Penerapan Metode *Port Knocking* dan *Access Client List* (ACL) untuk Keamanan Jaringan pada Mikrotik

Anselmus Odorikus Pala[1], Ronald David Marcus[2]
[1,2]Fakultas Teknologi Informasi, Universitas Merdeka Malang. 082142934241
e-mail: anselmusodorikuspala14@gmail.com[1], ronald.mangero@unmer.ac.id[2]

Kata Kunci:

Keamanan Jaringan
Port Knocking Access Client List
Mikrotik

ABSTRAK

Keamanan jaringan Mikrotik sangat penting mengingat semakin meningkatnya serangan dari perangkat yang tidak diizinkan (penyusup) yang berdampak pada keamanan jaringan. Salah satu cara untuk meningkatkan keamanan jaringan Mikrotik adalah dengan menerapkan metode *port knocking* dan *Access Client List. Port knocking* adalah teknik yang digunakan untuk mengakses *por*t yang telah diblokir dengan mengirimkan paket atau koneksi sesuai dengan aturan *knocking* yang telah dibuat. Metode ini membantu memastikan bahwa hanya pengguna yang sah yang dapat membuka akses ke *port* tertentu. Sementara itu, *Access Client List* digunakan untuk mengatur hak akses tiap perangkat yang terhubung ke jaringan. Dengan *Access Client List*, administrator dapat menyaring lalu lintas data dan mengontrol apakah suatu paket data dilewatkan atau dihentikan berdasarkan aturan yang ditetapkan. Kedua metode ini bekerja sama untuk menciptakan lapisan tambahan perlindungan yang memperkuat keamanan jaringan Mikrotik dari potensi ancaman.

Keyword:

Network Security
Port Knocking Access Client List
Microtic

ABSTRACT

Microtic network security is crucial given the growing number of attacks from unauthorized devices (intruders) that affect network security. One way to improve the security of Microtik networks is by implementing port knocking and access client list methods. Port knocking is a technique used to access a port that has been blocked by sending a package or connection according to the knocking rules that have been created. This method helps ensure that only authorized users can open access to a particular port. Meanwhile, Access Client List is used to set access rights for each device connected to the network. With Access Client Lists, an administrator can filter data traffic and control whether a data package is missed or terminated according to a set rule. These two methods work together to create an additional layer of protection that strengthens the security of the microtic network from potential threats.

ISSN: 2598-0076

I. PENDAHULUAN

Saat ini internet semakin pesat tidak hanya berpengaruh pada kemudahan berbagi informasi tetapi juga telah menjadi bagian yang berpengaruh dalam proses transaksi maupun transportasi digital menjadi penting , sampai pada titik di mana hampir semua aktivitas dilakukan melalui koneksi daring yang canggih untuk mencakup banyak aspek kehidupan sehari- hari tidak terbatas pada jaringan komputer. Semakin berkembang pesatnya jaringan (internet) juga memiliki dampak negatif yaitu sering terjadinya kejahatan dalam dunia internet yang biasanya terjadi dengan berbagai metode seperti mencuri data dan bahkan mentransfer data secara ilegal, hal tersebut merupakan akibat dari kecanggihan internet itu sendiri.

Keamanan jaringan suatu proses mencegah, mengamankan dan mengidentifikasi pengguna yang tidak sah (penyusup) untuk melakukan pengaksesan pada setiap bagian dari sistem jaringan komputer. Internet yang aman harus memiliki sistem pertahan yang baik agar tidak mudah di bobol atau diretas oleh para penyusup. Ada beberapa hal yang bisa dipertimbangakn dalam mengamankan sebuah jaringan salah satunya adalah dengan menerapkan metode port knocking dan Access Client List (ACL)..

Menurut Putu (2018) menyatakan bahwa secara definisinya, Port Knocking adalah sebuah teknik untuk membuat komunikasi dari mana saja, dengan cara tidak membuka port komunikasi secara bebas diakses [1]. Menurut Amarudin (2018) Port Knocking adalah konsep menyembunyikan layanan jarak jauh didalam sebuah firewall yang memungkinkan akses ke port tersebut hanya untuk mengetahui service setelah client berhasil diautentikasi ke firewall [2].

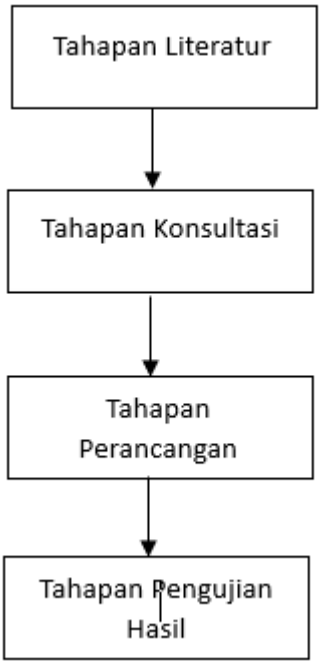
Menurut Pamuji (2020) Mikrotik adalah sebuah sistem operasi yang dapat diandalkan dengan berbagai fitur lengakap mengenai jaringan serta memiliki firewall dengan metode packet filtering yang mengatur semua paket baik yang melewati ataupun dituju ataupun yang diterima kemudian dilanjutkan atau ditolak. Selain firewall ini memiliki peran sebagai penghubung antar dua atau lebih jaringan untuk meneruskan dari satu jaringan ke jaringan yang lainnya [3]. Menurut wahana (2010) Mikrotik merupakan sistem operasi router yang dirilis dengan nama Mikrotik routerOS dan mampu diinstal pada komputer tanpa memerlukan perangkat keras tambahan , tidak seperti sistem operasi router lain yang hanya dapat diinstal pada perangkat keras tertentu [2].

ACL adalah teknik yang digunakan untuk dengan peralatan mikrotik. Paket data diambil dan ditransfer menggunakan teknik Access Client List (ACL) dari alamat sumber (resource) ke alamat tujuan (destination). Metode Access Client List akan menerima paket yang berisi data permission dan melarang paket yang berisi data deny untuk sampai ke alamat tujuan [4]**.** ACL yang paling dasar adalah ACL standar. Router target menerima aplikasi

ISSN: 2598-0076

ACL ini, berdasarkan secara eksekutif pada alamat sumber, mengizinkan atau menolak paket. Alamat yang dikenali dapat berupa alamat host atau alamat jaringan (Network Address). Standar ACL dapat diimplementasikan melalui proses TCP/ UDP atau penomoran port namun , standar ACL hanya dapat digunakan untuk menetapkan atau mengizinkan [5]. Suatu bentuk ACL yang disebut Extended ACL mempunyai tingkatan keamanan yang lebih dari pada Standard ACL. Mikrotik dari sumber menerima aplikasi ACL tergantung pada alamat sumber dan tujuan, dan dapat mengizinkan atau melarang paket. Selanjutnya juga Extended ACL memberikan kebebasan kepada administrator jaringan untuk menjalankan prosedur penyaringan dengan tujuan yang lebih berfokus [5].

II. METODE



Gambar 1. Tahapan Metode Penelitian

Tahapan Literature

Menerapkan metode pengumpulan data atau pengumpulan informasi dari berbagai jurnal, buku, website, dan sumber lain yang berhubungan dengan penelitian ini yaitu implementasi Keamanan Jaringan Menggunakan Metode Port Knocking dan Access Client List (ACL).

Tahapan Konsultasi

Melakukan wawancara terhadap dosen pembimbing atau dosen yang berkaitan dengan skripsi tujuannya untuk meminimalisir kesalahan dalam laporan penelitian ini.

Tahapan Perancangan

Mengimplementasikan dilapangan menggunakan alat yang dibutuhkan dalam penelitian.

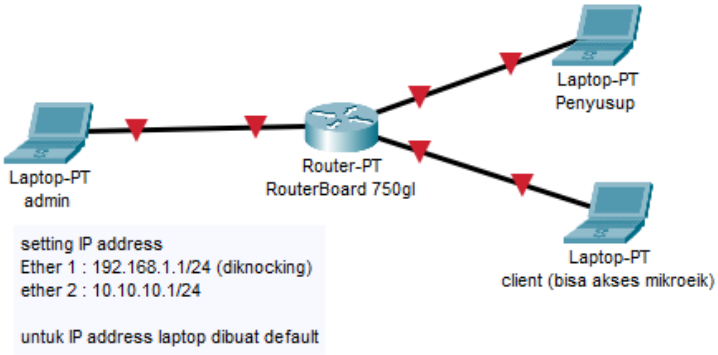
ISSN: 2598-0076

Tahapan pengujian dan Hasil

Pada tahap ini melakukan pengujian dari perancangan yang telah dilakukan untuk mengetahui hasil yang selanjutnya akan diambil kesimpulan dari perancangan tersebut.

Perancangan Jaringan dan implementasi

Port Knocking



Gambar 2. Perancangan Jaringan Port Knocking

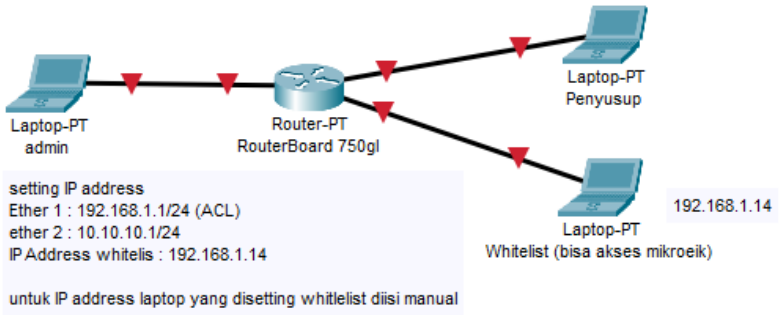
Dalam mengimplemantasikan metode port knocking ini, admin akan memberikan kata kunci dimana kata kunci ini yang akan memberikan keamanan pada mikrotik dari serangan hacker atau penyusup. Kata kunci yang diseting pada mikrotik tidak boleh di ketahui oleh siapapun dengan alasan mengamankan jaringan.

Selain itu, pemberian kata kunci ini didasarkan pada port. kata kunci atau port ini tidak ada dalam mikrotik namun dalam pengaturannya diasumsikan ada karena digunakan untuk mengamankan jaringan itu sendiri. Port yang dimaksud adalah komponen angka yang di rasa unik dan susah untuk tebak oleh para penyusup, contoh kombinasi angka port 1111, port 2222 dan seterusnya. Dalam keamanan jaringan yang diterapkan pada skripsi ini mengunakan kombinasi port 3333, dimana port ini tidak ada dalam mikrotik. Namun port inilah yang akan mengamankan jaringan tersebut sehingga port 3333 tidak boleh di ketahui oleh siapapun. Apabila port – port unik keamanan yang dimaksud diketahui, maka siapapun dapat masuk kedalam tampilan mikrotik dan dapat meremote mikrotik.

Pengaturan – pengaturan keamanan ini hanya dilakukan pada ether 1. Alasannya cukup sederhana karena ether 1 merupakan sumber internet yang bila tidak diamankan maka akan berbahya untuk jaringan itu sendiri ataupun berbahaya untuk kerahasian data – data dari client yang terhubung pada jaringan tersebut. Pada penerapan keamanan pada skripsi ini tidak menggunakan intenet. Namun apabila menggunakan internet pengaturannya tetap sama ketika tidak/tanpa menggunakan internet.

ISSN: 2598-0076

Access Client List



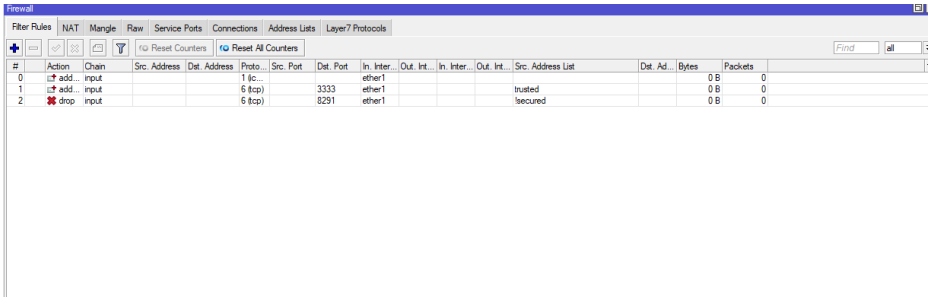
Gambar 3. Perancangan Jaringan ACL

Berbeda dengan pengaturan keamanan port knocking, pengaturan ACL lebih mudah. Dimana pengatuarannya hanya membuat group IP, dimana Ip yang dibuat difungsikan sebagai IP yang diperbolehkan untuk mengakses mikrotik (Whitelist) dan IP yang tidak diperbolehkan untuk mengakses mikrotik (Blacklist).

Pada skiripsi ini, pengaturan ACL yang diterapkan adalah whitelist dengan IP yang diperbolehkan mengakses mikrotik yaitu IP Address 192.168.1.14. IP ini akan secara otomatis bisa log in kedalam tampilan mikrotik walapun sudah di berikan keamana port knocking. Jadi konsepnya pc/laptop yang memiliki IP ini tidak perlu melakukan ping atau knocking melalui cmd untuk bisa masuk kedalam tampilan mikrotik.

III. HASIL DAN PEMBAHASAN

Konfigurasi Mikrotik untuk Port Knocking

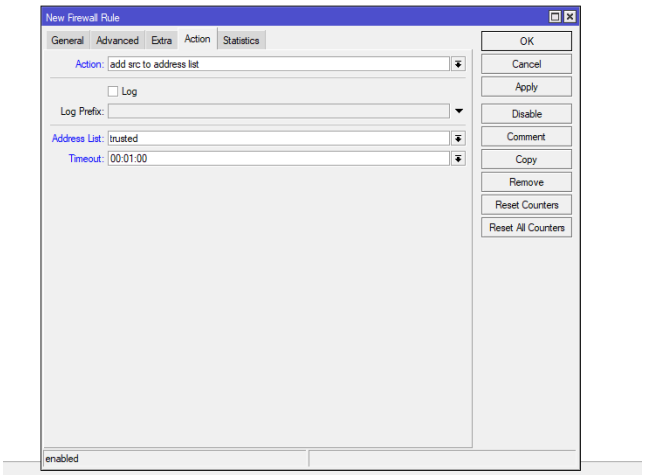


Gambar 4. Konfigurasi mikrotik untuk port knocking

Sebelum konfigurasi berhasil dilakukan, terlebih dahulu di buat 3 rules yang di gunakan untuk mengamankan mikrotik. 3 rule itu yaitu

ISSN: 2598-0076

Rule trusted



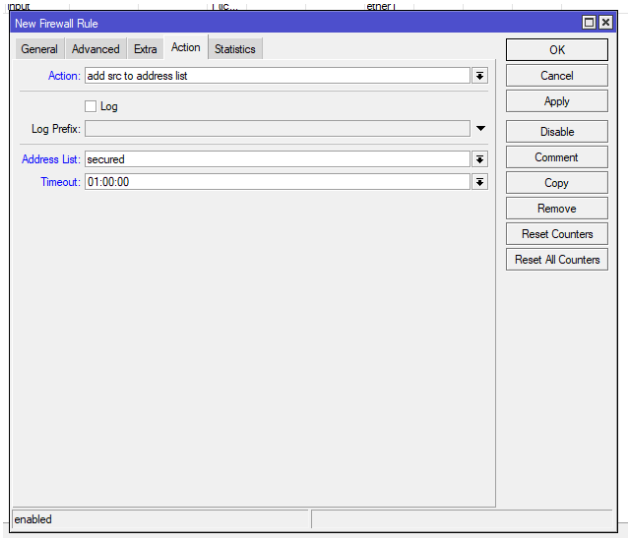
Gambar 5. Konfigurasi Rule Trusted

Caranya :

Masuk ke menu IP → firewall :

Tambahkan rule baru caranya di General untuk chainya diisi input → di Protocol diisi icmp → di In.Interface diisi ether 1 Tab action diisi add src to address list → beri nama address list menjadi trusted → time outnya 1 menit → apply dan ok

Rule secured



Gambar 6. Konfigurasi Rule secured

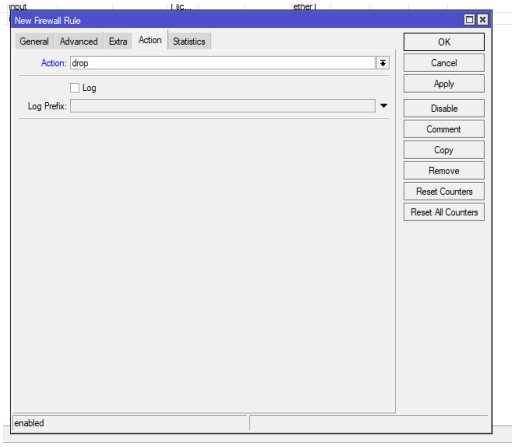
Di general isikan chain input → Protocol isikan 6(TCP) → Dst. Port isikan 3333 → In. Interface isikan ether 1

Advanced isikan trusted

ISSN: 2598-0076

Action isikan add src to address list → address list isikan Secured → Time Out isikan saru jam → klik apply lalu ok

Rule drop



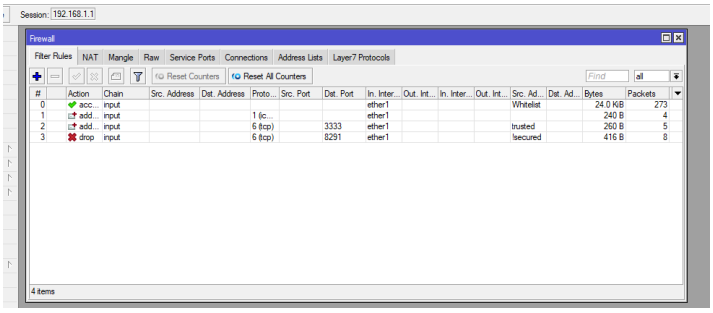
Gambar 7. Konfigurasi Rule Drop

Di general isikan chain input → Protocol isikan 6(TCP) →Dst.Port 8291 → In. Interface isiskan ether 1

Tab advenced bagian Src. Address List isikan address list yang sebelumnya telah dibuat yaitu secured kemudian centang

Tab action lalu isikan drop lalu apply dan ok

Konfigurasi Mikrotik Untuk Access Client List

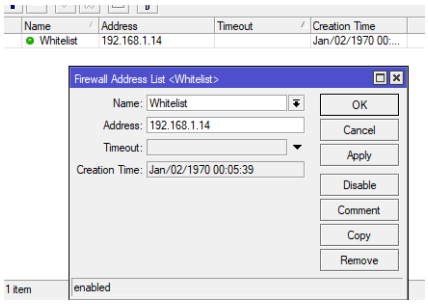


Gambar 8. Konfigurasi Mikrotik Untuk ACL

Sebelum konfigurasi dilakukan terlebih dahulu membuat address list untuk IP address yang akan di ijinkan untuk mengakses mikrotik atau beri nama Whitelist.

Cara membuatnya, yaitu

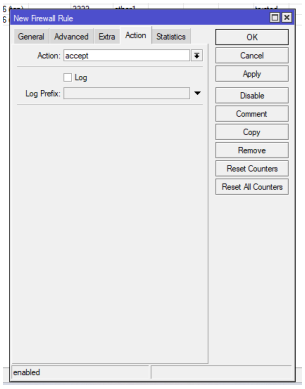
ISSN: 2598-0076



Gambar 9. Membuat IP Whitelist

Caranya : Ke menu IP, lalu firewall ke tab address list buatkan IP address yang akan di ijinkan masuk untuk meremote mikrotik dan beri nama Whitelist. Contoh Ipnya : 192.168.1.14

Membuat rules Whitelist



Gambar 10. Membuat rule Whitelist

Caranya :

Di general bagian chain isikan input dan In. Interface isikan ether 1

Di advanced isikan Whitelist

Di action isikan accept

Uji Coba Port Knocking

Percobaan 1

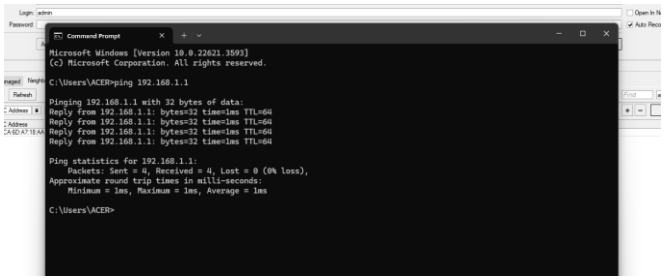
Coba masuk ke dalam tampilan mikrotik tanpa melakukan ping hasilnya tidak bisa masuk kedalam tampilan mikrotik

Gambar 11. Tampilan Log in Winbox

ISSN: 2598-0076

Percobaan 2

Lakukan ping seperti biasa ke ip address ether 1 dan coba masuk tampilan mikrotik hasilnya gagal login.

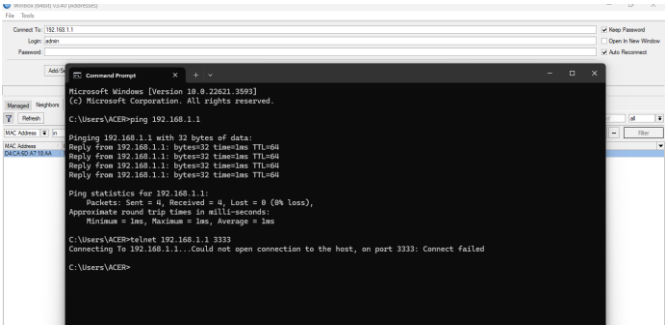


Gambar 12. Tampilan ping cmd

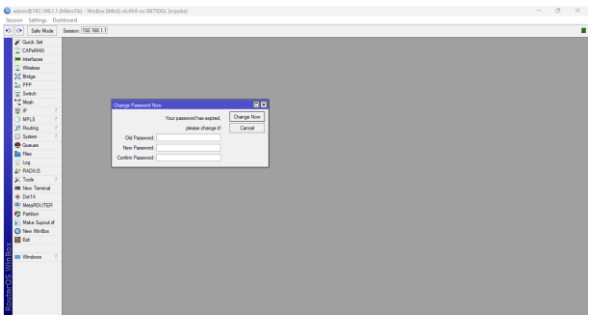
Gambar 13. Tampilan Log in Winbox

Percobaan 3

Selanjutnya lakukan ping dengan cara telnet 192.168.1.1 3333 lalu coba masuk ke tampilan mikrotik dan hasilnya berhasil masuk



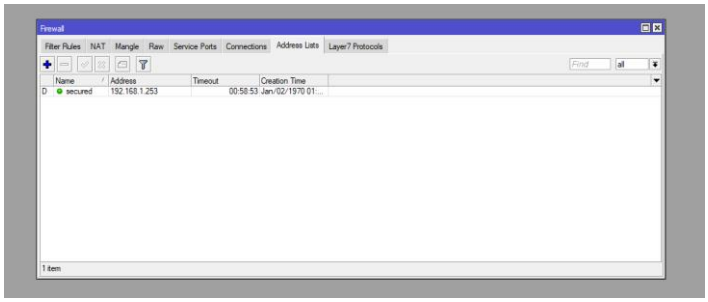
Gambar 14. Tampilan ping dan Telnet di cmd



Gambar 15. Tampilan Winbox dari Mikrotik

ISSN: 2598-0076

Cek di address list kita akan masuk sebagai secured

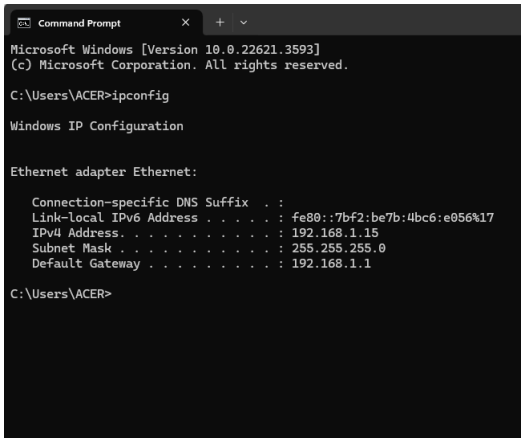


Gambar 16. Tampilan berhasil masuk dengan Secured

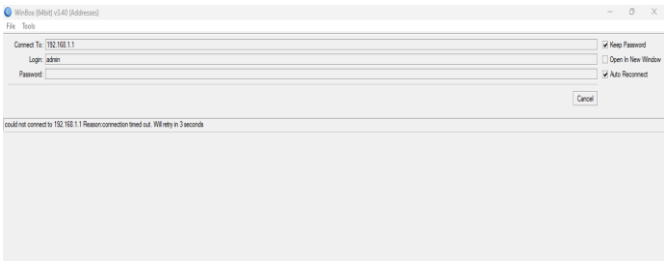
Uji Coba Access Client List (ACL)

Percobaan 1

Coba masuk menggunakan laptop dengan Ip address yang tidak sesuai dengan address list yaitu 192.168.1.14 . Contoh IP yang digunakan untuk log in tampilan mikrotik, yaitu IP address 192.168.1.15, hasilnya tidak berhasil masuk kedalam winbox.



Gambar 17. Mengecek ip untuk testing

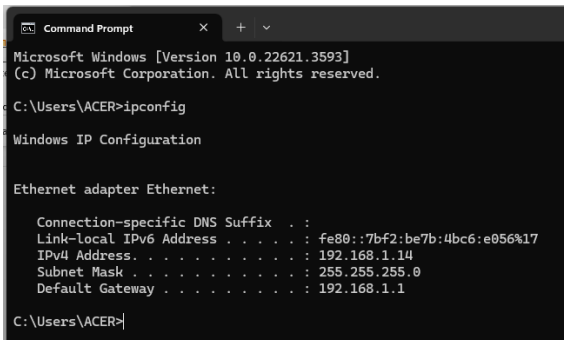


Gambar 18. Tampilan Log in gagal winbox

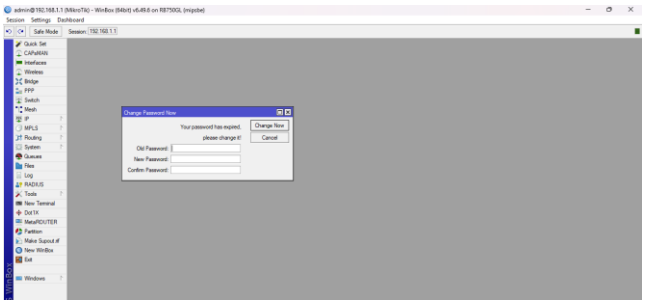
Percobaan 2

Selanjutnya coba seting ip address laptop yang akan digunakan untuk meremote mikrotik menjadi ip address 192.168.14, hasilnya dapat masauk kedalam tampilan mikrotik

ISSN: 2598-0076



Gambar 19. Mengecek ip untuk testing



Gambar 20. Tampilan log in berhasil

Analisis Hasil Port Knocking

Tabel 1. Analisis Hasil Port Knocking

No	Pengujian	Keterangan
1	Tanpa melakukan ping ke IP Address 192.168.1.1	Gagal
2	Melakukan ping ke IP Address 192.168.1.1	Gagal
3	Melakukan telnet : telnet 192.168.1.1 3333	Berhasil

Analisis Hasil Access Client List (ACL)

Tabel 2. Analisis Hasil ACL

No	Pengujian	Keterangan
1	Log in IP Address 192.168.1.15 (bukan IP yang di setting di address list)	Gagal
2	Log in IP Address 192.168.1.14 (IP yang di setting di address list)	Berhasil

ISSN: 2598-0076

IV. SIMPULAN

Berdasarkan hasil penelitian yang peneliti peroleh dilapangan dapat disimpulkan sebagai Ketika sudah dilakukan pengaturan port knocking pada ether 1 mikrotik RB GL750, kemudian hendak melakukan remote melalui ether 1 tanpa melakukan ping ke ip address ether 1 maka hasilnya tidak bisa masuk ketampilan mikrotik (gagal remote). Ketika sudah dilakukan pengaturan port knocking di ether 1, kemudian sudah melakukan ping ke ip address(192.168.1.1) ether 1 mikrotik untuk meremote mikrotik maka hasilnya tidak bisa masuk ke tampilan mikrotik (gagal remote).

Ketika sudah dilakukan pengaturan port knocking di ether 1, kemudian sudah melakukan ping (192.168.1.1 lalu telnet ke ip address (telnet 192.168.1.1 3333) ether 1 maka hasilnya berhasil masuk ke tampilan mikrotik. Selain melakukan ping dan telnet ada cara lain yaitu dengan menginstal knock client di laptop atau pc kemudian lakukan hal yang sama ketika akan meremote mikrotik dengan mengetikkan perintah di cmd knok kemudian ip address lalu kata kunci contoh (knock 192.168.1.1 3333). Ketika sudah dilakukan pengaturan Access Client List (ACL) di ether 1 mikrotik, Ip address yang telah di buat untuk dapat meremote mikrotik (192.168.1.14) tidak perlu melakukan ping atau telnet ke mikrotik untuk dapat masuk ke dalam tampilan mikrotik. Namun apabila bukan Ip address 192.168.1.14 maka perlu dilakukan ping dan telnet ke Ip address ether 1.

DAFTAR RUJUKAN

[1] W. F. Fatoni, . A. Hidayat and Mustika, "IMPLEMENTASI SISTEM KEAMANAN JARINGAN KOMPUTER," *Jurnal Mahasiswa Ilmu Komputer (JMIK),* vol. 03, p. 292, 2022.

[2] W. . F. Fatoni, A. Hidayat and M. , "MPLEMENTASI SISTEM KEAMANAN JARINGAN KOMPUTER DENGAN METODE PORT KNOCKING PADA LKP SURYA KOMPUTER," *Jurnal Mahasiswa Ilmu Komputer (JMIK),* pp. 294-295, 2022.

[3] M. R. Amar, S. Anwar and O. Nurdiawan, "Optimalisasi Menggunakan Access Control List Berbasis Mikrotik pada Ammi event Organizer," *MEANS (Media Informasi Analisa dan Sistem),* vol. 7, p. 118, 2022.

[4] R. Sulaiman, R. S. A. Fathul and A. M. Raya, "Implementasi Metode Access Control List Pada Mikrotik dalam mengamankan jaringan internet dikantor lurah Air Selemba," *SABER:Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi,* pp. 213-214, 2024.

[5] B. K. Sihotang, S. Sumarno and B. E. Damanik, "Implementasi Access Control List Pada Mikrotik dalam Mengamankan Koneksi Internet Koperasi Sumber Dana Mutiara," *Jurnal Riset Komputer,* pp. 229-234, 2020.

ISSN: 2598-0076