan Router Mikrotik Lab PTI

Use Case Diagram

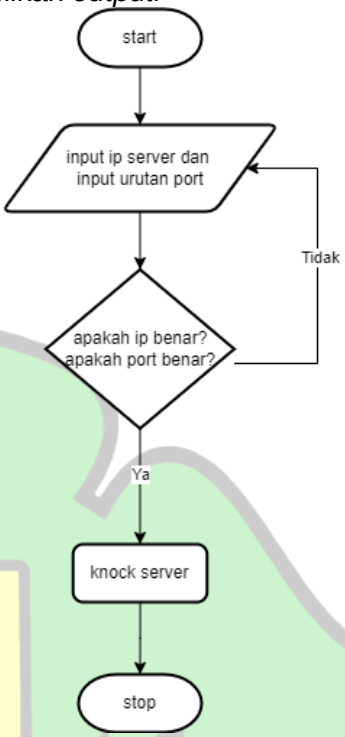
Sistem yang dirancang ini memerlukan tahap pertama yaitu dengan pelaksanaan analisa dari gambaran keseluruhan sistem yang akan dibangun. Gambaran sistem yang akan dibangun nantinya dibentuk dalam *use case diagram.*



Gambar 4 *Use Case Diagram*

Flowchart

Flowchart dijadikan sebagai alat bantu untuk membuat desain logika, tahap ini bertujuan untuk menunjukkan bagaimana alur program yang akan dirancang, mulai dari input data hingga program menghasilkan *output.*



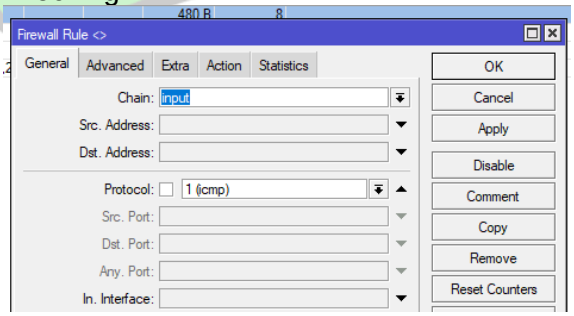
Gambar 5 *Flowchart*

Pada *flowchart* ini setelah user melakukan *start* maka akan diminta untuk *input* IP (*Internet Protocol*) dan *input* urutan *port,* kemudian sistem akan memeriksa IP *server* dan urutan *port* yang sudah di *input* itu benar atau salah, jika benar maka *user* bisa lanjut ketahap *port knocking* namun apabila salah, maka harus kembali menginput IP *server* dan urutan *port* yang benar hingga *port* bisa diakses.

HASIL DAN PEMBAHASAN

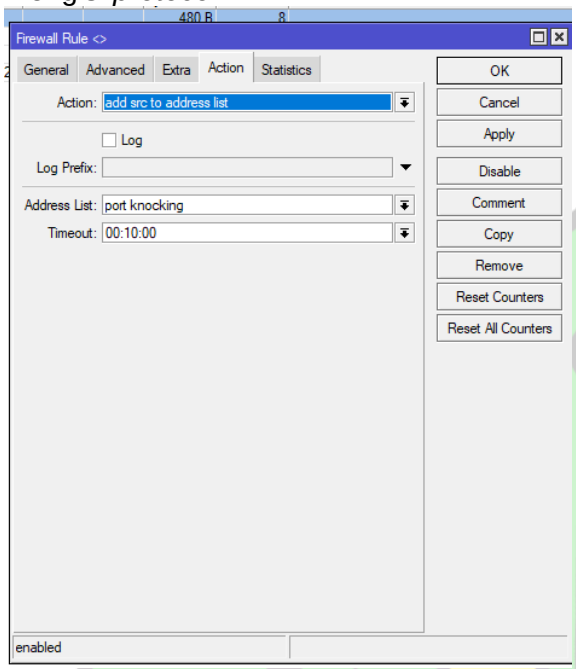
Hasil

Setting mikrotik dengan metode *port* knocking



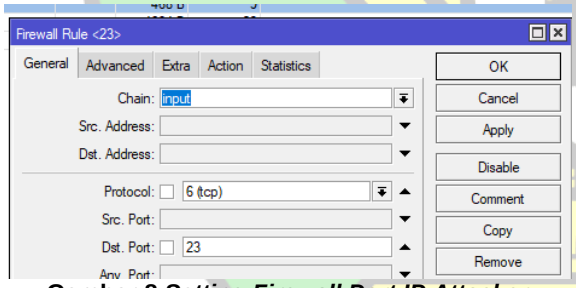
Gambar 6 *Setting Firewall Port Knocking*

Langkah utama untuk mengkonfigurasi *port knocking* adalah pilih menu IP dan klik *Firewall,* pada menu *General* pilih *input* untuk mengisi *Chain,* dan pilih *icmp* untuk mengisi *protocol*.



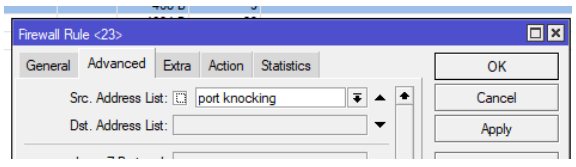
Gambar 7 *Setting Firewall Port IP Legal*

Kemudian pada menu *Action* pilih *add src to address list,* isi *Address List* dan isi *Timeout,* selanjutnya klik *Apply* dan *ok.*



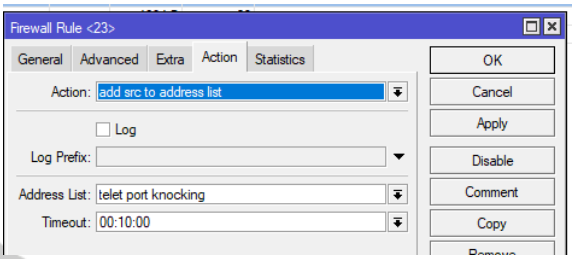
Gambar 8 *Setting Firewall Port IP Attacker*

Kemudian mengatur konfigurasi *port* IP untuk para penyerang kembali lagi kembali ke menu utama dan klik (+) kembali isi *General* dengan *Input* isi *Protocol* dengan 6 (tcp/ *Transmission Control Protocol)* dan isi *Dst. Port* 23 (Telnet).



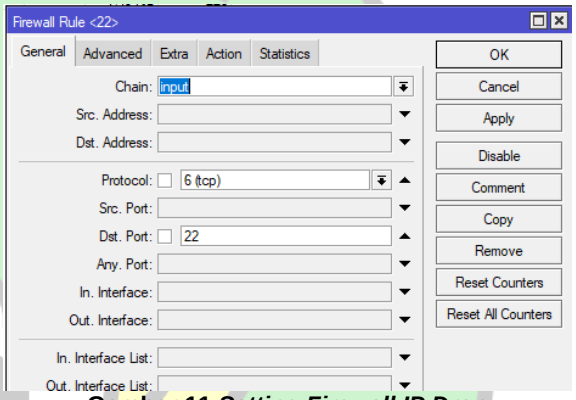
Gambar 9 Pengisian *Advanced*

Klik menu *Advanced* lalu isi *Src.Address Lisst* dengan *Port Knocking* yang sudah di isi pada tahap sebelumnya selanjutnya pilih menu *Action*.



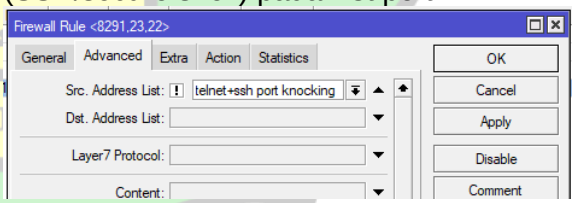
Gambar 10 Pengisian *Action*

Isi *Action* dengan *add src to addres list* lalu isi kembali *Addres list* dengan nama yang berbeda dari tahap selanjutnya kemudian isi *Timeout* lalu *apply* dan *ok.*



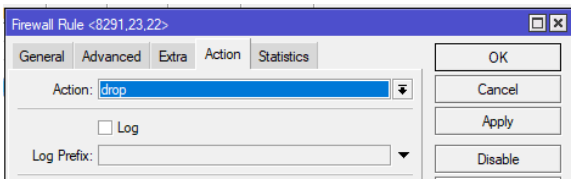
Gambar 11 *Setting Firewall IP Drop*

Pada tahap mengatur konfigurasi *port* IP untuk pengaturan drop melibatkan beberapa langkah, isi Input pada menu General, 6(tcp) pada Protocol dan isi 22 (SSH/*secure shell*) pada Dst.port.



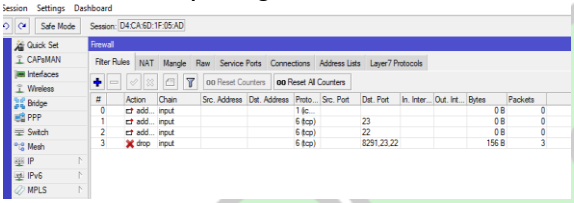
Gambar 12 *Advanced Firewall IP Drop*

Langkah selanjutnya adalah memilih menu Advance, dan isi Src.Address List dengan nama yang tadinya sudah di buat pada tahap sebelumnya, kemudian klik pada kolom hingga muncul tanda seru (!) sebagai tanda pengecualian.



Gambar 13 *Actoin Firewall IP Drop*

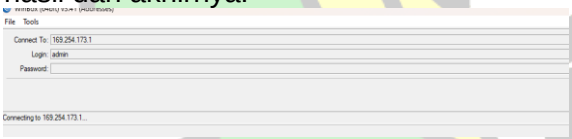
Setelah itu klik menu *Action* isi dengan pilihan Drop lalu klik *Apply* dan Ok. Jika sudah maka tampilan pada menu *Filter Rules* akan seperti gambar 3.8



Gambar 14 Tampilan Pada Menu *Filter Rules*

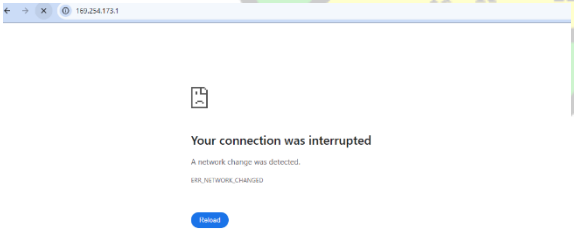
Pembahasan

Setelah melakukan tahap tersebut, tahap selanjutnya yang akan dilakukan adalah tahap pengujian akhir, yang menghasilkan hasil dari penerapan keamanan jaringan yang baru. penerapan peningkatan keamanan tersebut adalah penggunaan metode *Port Knocking*, berikut hasil dari akhirnya.



Gambar 15 Status *Port Knocking* Berhasil

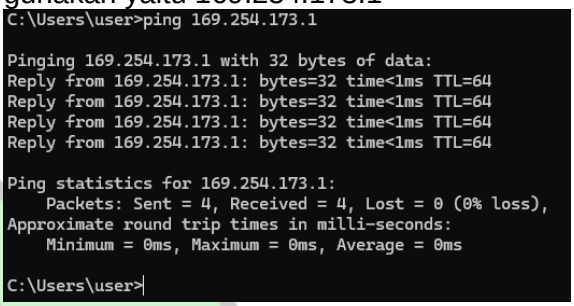
Pengujian secara remote pada router dilakukan melalui winbox dengan menargetkan alamat IP 169.254.173.1, hasilnya tidak bisa mengakses router karena harus melakukan ping terlebih dahulu.



Gambar 16 *Port Knocking* Sebelum Melakukan Ketukan

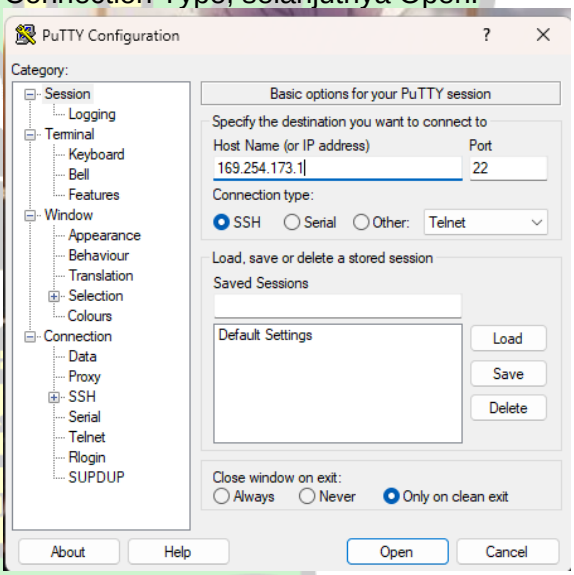
Webfig tidak akan bisa diakses apabila proses ketukan pada *Port Knocking* belum dilakukan.

Ketukan pertama yang dilakukan adalah melakukan ping kepada IP yang di gunakan yaitu 169.254.173.1



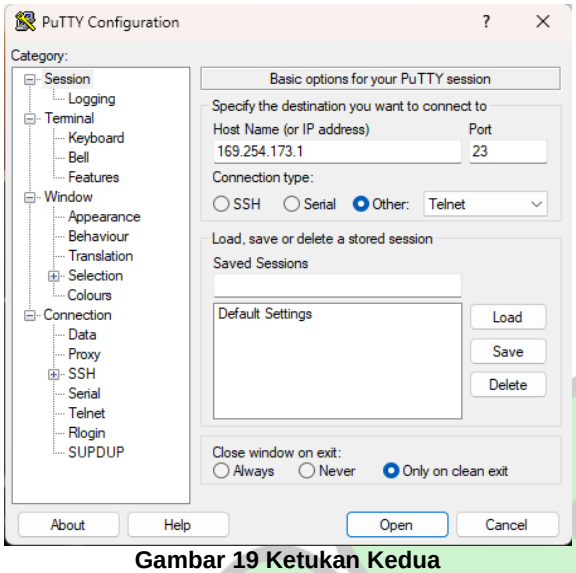
Gambar 17 Ketukan Yang Dilakukan Pada *Command Prompt*

Setelah ketukan pertama dengan melakukan ping terhadap IP 169.254.173.1 pada *Command Prompt*, ketukan selanjutnya dilakukan pada aplikasi PuTTY Configuration dengan mengisi Host Name (or IP address) dengan IP yang digunakan, isi *Port* dengan 22 dan pilih SSH untuk Connection Type, selanjutnya Open.



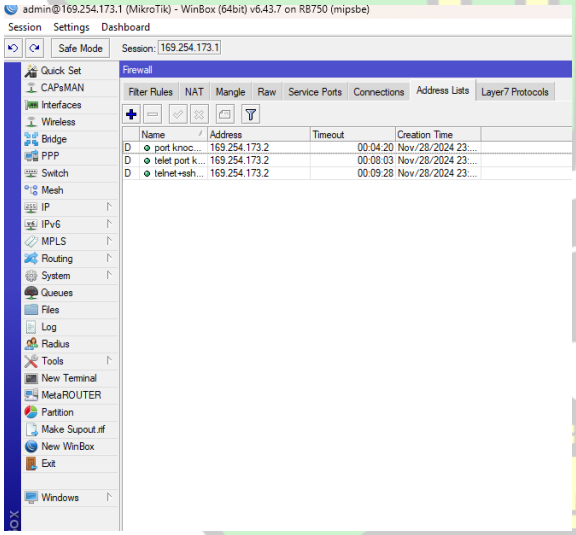
Gambar 18 Ketukan Yang Dilakukan Pada Aplikasi PuTTy Configuration

Sama halnya seperti tahap sebelumnya namun pada ketukan ini isi *Port* dengan 23 dan klik *Other* untuk mengisi *Connection Type,* dan kemudian *Open.*



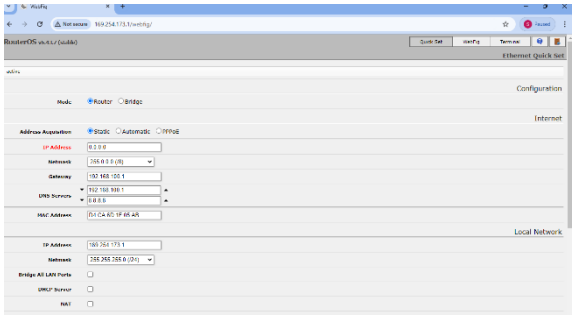
Gambar 19 Ketukan Kedua

Setelah melakukan urutan ketukan dengan benar maka router bisa di akses, dan gambar 20 adalah tampilan ketukan yang berhasil pada router, sehingga bisa melakukan akses.



Gambar 20 Ketukan Berhasil

Apabila urutan ketukan dilakukan dengan benar maka router dan Webfig akan bisa di akses seperti pada gambar 21



Gambar 21 Webfig Berhasil Diakses

KESIMPULAN

Peningkatan keamanan layanan jaringan dengan menggunakan *Port* Knocking melalui penguncian atau pemblokiran port, sehingga yang dapat mengaksesnya dibatasi. Metode *Port Knocking* ini adalah salah satu teknik yang efektif untuk peningkatan keamanan layanan jaringan dari berbagai serangan.

Penggunaan teknik *Port Knocking* hanya bisa dilakukan oleh user yang mengetahui urutan ketukan yang telah dibuat. Hal ini mengartikan bahwa pengguna diharuskan mengetuk terlebih dahulu agar dapat terkoneksi ke *port* setelah melakukan ketukan urutan yang benar.

Dengan cara ini resiko kebocoran data dapat dikurangi, dan membatasi user yang dapat mengakses jaringan hanya user yang memiliki hak akses, serta dapat mengurangi serangan lainnya. Tujuan dari implementasi ini adalah untuk memenuhi peningkatan keamana layanan jaringan yang dibutuhkan.

DAFTAR PUSTAKA

AMAL, MUH ICHLASUL, ELSA SYAFIRA RAHMASITA, EDWARD SURYAPUTRA, AND NUR AINI RAKHMAWATI. 2022. "Analisis Klasifikasi Sentimen Terhadap Isu Kebocoran Data Kartu Identitas Ponsel Di Twitter." *Jurnal Teknik Informatika dan Sistem Informasi* 8(3): 645–60.

AL AMIEN, JANUAR. 2020. "Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking." *Jurnal Fasilkom* 10(2): 159–65.

ARDIANSYAH, RISNITA, AND M. SYAHRAN JAILANI. 2023. "Teknik Pengumpulan Data Dan Instrumen Penelitian Ilmiah Pendidikan Pada Pendekatan Kualitatif Dan Kuantitatif." *Jurnal IHSAN : Jurnal Pendidikan Islam* 1(2): 1–9.

AZIZ, AULIA SYARIF, AND SAFRIATULLAH. 2021. "Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius." *Journal of Informatics and Computer*

Science 7(2): 106–12.

EKA PUTRA, FAUZAN PRASETYO, AMIR HAMZAH, WALID Agel, and R. Okky Firmansyah Kusuma. 2024. "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering Dan Port Knocking." *Jurnal Sistim Informasi dan Teknologi* 5(4): 82–87.

AL FIKRI, KHASHAAISHA, AND DJUNIADI. 2021. "Keamanan Jaringan Menggunakan Switch Port Security." *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan* 5(2): 302–7. http://bit.ly/InfoTekJar.

MUNAWAR, ZEN, M KOM, AND NOVIANTI INDAH PUTRI. 2020. "Keamanan Jaringan Komputer Pada Era Big Data." *Jurnal Sistem Informasi-J-SIKA* 02(01): 14–20.

NURBAHRI, ROBY, AND GUNADI WIDI NURCAHYO. 2023. "Jurnal Sistim Informasi Dan Teknologi Analisis Penggunaan Metode Port Knocking Pada Sistem Keamanan Jaringan Komputer (Studi Kasus Di Universitas Baiturrahmah)." *Sistim Informasi dan Teknologi* 5(1): 102–8.

SANJAYA, TONY, AND DIDIK SETIYADI. 2019. "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim." *Jurnal Mahasiswa Bina Insani* 4(1): 1–10.

OKTAVIANSYAH, PARADIKA DWI. 2022. "Penerapan Sistem Pengamanan Port Pada Mikrotik Menggunakan Metode Port Knocking." *NetPLG Journal of Network and Computer Applications* 1(2): 13–24