

IMPLEMENTASI SISTEM KEAMANAN JARINGAN KOMPUTER DENGAN MENGGUNAKAN METODE *PORT KNOCKING* PADA INDO METRO

Depitasari¹, Arif Hidayat², Danang Prabowo³

¹²³Program Studi Ilmu Komputer, Fakultas Ilmu Komputer,
Universitas Muhammadiyah Metro

¹²³ Jl. Gatot Subroto, Yosodadi, Kec. Batanghari, Kota Metro, Lampung 34381, Indonesia

¹ depita419@gmail.com, ² androidarifhidayat@gmail.com, ³ danang32@gmail.com

Abstrak : Internet menjadi kebutuhan yang utama sehingga hampir semua aktifitas dilakukan dengan jaringan internet. Seiring perkembangan dunia teknologi di berbagai aspek dan bidang kehidupan, salah satunya pada bidang jaringan komputer (networking) . Tujuan penelitian ini adalah untuk mengimplementasikan sistem keamanan jaringan komputer dengan metode Port Knocking. Penelitian ini akan menggunakan metode pengembangan (research and development) dengan menggunakan pendekatan pengembangan model 4D (four-D model) yang dikemukakan oleh Sivasailam Thiagarajan dkk (1974) . Adapun tahapan model pengembangan meliputi tahap Define (pendefinisian), tahap Design (perancangan), tahap Development (pengembangan), dan tahap Disseminate (ujicoba). Berdasarkan hasil analisis sebuah keamanan jaringan menggunakan metode port knocking mampu menjaga router agar tidak mudah di serang penyusup atau hacker. Berdasarkan analisis yang dilakukan maka sebuah sistem keamanan jaringan menggunakan metode port knocking ini di gunakan pada INDO METRO .

Kata Kunci: Sistem Keamanan, Jaringan Komputer, Port Knocking

Abstract: *The internet has become a primary need so that almost all activities are carried out with an internet network. Along with the development of the world of technology in various aspects and fields of life, one of which is in the field of computer networks (networking). The purpose of this study is to implement a computer network security system with the Port Knocking method. This study will use a development method (research and development) using the 4D model development approach (four-D model) proposed by Sivasailam Thiagarajan et al (1974). The stages of the development model include the Define stage, the Design stage, the Development stage, and the Disseminate stage (trial). Based on the results of the analysis, a network security using the port knocking method is able to keep the router from being easily attacked by intruders or hackers. Based on the analysis carried out, a network security system using the port knocking method is used at INDO METRO.*

Keywords: *Safety System, Computer Network, Port Knocking*

PENDAHULUAN

Keamanan jaringan adalah proses mencegah dan mengidentifikasi pengguna yang tidak sah yang disebut “penyusup” untuk mengakses bagian mana pun dari sistem jaringan komputer. Banyaknya perusahaan, kantor dan institusi yang menggunakan internet untuk mengakses berbagai jenis informasi yang mereka butuhkan, seperti INDO METRO.

INDO METRO merupakan salah satu pusat perbelanjaan modern pada Kota Metro yang menyediakan produk-produk bahan bangunan yang lengkap guna memenuhi kebutuhan konsumen. Sebagai salah satu pusat perbelanjaan modern, tentu INDO METRO memiliki jaringan internet untuk menunjang manajemen komunikasi, dan pelayanan kepada konsumen. Pada hasil pengamatan yang dilakukan, didapat

informasi bahwa kecepatan jaringan internet yang ada di INDO METRO adalah 30 Mbps, dengan rincian 10 Mbps untuk pengguna user dan 20 Mbps untuk gudang keramik. Selain itu, didapat informasi juga bahwa *user* yang aktif pada INDO METRO berjumlah 25 *user*. INDO METRO memiliki total 10 unit PC dengan rincian 7 PC digunakan pada gudang, dan 3 PC digunakan pada kasir.

Dari hasil pengamatan yang dilakukan, terdapat masalah bahwa transaksi jaringan komputer pada INDO METRO dikatakan tergolong tinggi karena banyaknya *user* yang mengakses contohnya seperti kasir, staf, tim akutansi, dan marketing yang diakses secara bersamaan sehingga mengakibatkan koneksi yang tidak memadai atau lambat. Selain itu, ada masalah yang menjadi kendala saat ini, yaitu bahwa sistem jaringan komputer sudah aktif, tetapi router mikrotik belum dilengkapi dengan sistem keamanan yang sesuai dan handal. Sehingga bisa mengakibatkan kebocoran data atau pihak yang tidak berwenang. Berdasarkan analisis sistem jaringan komputer yang sudah berjalan bahwa kebutuhan pengguna belum terpenuhi secara memadai karena kurangnya keamanan pada sistem jaringan komputer sehingga mengakibatkan penyusup bisa masuk dan merubah settingan pada router mikrotik dan menyebabkan permasalahan yang cukup fatal maka dari itu perlu dibuatkan sistem keamanan jaringan komputer yaitu Port Knocking.

Solusi untuk mengatasi agar “penyusup” tidak bisa masuk ke *device router MikroTik* yaitu mengimplementasikan metode keamanan jaringan yaitu menggunakan metode *Port Knocking*. *Port Knocking* merupakan suatu metode untuk keamanan jaringan dengan memanfaatkan sistem *firewall* dengan menggunakan sistem kerja

seperti membuka atau menutup akses *port* tertentu pada perangkat jaringan. Manfaat dari metode *Port Knocking* yaitu memberikan autentikasi bagi pengguna sebelum dapat mengakses ke suatu *server* pada perangkat jaringan. Metode ini juga dapat dijalankan pada protokol TCP, dan ICMP.

KAJIAN PUSTAKA DAN LANDASAN TEORI

Jaringan Komputer

Menurut Putri dan Solikin (2016:7) menyimpulkan bahwasannya:

Jaringan komputer merupakan himpunan interkoneksi sejumlah komputer *autonomous*. Dijelaskan bahwa jaringan komputer merupakan kumpulan beberapa komputer yang saling terhubung dengan komputer yang lain melalui media perantara seperti media kabel ataupun media tanpa kabel (*nirkabel*).

Peer to Peer

Menurut Agustina dan Suprianto (2019: 4) mengambil kesimpulan bahwa:

Sistem operasi jaringan model *peer to peer* memungkinkan seorang *user* membagi sumber dayanya yang ada dikomputernya, baik itu file data, *printer*, dll dan mengakses sumber data pada komputer lain. Model ini tidak mempunyai sebuah file *server* atau sumber daya yang terpusat, seluruh *komputer* mempunyai kemampuan yang sama untuk memakai sumber daya yang tersedia dijaringan.

Client-Server

Menurut Haryanto (2015: 20) mengambil kesimpulan:

Sistem operasi jaringan *Client Server* memungkinkan jaringan untuk mensentralisasi fungsi dan aplikasi kepada satu atau dua *dedicated file server*. Sebuah file *server* menjadi jantung dari keseluruhan system memungkinkan untuk

mengakses sumber daya, dan menyediakan keamanan.

TCP/IP

Menurut Syafrizal yang dikutip Widodo (2017: 2) mengambil kesimpulan bahwa: *Transmission Control Protocol/Internet Protocol* (TCP/IP) adalah sekumpulan protokol yang terdapat di dalam jaringan komputer yang digunakan untuk berkomunikasi atau bertukar data antar komputer. TCP/IP merupakan protokol standar pada jaringan internet yang menghubungkan banyak komputer yang berbeda jenis mesin maupun sistem operasi agar dapat berinteraksi satu sama lain TCP/IP secara umum berfungsi untuk memilih rute terbaik transmisi data, memilih rute alternative jika suatu rute tidak dapat digunakan, mengatur dan mengirimkan paket-paket pengiriman data dan lain-lain. TCP/IP merupakan protokol yang memungkinkan sistem diseluruh dunia berkomunikasi pada jaringan tunggal yang disebut Internet.

Port Knocking

Menurut Kusuma (2016: 8) menarik kesimpulan bahwasannya: Port Knocking merupakan suatu sistem keamanan yang bertujuan untuk membuka atau menutup akses block ke port tertentu dengan menggunakan Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, dan ICMP. Sehingga untuk masuk dan menggunakan akses ke port tertentu yang telah dibatasi, maka user harus mengetuk terlebih dahulu dengan memasukkan Rule yang harus dilakukan terlebih dahulu. Rule yang dimana hanya diketahui oleh pihak administrator jaringan. Sebuah sistem harus memiliki keseimbangan antara keamanan dan fleksibilitas. Salah satu cara

untuk mencapai sistem seperti demikian yaitu dengan menggunakan akses firewall.

Keamanan Jaringan

Menurut Anugrah dan Rahmanto (2017: 91) menyimpulkan bahwasannya: “keamanan jaringan untuk dapat memperkuat sistem keamanan jaringan pada *server* dari serangan seperti *Port Scanning* dan *Denial of Service (DoS)*”.

MikroTik

Menurut Bahtiar dalam Fahtoni, dkk (2022) menyatakan bahwa:

MikroTik sendiri merupakan nama perusahaan kecil yang berkantor di pusat negara *Latvia*, dan dibentuk oleh *John Trully* serta *Arnis Riekstins*. Sekitar tahun 1966, mereka berdua memulai dengan sistem operasi Linux dan MS DOS dan dikombinasikan dengan teknologi berbasis *wireless (nirkabel)* LAN atau WLAN *Aeronet* yang berkecepatan hingga 2 Mbps di *Moldova*. Kemudian melayani sekitar lima pelanggan baru di *Latvia*. Seiring berjalannya waktu, prinsip dasar dari MikroTik bukan membuat *wireless ISP (Internet Service Provider)* lagi. Akan tetapi, dapat membuat program *router* yang andal dan dapat dijalankan diseluruh negara.

Menurut Hasrul (2020:15) menarik kesimpulan bahwa:

Mikrotik adalah sistem operasi komputer dan software komputer untuk menjadikan komputer biasa menjadi sebuah router. Mikrotik dibedakan menjadi mikrotik operation system (OS) dan mikrotik board yang tidak memerlukan komputer, cukup dengan board yang include dengan mikrotik OS.

LAN Card

Menurut Kustanto (2015:33) dapat disimpulkan bahwa:

LAN Card atau Network Interface Card (NIC) adalah perangkat yang berfungsi menghubungkan komputer yang satu dengan komputer yang lain dalam sebuah jaringan. LAN Card atau NIC ini memiliki nomor alamat yang disebut MAC Address.

Flowchart

Menurut Subianto (2014: 55) menarik kesimpulan sebagai berikut:

Diagram Arus Data adalah suatu network yang menggambarkan suatu sistem automat atau komputerisasi, manualisasi atau gabungan dari keduanya, yang penggambarannya disusun dalam bentuk kumpulan komponen sistem yang saling berhubungan sesuai dengan aturan mainnya.

METODE

Penelitian ini menggunakan metodologi pengembangan (*Research and Development*) dengan menggunakan pendekatan pengembangan model 4D (*four-D*) yang dikemukakan oleh Sivasailam Thiagarajan dan Semmel tahun 1974. Adapun tahapan model pengembangan meliputi: Tahap *Devine* (pendefinisian), tahap *Design* (perancangan), tahap *Development* (pengembangan), dan tahap *Disseminate* (penyebarluasan).

a. Observasi

Menurut Arikunto yang dikutip Putri dan Setyadi (2019 : 7) Observasi adalah: kegiatan yang meliputi kegiatan pemusatan perhatian terhadap suatu objek dengan menggunakan seluruh indera. Tujuan dari observasi ini adalah peneliti jadi mempunyai kesempatan untuk lebih mengenal dan mengamati calon informan di tempat penelitian. Dengan melakukan observasi maka diharapkan akan memperoleh data-data atau informasi yang sesuai dengan penelitian. Pada penelitian

ini penulis menggunakan teknik observasi tidak berperan serta (*non-participant observation*).

b. Wawancara (Interview)

Peneliti mendapat informasi langsung dengan teknik wawancara dari kepala IT. Pengumpulan data dengan cara bertanya dan menjawab pertanyaan langsung kepada pihak yang berwenang yang bersangkutan dengan subjek penelitian. Dari hasil wawancara, penulis mendapatkan data gambaran umum dan sejarah perkembangannya pengumpulan data dengan cara bertanya dan menjawab pertanyaan langsung kepada pihak yang berwenang yang bersangkutan dengan subjek penelitian.

c. Dokumentasi (Dokumentation)

Menurut Sugiyono yang dikutip Nurani, dkk. (2020: 54) Dokumentasi adalah : Suatu cara yang digunakan untuk memperoleh data dan informasi dalam bentuk buku, arsip, dokumen, tulisan angka dan gambar yang berupa laporan serta keterangan yang dapat mendukung penelitian. Dokumentasi digunakan untuk mengumpulkan data. Dengan teknik dokumentasi ini, penulis mengumpulkan dan menganalisa data-data penting tentang INDO METRO.

d. Studi Pustaka

Menurut Nazir yang dikutip Nakila (2019:158), Studi Pustaka adalah: Langkah yang penting dimana setelah seorang peneliti menetapkan topik penelitian, langkah selanjutnya adalah melakukan kajian yang berkaitan dengan teori yang berkaitan dengan topik penelitian. Dalam pencarian teori, peneliti akan mengumpulkan informasi sebanyak-banyaknya dari kepustakaan yang berhubungan. Sumber-sumber kepustakaan dapat diperoleh dari buku,

jurnal, majalah, hasil-hasil penelitian (tesis dan disertasi), dan sumber-sumber lainnya yang sesuai (internet, koran dll).

HASIL DAN PEMBAHASAN

Berikut merupakan hasil dari perancangan *captive portal* dengan menggunakan metode pengembangan NDLC (Network Development Life Cycle) yang memiliki tahapan Analisis, Perancangan, Simulasi, Implementasi, Monitoring, dan Management.

Analisis (*Analysis*)

Tahapan-tahapan metode pengembangan *Network Development Life Cycle (NDLC)* ini dimulai pada tahapan analisis, dimana pada tahap ini membahas proses analisis kebutuhan sistem, kebutuhan perancangan dan penerapan upaya optimalisasi *bandwidth*.

a. Kebutuhan Hardware

Kebutuhan *hardware* (perangkat keras), yang penulis mengajukan untuk digunakan dalam menerapkan keamanan jaringan menggunakan metode pemblokiran *port* dan *port knocking*. Kebutuhan hardware dapat dilihat melalui tabel 1 dibawah ini.

Tabel 1. Kebutuhan Hardware

No.	Perangkat	Kegunaan
1	Laptop / PC	Gunakan untuk konfigurasi dan menjalankan program yang akan di aplikasikan ke sistem monitoring suhu, sekaligus dapat digunakan untuk monitoring secara langsung.
2	Konektore Rj45	Dalam jaringan, di mana anda menghubungkan komputer atau elemen jaringan lainnya satu sama lain.
3	Kabel UTP	UTP adalah kabel yang disediakan untuk transmisi data, terdiri dari empat pasang kabel (biru, oranye, hijau dan coklat) yang dipilih menurut aturan tertentu dan digunakan untuk mengirim dan menerima data.
4	HUB / Switch	Sebagai titik koneksi umum untuk perangkat di jaringan anda. Switch jaringan adalah perangkat jaringan komputer yang menghubungkan berbagai perangkat di jaringan komputer.
5	Tang kriting	Salah satu jenis alat pemotong khusus untuk kabel jaringan.
6	Kabel Tester/LAN Tester RJ45 RJ11	Alat untuk memeriksa koneksi kabel LAN untuk RJ 45 dan RJ 11. Dilengkapi dengan lampu indikator, tombol pengatur kecepatan, baterai dan saku kecil.
7	Mikrotik Rb941-2nD- Tc	Menghubungkan beberapa jaringan area lokal ke Internet. Selain itu, <i>router proxy</i> memainkan peran penting dalam

b. Kebutuhan Software

Kebutuhan *software* atau perangkat lunak yang penulis ajukan berguna untuk menjalankan metode *port knocking* yang digunakan dalam implementasi keamanan jaringan komputer dan sebuah *software* untuk hasil dari kerja sistem yang dibuat. Kebutuhan *software* dapat dilihat melalui tabel 2 dibawah ini.

Tabel 2. Kebutuhan Software

No	Software	Kegunaan
1	Sistem operasi windows 7,8 & 10	Sebagai sistem operasi yang digunakan untuk menjalankan program dari sistem yang akan dibuat.
2	Google Chrome	Sebuah aplikasi <i>browser</i> yang juga digunakan untuk menjelajah dunia maya.
3	Winbox	Utilitas untuk menghubungkan dan mengkonfigurasi MikroTik menggunakan alamat MAC atau protokol IP.
4	Putty	Untuk akses jarak jauh seperti login, Telnet. Aplikasi ini juga memungkinkan untuk mengontrol sistem dari jarak jauh atau di lokasi lain.

c. Kebutuhan Brainware

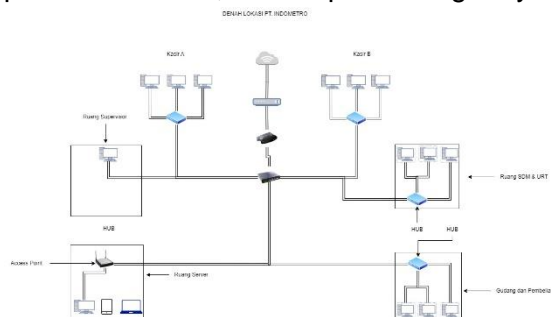
Brainware dibutuhkan untuk mengimplementasikan keamanan jaringan komputer dengan metode pemblokiran *port* dan *port knocking* yang dimiliki. Dan kebutuhan ini nantinya akan berguna ketika sudah diakses oleh server. Kebutuhan *brainware* dapat dilihat melalui tabel 3 dibawah ini.

Tabel 3. Kebutuhan Brainware

Brainware	Kegunaan
Pemilik atau pengguna komputer	Orang menggunakan, menjalankan, memanfaatkan, dan mengoperasikan perangkat komputer.

Perancangan

Desain atau perancangan adalah tahapan perancangan topologi jaringan yang sudah dipersiapkan penulis untuk digunakan pada indo metro, berikut perancangannya.



Gambar 1 Topologi Tree Indo Metro

Development (Pengembangan)

a. Instalasi WinBox

Melakukan instalasi winbox terlebih dahulu, Winbox adalah perangkat lunak untuk me-remote mikrotik dalam GUI (*Graphic User Interface*) sehingga user dengan mudah dapat mengakses dan mengkonfigurasi *router* sesuai kebutuhan dengan mudah, efektif, dan efisien selain itu instalasi dapat dilakukan pada standard PC (*Personal Computer*).

- b. Konfigurasi Port Ethernet Router
 - Ether 1 ISP/ Internet -> Ether 1-internet / atau bersumber hospot
 - Ether 2 Server -> Ether 2-server yang akan dipergunakan pada ruangan server
 - Ether 3 *Client* -> Ether 3-client yang akan dipergunakan pada staff

c. Penjelasan IP Address

ISP yang digunakan adalah indihome dengan otomatis IP Address yang diterima. *Address* ini digunakan untuk memberikan *IP Address* yang akan menjadi default gateway router mikrotik

d. Membuat Konfigurasi Jaringan

Setelah semua alat yang dibutuhkan sudah tersedia, langkah selanjutnya adalah membuat konfigurasi pada *router* mikrotik. Konfigurasi yang dibuat yaitu setting bersumber dari Hospot yang akan digunakan sebagai sumber jaringan internet.

Disseminate (Penyebarluasan)

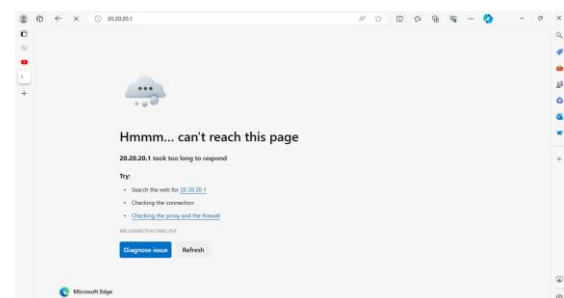
a. Validation testing

1). Uji Coba Konfigurasi *Port Knocking*

Setelah konfigurasi *port knocking* selesai dibuat langkah selanjutnya adalah melakukan uji coba terhadap konfigurasi *port knocking* yang sudah dibuat. Uji coba dilakukan pada client yang terhubung melalui jaringan wifi. Berikut adalah hasil uji coba yang dilakukan:

a). Blocking Akses

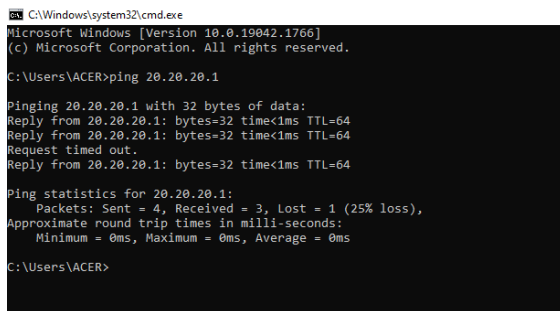
Uji coba ini dilakukan sebelum *client* memenuhi *Rule knocking* yang dibuat. Apabila client tidak dapat mengakses router mikrotik maka dapat dikatakan konfigurasi ini berjalan dengan baik. Uji coba dilakukan dengan mengakses mikrotik menggunakan Winbox dan melalui webfig. Hasilnya seperti pada Gambar 2.



Gambar 2. Tes Ping Gagal Sebelum Melakukan *Knocking*

b). Melakukan Pengetukan atau *Knocking* Uji Coba

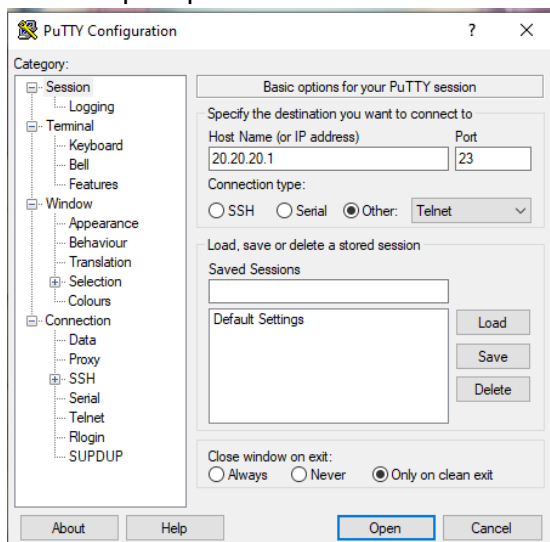
Selanjutnya adalah melakukan *Knocking* melalui *client* yang terhubung melalui jaringan wifi. Tujuan dari uji coba ini adalah untuk membuka *port* yang tertutup agar *client* dapat mengakses mikrotik. *Knocking* yang dilakukan harus sesuai dengan *Rule* yang sudah dibuat yaitu dengan cara mengirimkan paket ICMP atau PING dan melakukan Telnet terhadap *Default Gateway* yang terdaftar pada mikrotik. Berikut *knocking* pertama pada *client* dapat dilihat pada Gambar 3.



Gambar 3. *Knocking* Pertama Pada Melalui PING (Paket ICMP)

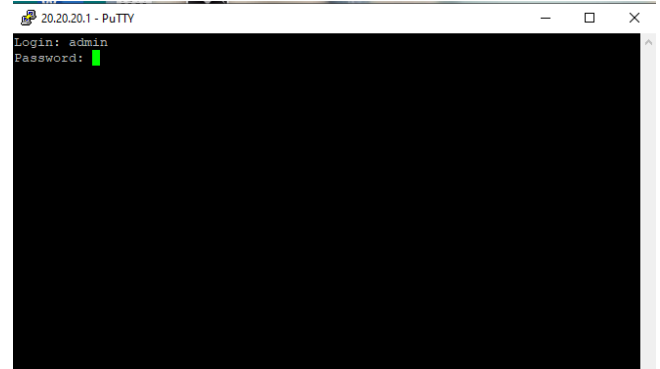
1. Melakukan PING Telnet

Selanjutnya adalah melakukan *Rule* terakhir sebelum semua bisa membuka *knocking* tersebut. Yaitu melakukan Telnet terhadap *Default Gateway* yang terdaftar pada mikrotik melalui aplikasi *Putty*. Dapat dilihat seperti pada Gambar 4.



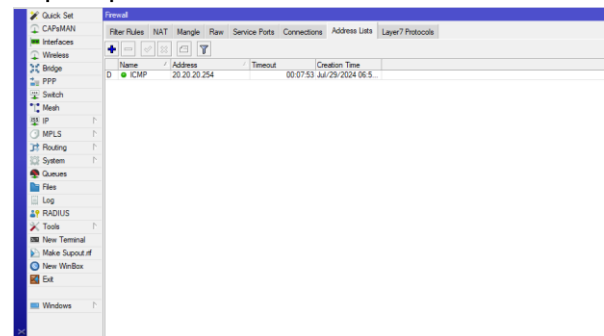
Gambar 4. Melakukan PING Telnet sebagai *Rule* terakhir untuk membuka *knocking*

Setelah masuk pada login masukan “Admin” dan password kosong (-) dapat dilihat seperti pada Gambar 59.



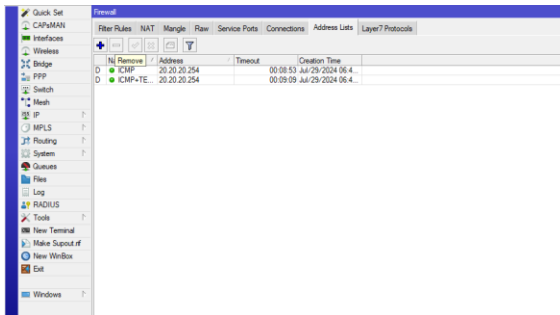
Gambar 4. Konfigurasi Telnet Telah Berhasil

RePort knocking pertama, otomatis akan terdeteksi sebagai *clinet* yang “ICMP”, harus melewati Telnet untuk bisa masuk sebagai “ICMP+TELNET” dapat dilihat seperti pada Gambar 5.



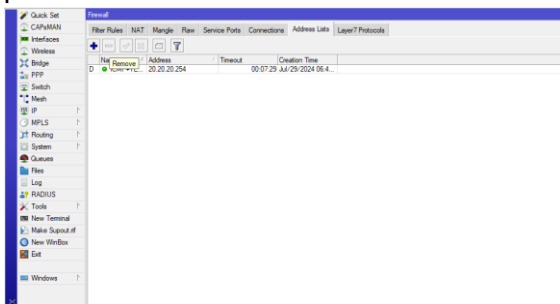
Gambar 5. *RePort Knocking* Pertama Sudah Terdeteksi Sebagai “ICMP”

Rule knocking kedua adalah dengan melakukan Telnet terhadap *Default Gateway* Mikrotik. Apabila *client* berhasil memenuhi *Rule knocking* kedua akan ditandai dengan *Address List* Name ICMP+TELNET. Konfigurasi dapat dikatakan berhasil apabila *client* yang terdaftar dalam *Address List* dengan nama ICMP+TELNET dapat mengakses mikrotik. Setelah melewati *timeout* yang dibuat pada *Rule knocking* pertama maka *Address List* dengan nama ICMP akan otomatis dihapus.



Gambar 6. Knocking Kedua Terdeteksi Sebagai “ICMP+TELNET” Artinya Sudah Diizinkan Mengakses atau Meremot Router.

Berikut adalah menghapus *Address List knocking* pertama secara Otomatis. Seperti pada Gambar 7.



Gambar 7. Menghapus Address List Knocking Pertama Secara Otomatis

KESIMPULAN

Indo Metro merupakan tempat penelitian skripsi yang dilakukan oleh penulis saat ini sudah memiliki jaringan internet yang sudah berjalan, yaitu menggunakan jaringan topologi tree, akan tetapi jaringan internet tersebut masih mempunyai permasalahan yaitu: Tidak adanya sebuah keamanan jaringan internet yang digunakan terhadap router mikrotik, sehingga dapat dihack oleh penyusup dengan mudah karena *port-port* yang ada bisa di akses dengan bebas tanpa ada konfigurasi atau keamanan, maka dari itu keamanan *router* mikrotik jaringan komputer sangatlah penting untuk menjaga kerahasiaan data dan informasi yang terdapat pada server. Sehingga dari kendala sistem jaringan yang ada, perlu dibuatkannya suatu sistem

keamanan, yang disebut Port Knocking, yang menggunakan dua tahapan yaitu ICMP dan Telnet. Dimana pengguna terpercaya memanipulasi aturan firewall dengan mengirimkan informasi di seluruh port yang tertutup, sehingga setelah user atau pengguna mengetuk Rule yang ditentukan baru akan bisa mengakses, jika bisa membuka port yang telah ditentukan baru bisa mengakses router mikrotik. Penelitian ini menghasilkan sebuah sistem keamanan jaringan yang mengamankan sebuah router mikrotik dengan menggunakan metode *Port Knocking*, yang berfungsi menjadi salah satu alternatif untuk menjaga keamanan dalam suatu jaringan komputer, mencegah penyerang untuk mengakses *Router* Mikrotik, dan bagi para Administrator mereka dapat menentukan siapa-siapa saja yang memiliki hak akses untuk memasuki *port-port* tertentu.

Jaringan yang dibangun ini berhasil untuk melindungi *Router* terhadap akses ilegal yang dilakukan client. Client yang ingin mengakses *router* harus melakukan ketukan atau *knocking* sesuai urutan yang dibuat. hanya seorang administrator yang dapat mengakses Router. Dengan mendaftarkan *IP Address* pada *Address Lists* yang diberi nama Telnet).

REFERENSI

- [1] Agustina, R., dan Suprianto, D. 2019. Pelatihan Jaringan Untuk Guru Dan Siswa SMK Al Kaaffah Kapanjen Kabupaten Malang. *Jurnal Aplikasi Dan Inovasi Ipteks "Soliditas"(J-Solid)*, 2(1), h. 1-9.
- [2] Anugrah, I., dan Rahmanto, R. H. 2017. Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. *PIKSEL: Jurnal Penelitian Ilmu Komputer Sistem Embedded and Logic*, 5(2), h. 91-106.
- [3] Fahtoni, W. F., Hidayat, A., & Mustika. 2022. Implementasi Sistem Keamanan

- Jaringan Komputer Dengan Metode Port Knocking Pada LKP Surya Komputer. *Jurnal Mahasiswa Ilmu Komputer*, 3 (1).
- [4] Hasrul, Muh. 2020. "Aspek Hukum Pemberlakuan Pembatasan Sosial Berskala Besar (Psbb) Dalam Rangka Penanganan Corona Virus Disease 2019 (Covid-19)". *Legislatif* 3 (2):385-98.
- [5] Haryanto Victor. 2015. Sistem Jaringan komputer Untuk Pemula. Yogyakarta dengan MADCOMS. Hal: 13-21
- [6] Kusuma, G. H. A. 2021. Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing (JIAC)*, 2(2), h. 1-4.
- [7] Kustanto, & Daniel T. Saputro. 2015. *Belajar jaringan Komputer berbasis MikroTik OS*. Gava Media. Yogyakarta
- [8] Putri, A. dan Solikin. 2016. Analisa Kinerja Koneksi Jaringan Komputer Pada SMK Teknologi Bistek Palembang, (online),
- [9] Sugiyono. (2020). Metode Penelitian Kualitatif. Bandung: Alfabeta.
- [10] Widodo, A. 2017. Implementasi Monitoring Jaringan Komputer Menggunakan Dude. *Jurnal Teknologi Informasi*, 11(1), h. 1-10.