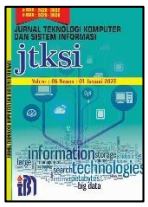


JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi)

JTKSI, Volume 6, Nomor 01, Januari 2023
E ISSN: 2620-3030; P ISSN: 2620-3022, pp.94-101
Accredited SINTA 4 Nomor 200/M/KPT/2020
http://ojs.stmikpringsewu.ac.id/index.php/jtksi

Received: 30 Desember 2022; Revised: 13 Januari 2023; Accepted: 16 Januari 2023

Implementasi Multiple Port knocking dan Port blocking Untuk Peningkatan Keamanan Hak Akses Administrator Pada Routerboard Mikrotik

Dian Novianto[1], Yohanes Setiawan Japriadi[2], Lukas Tommy[3]
[1,2,3]Program Studi Teknik Informatika, ISB Atma Luhur, Kota Pangkalpinang, Kepulauan Bangka Belitung
Jl. Jend. Sudirman, Kel. Selindung, Pangkalbalam, Kota Pangkalpinang, Kepulauan Bangka Belitung, Indonesia
Email : diannovianto@atmaluhur.ac.id[1], ysetiawanj@atmaluhur.ac.id[2], lukastommy@atmaluhur.ac.id[3]

Abstract

Access rights to network systems are things that must be limited because they involve the operations of an organization. Making a password alone is not enough, because there is a brute force attack that can guess the password, so that other people who are not entitled, can get access rights to the network system. Therefore it is necessary to create a mechanism to avoid brute force attacks to secure access rights, especially administrator access rights. One combinations of method that can be used is port knocking and port blocking, using 3 combinations of port knocking and port blocking will increase the chances of a brute force attack failing because failure to knock will activate the firewall to enable port blocking. For the application of this method, a tool is needed in the form of an RB951Ui-2nD routerboard, besides that, a network system development method is needed which is a reference in system development, in this study the method used is PPDIOO which consists of Prepare, Plan, Design, Implement, Operate, and Optimize. And also some supporting tools for the development of the system in the form of Unified Modeling Language (UML). The result of applying 3 combinations of multiple port knocking, produces 6 opportunities that can strengthen the router's access security system from brute force attacks.
Keywords : *Port knocking, port blocking, mikrotik*

Abstrak

Hak akses terhadap sistem jaringan merupakan hal yang harus dibatasi, karena menyangkut operasional sebuah organisasi. Membuat kata sandi saja tidaklah cukup, karena adanya serangan brute force yang dapat menebak kata sandi tersebut, sehingga orang lain yang tidak berhak, bisa mendapat hak akses atas sistem jaringan. Oleh karena itu perlunya membuat sebuah mekanisme untuk terhindar dari serangan brute force untuk mengamankan hak akses khususnya hak akses administrator. Salah satu kombinasi metode yang dapat digunakan adalah *port knocking* dan *port blocking*, dengan menggunakan 3 kombinasi *port knocking* dan *port blocking* akan meningkatkan peluang gagalnya serangan brute force, karena kegagalan pada *knocking* akan mengaktifkan *firewall* untuk mengaktifkan *port blocking*. Untuk penerapan metode ini, dibutuhkan alat berupa routerboard mikrotik tipe *RB951Ui-2nD*, selain itu diperlukan metode pengembangan sistem jaringan yang menjadi acuan dalam pengembangan sistem, dalam penelitian ini metode yang digunakan adalah PPDIOO yang terdiri dari: *Prepare, Plan, Design, Implement, Operate, dan Optimize*. Dan juga beberapa tools pendukung untuk pengembangan sistem tersebut berupa *Unified Modelling Language* (UML). Hasil dari penerapan *multiple port knocking* 3 kombinasi, menghasilkan 6 kombinasi peluang yang dapat memperkuat sistem pengamanan hak akses terhadap router dari serangan *brute force*.
Kata Kunci : *Port knocking, port blocking, mikrotik*

I. PENDAHULUAN

Keamanan jaringan adalah sebuah sistem yang dibangun agar jaringan komputer dapat berjalan dengan baik dan terhindar dari ancaman baik dari luar maupun dari dalam yang dapat merusak sistem jaringan dan menyebabkan jaringan tidak dapat berkerja sehingga dapat mengganggu operasional sebuah organisasi yang sangat tergantung dengan jaringan komputer, seperti ancaman pencurian data perusahaan, bobolnya sistem karena kata sandi yang diketahui oleh orang lain yang tidak berhak dan segala macam serangan serta usaha penyusupan atau pemindaian untuk mencapai tujuan. Keamanan jaringan dapat dilakukan dengan cara memberikan proteksi atau perlindungan pada *router* sebagai pengatur lalu lintas data di jaringan. Proteksi dan keamanan pada *router* sangatlah penting untuk menjaga kelangsungan jaringan komputer sebuah organisasi. Terutama untuk menjaga *router* Mikrotik dari segala macam akses ilegal yang mencoba untuk

masuk ke sistem jaringan komputer dan mengelola jaringan pada *router* milik sebuah organisasi, serangan brute force merupakan serangan yang paling banyak terjadi untuk mendapatkan hak akses administrator, dari hasil survey yang dilakukan oleh kaspersky, pada tahun 2020 terjadi peningkatan serangan brute force sebesar 197 %[1]. Sehingga mebuat kata sandi saja tidaklah cukup untuk mengamankan hak akses, karena adanya serangan brute force yang dapat menebak kata sandi tersebut, sehingga orang lain yang tidak berhak, bisa mendapat hak akses atas sistem jaringan. Bruteforce, adalah metode trial dan error yang digunakan oleh program aplikasi untuk memecahkan data yang telah dienkripsi seperti username dan *password* atau standar data enkripsi (DES). Pengujian serangan brute force dilakukan untuk menganalisa username dan *password* dengan cara mencoba setiap kemungkinan username dan *password* yang ada[2].

Salah satu kombinasi metode yang dapat digunakan adalah kombinasi *port knocking* dan *port blocking*. Metode *Port knocking* merupakan metode yang digunakan untuk membuka akses ke *port* tertentu yang telah ditolak oleh *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa *protocol* TCP, UDP maupuan ICMP. Jika koneksi yang dikirimkan oleh *host* tersebut sudah sesuai dengan *rule knocking* yang diterapkan, maka secara dinamis *firewall* akan memberikan akses ke *port* yang sudah ditolak [3]. Sedangkan *port blocking* merupakan tindakan menutup *port* sehingga mencegah akses *host* ke *port* tersebut. *Port blocking* menggunakan *firewall* untuk menjalankan aksinya. *Firewall* sendiri merupakan sebuah sistem atau sebuah perangkat yang memberi akses pada lalu lintas di jaringan komputer yang dianggap aman untuk dilewati dan melakukan pencegahan terhadap lalu lintas di jaringan yang dianggapnya tidak aman [4].

Multiple *port knocking* dilakukan dengan melakukan pengetukan *port* atau layanan lebih dari satu, khususnya *port* atau layanan yang sering digunakan oleh host administrator jaringan, baik untuk pengecekan koneksi maupun saat akan masuk kedalam sistem *router*, antara lain ICMP(A), *telnet port* 23 (B), dan ssh *port* 23 (C). Layanan *port* tersebut harus diketuk secara berurutan, sehingga apabila dihitung akan menghasilkan 6 kombinasi *port knocking* (ABC, ACB, BAC, BCA, CAB, dan CBA), sehingga dapat memberikan pilihan bagi administrator untuk menggunakan salah satu pola tersebut. Sedangkan *port blocking* bertugas untuk menutup *port* tersebut sebelum dilakukan *knocking*, dan *port* apabila *knocking* dilakukan dengan benar, dan juga memblokir alamat IP pengakses apabila salah melakukan *knocking*. Dengan memanfaatkan port *knocking* maka tindakan brute force tidak dapat dilakukan, dikarenakan proses masuk ke sistem router yang tidak hanya mengandalkan kata sandi saja. Jika kata sandi diketahui namun pola port *knocking* tidak diketahui, maka tetap tidak dapat masuk kedalam sistem router.

Model pengembangan jaringan yang digunakan dalam penelitian ini adalah metode PPDIOO yang terdiri atas Persiapan, Perencanaan, Desain, Implementasi, Operasi, dan Optimalisasi. PPDIOO merupakan metode pengembangan dalam bidang jaringan komputer yang di kembangkan oleh perusahaan Cisco [5]. Dengan mengacu pada metodologi ini, peneliti sudah mengetahui langkah-langkah kunci untuk mencapai keberhasilan dalam perancangan jaringan yang dilakukan[6].

Manfaat yang akan didapat dari penelitian ini nantinya dapat menghasilkan sebuah kombinasi mekanisme pengamanan akses ilegal terhadap *router* yang menjadi pengatur lalu lintas data pada sebuah organisasi. Selain itu juga dapat terhindar dari serangan brute force, dan mem*filter* request yang tidak sesuai.

II. METODE PENELITIAN

Metode penelitian yang penulis gunakan dalam penelitian ini menggunakan metode kualitatif, dimana peneliti yang akan menjadi alat utama dalam proses pengumpulan data [6]. Pengumpulan data dilakukan oleh penulis dengan mengumpulkan referensi yang berhubungan dengan topik penelitian, baik dari jurnal ilmiah maupun dari buku bacaan. Karena dengan cara ini penulis dapat lebih mengerti konsep dari *port knocking* dan *port blocking*, terutama cara kerja dari *firewall* saat menutup dan membuka akses kedalam *router*. Sehingga nantinya dalam pengembangan mekanisme kombinasi multiple *port knocking* dan *port blocking* akan berjalan dengan baik.

Model pengembangan *PPDIOO* memiliki beberapa tahapan yang menjadi acuan dan harus dijalankan oleh penulis, tahapan tersebut antara lain: tahap pertama adalah persiapan yang berupa studi pustaka, tahap kedua adalah perencanaan berupa pengumpulan kebutuhan teknis dan non teknis, tahap ketiga adalah desain berupa perancangan topologi jaringan yang akan dibuat dan disimulasikan, tahap keempat adalah implementasi berupa pengaturan sistem pada *router*board mikrotik, tahap kelima adalah operasi berupa tindakan ujicoba terhadap sistem yang telah dibuat, dan tahap keenam adalah optimasi berupa penambahan ataupun perbaikan dari kekurangan sistem yang ditemukan.

Implementasi terhadap penjelasan pada paragraf sebelumnya mengenai model pengembangan jaringan PPDIOO dalam penelitian ini, sebagai berikut:

1. Persiapan

Dimana dalam tahapan ini penulis akan menyiapkan peralatan dan bahan-bahan atau studi literatur dengan cara mengumpulkan referensi yang ada dijurnal lima tahun terakhir agar memudahkan penulis dalam menjalankan penelitian. Adapun judul penelitian yang menjadi referensi antara lain:

a. Penelitian yang dilakukan oleh Amarudin, pada tahun 2018 dengan judul "Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik *Router* OS Menggunakan Metode *Port knocking*"[[3].

b. Penelitian dari Randi Rizal, Ruuhwan, Kelvin Ajie Nugraha, pada tahun 2020 dengan judul "Implementasi Keamanan Jaringan Menggunakan Metode *Port blocking* dan *Port knocking* Pada Mikrotik RB-941"[7].

c. Penelitian oleh D. Desmira, dan R. Wiryadinata pada tahun 2022 mengenai "Rancang Bangun Keamanan *Port* Secur Shell (SSH) Menggunakan Metode *Port knocking*"[8].

d. Penelitian oleh Januar Al Amin pada tahun 2020 mengenai "Implementasi Keamanan Jaringan Dengan IP Table Sebagai *Firewall* Menggunakan Metode *Port knocking*"[9].

e. Penelitian oleh M Julkarnain dan A Afahar pada tahun 2021 mengenai "Implementasi *Port knocking* Untuk Keamanan Jaringan Smk 1 Sumbawa Besar"[10].

f. Penelitian oleh Ahmad Zafrullah Mardiansyah, Yayank Muhammad Abdussyakur, Andy Hidayat Jatmika, pada tahun 2021 mengenai "Optimasi *Port knocking* dan Honeypot Menggunakan Ip Tables Sebagai Keamanan Jaringan Pada Server" [11].

2. Perencanaan

Pada tahap perencanaan ini yang dilakukan oleh penulis adalah menganalisa kebutuhan-kebutuhan teknis dan non teknis, sehingga dalam proses atau tahap selanjutnya dapat berjalan dengan baik. Adapun dalam penelitian sistem keamanan jaringan berbasis *router*board mikrotik ini, spesifikasi kebutuhan perangkat keras dan perangkat lunak yang peneliti gunakan terlihat seperti pada tabel 1 dan 2:

Tabel 1. Kebutuhan Perangkat Keras

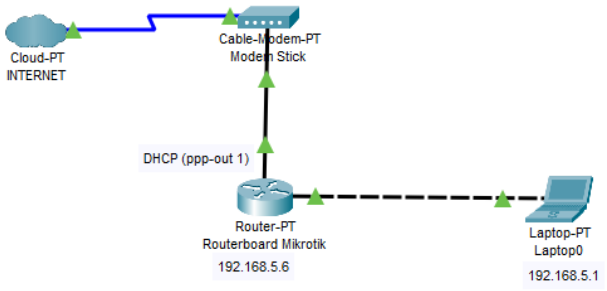
No	Perangkat Keras	Spesifikasi
1	Laptop acer	Processor A8-4500M up to 2.80 GHz, GPU: AMD HD8750 2GB Vram, RAM 4GB, SSD 240GB, HDD 500GB
2	Mikrotik *Router*board	RB951Ui-2^{nD}
3	Kabel UTP	CAT 5E
4	Konektor	RJ45
5	Modem Stik	Telkomsel Flash

Tabel 2. Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Spesifikasi
1	Winbox	Versi 3.31
2	*Putty*	Versi 0.6.7
3	Nmap	Versi 80
4	Packet Tracer	Versi 8.1.1.xxx
5	Windows	Versi 8.1
6	Mikrotik *Router*OS	Versi 7.1 beta 6
7	Astah Profesional	Versi 8.2.0

3. Desain

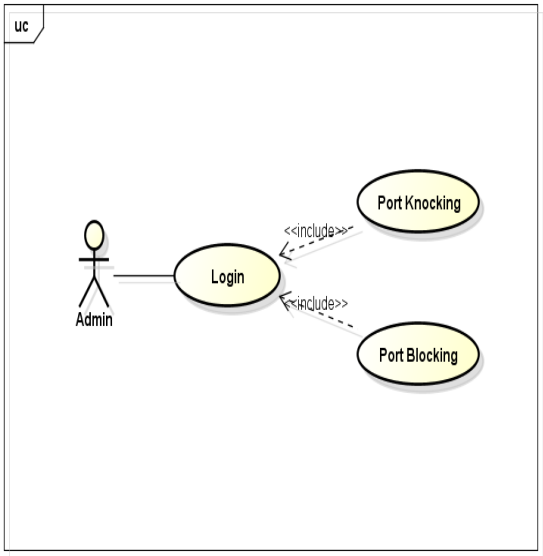
Implementasi tahapan ketiga adalah tahap desain, dalam tahapan ini yang dilakukan oleh penulis adalah mendesain topologi jaringan dan alur kerja dari sistem dalam topologi yang dibangun, baik untuk *port knocking* maupun *port blocking*. Dimana dalam prosesnya penulis mendesain topologi jaringan menggunakan aplikasi *cisco packet tracer* versi 8.1.1 dan untuk diagram UML menggunakan *software astah professional*.



Gambar 1. Topologi Jaringan

Topologi yang dirancang akan digunakan dalam implementasi pada tahapan PPDIOO selanjutnya. Selain membuat rancangan topologi, penulis juga membuat rancangan diagram UML, antara lain: *use case diagram*, *activity diagram*, dan *deployment diagram*. Berikut ini merupakan diagram UML yang sudah dibuat oleh penulis dari hasil analisa, yang akan menggambarkan interaksi *user* dan sistem di jaringan yang akan dibangun.

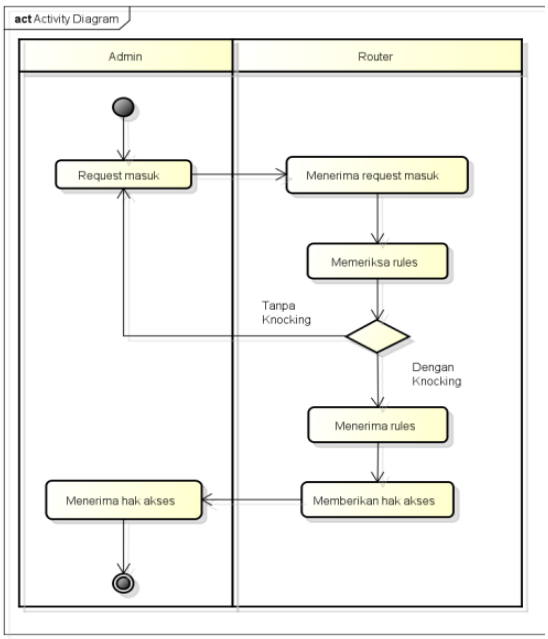
a. *Use Case*



Gambar 2. *Use Case*

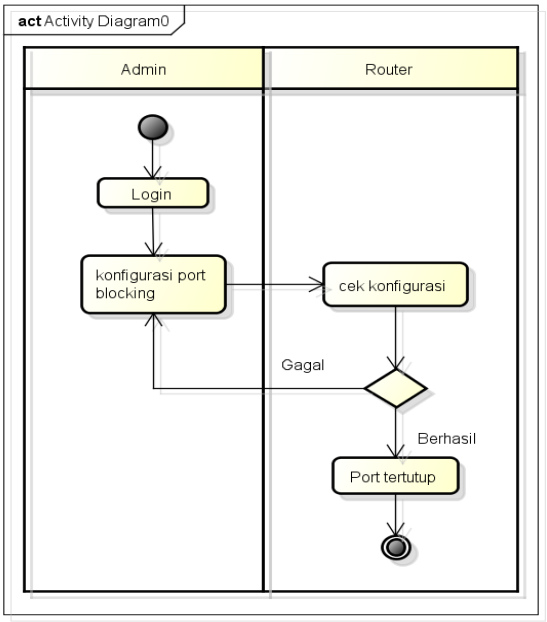
Dari gambar 2, untuk dapat login seorang administrator jaringan membutuhkan langkah *port knocking* yang tepat agar dapat membuka *port* yang di blokir oleh *firewall*, sehingga relaasi *port knocking* dan *port blocking* include terhadap login.

b. Activity Diagram



Gambar 3. *Activity Diagram Port knocking*

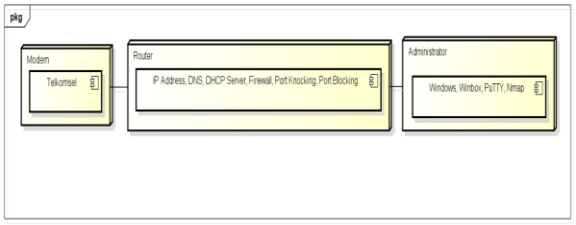
Pada gambar 3 menjelaskan alur proses *knocking* yang dimulai oleh pengguna meminta untuk dapat masuk ke sistem *router*, lalu *router* menerima permintaan masuk tersebut. Kemudian *router* akan memeriksa permintaan tersebut, apakah disertai *port knocking* atau tidak. Jika pengguna menggunakan *port knocking* yang benar, maka *router* menerima *rule*s tersebut dan *router* akan memberikan hak akses. Sedangkan jika pengguna tidak melakukan *knocking* atau *port knocking* yang dilakukan salah, maka *router* akan menolak permintaan akses masuk ke sistem *router*, dan apabila salah melakukan *knocking* maka alamat ip dari pengguna akan di blokir oleh *firewall* sementara waktu dan harus menunggu beberapa saat sebelum mencoba masuk kembali.



Gambar 4. *Activity Diagram Port blocking*

Pada gambar 4, proses penutupan *port* dilakukan oleh administrator jaringan, sehingga kondisi awal sebelum dilakukan *knocking*, semua *port* yang dibutuhkan dalam keadaan tertutup atau terblok. Konfigurasi dilakukan dengan login terlebih dahulu ke sistem *router*board mikrotik lalu dari menu *firewall port* di tutup.

c. Deployment diagram

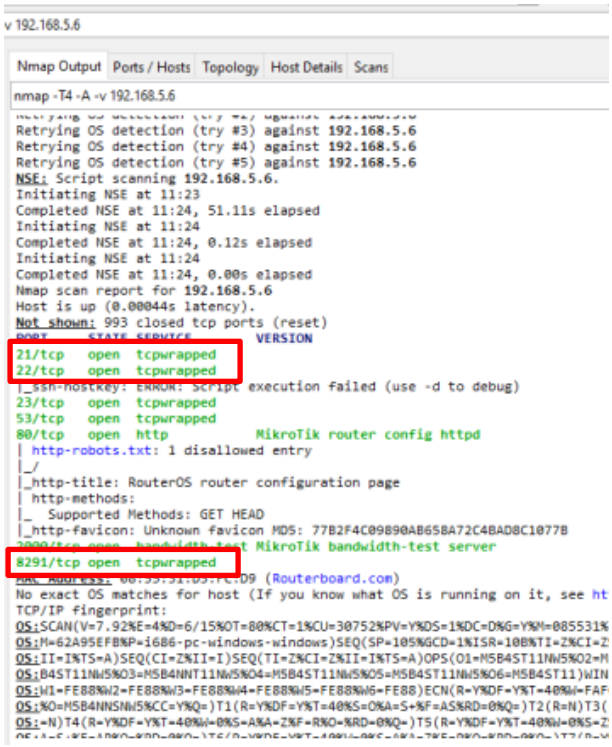


Gambar 5. *Deployment diagram*

Pada gambar 5 terdapat 3 komponen yang akan digunakan pada implementasi *port knocking* dan *port blocking* di jaringan, yaitu Modem yang merupakan sumber internet, *Router* yang digunakan untuk konfigurasi IP Address, DNS, DHCP Server, *Port knocking* dan *Port blocking* pada *Firewall*. Dan perangkat admin yang menggunakan sistem operasi windows, perangkat lunak winbox, PuTTY, dan Nmap untuk melakukan proses konfigurasi agar sesuai dengan kebutuhan penelitian.

4. Implementasi

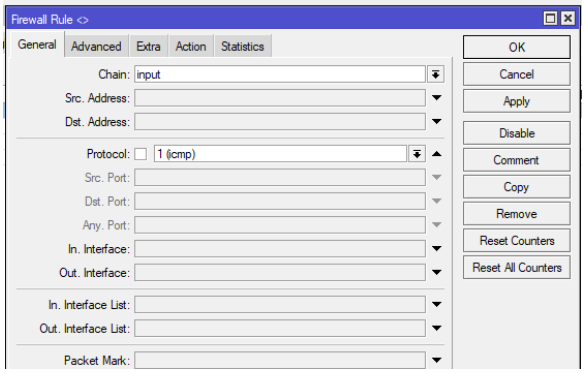
Dalam tahapan ke empat atau implementasi ini, penulis akan melakukan konfigurasi pada beberapa fitur yang ada didalam *router*board mikrotik menggunakan aplikasi *winbox*, hal ini dimaksudkan agar penulis bisa mencapai tujuan dari penelitian ini, yaitu meningkatkan keamanan akses terhadap *router* menggunakan metode *port knocking* dan *port blocking*. Langkah awal yang harus dilakukan untuk membuat sistem *port knocking* dan *port blocking* dengan melakukan pengecekan terlebih dahulu terhadap *port-port* yang biasanya digunakan oleh administrator untuk masuk kedalam sistem *router* menggunakan aplikasi Nmap.



Gambar 6. Hasil pemindaian *Nmap*

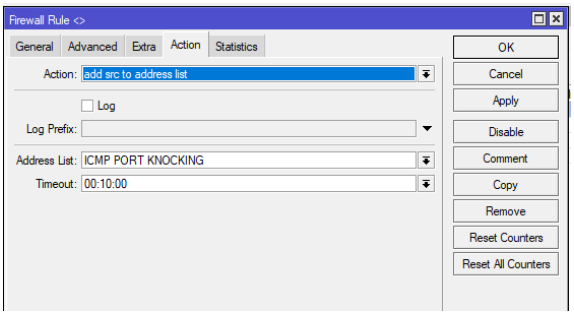
Pada Gambar 6, terlihat beberapa *port* service pada mikrotik dalam keadaan terbuka atau open *port* seperti *port* 21, *port* 22, *port* 23, *port* 8291, dan *port* 80. Untuk menutup semua *port* tersebut penulis menggunakan metode *port blocking* untuk menutup akses ke *router* mikrotik. Dan hanya yang mengetahui urutan *port knocking* yang benar saja yang bisa mengakses *router* mikrotik tersebut. Untuk *port knocking* dalam penelitian ini, penulis menggunakan kombinasi *knocking* menggunakan ICMP, Telnet, dan SSH.

Ping (Packet Internet Gopher) merupakan perintah yang biasa digunakan oleh admin jaringan untuk mengecek koneksi pada sebuah komputer yang saling terhubung dalam jaringan.



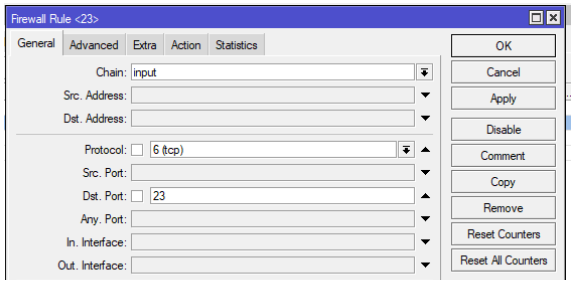
Gambar 7. *Rule* ICMP *Knocking*

Pada menu *firewall*, chain yang ditambahkan adalah input, dan *protocol* nya ICMP.



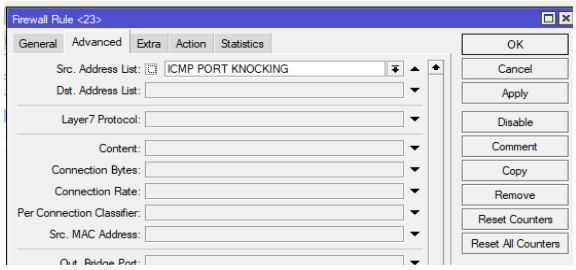
Gambar 8. *Rule* ICMP *Knocking* 2

Gambar 7 dan 8 menunjukan aturan pada *firewall* saat ada permintaan masuk pada *protocol* icmp, maka alamat ip tersebut akan disimpan didalam *address list* selama 10 menit dengan nama ICMP *PORT KNOCKING*, karena hanya yang sudah melakukan *knocking* dengan ping yang bisa melanjutkan *knocking* selanjutnya yaitu dengan telnet.



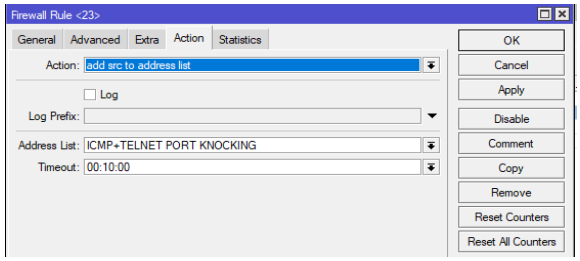
Gambar 8. *Rule* Telnet *Knocking*

TELNET merupakan akronim atau singkatan dari *Telecommunication Network*, sebuah perangkat lunak yang dapat digunakan untuk melakukan pengendalian jarak jauh pada sistem komputer atau *remote access*, *port* yang digunakan oleh service telnet adalah *port* 23 dan *protocol* TCP.



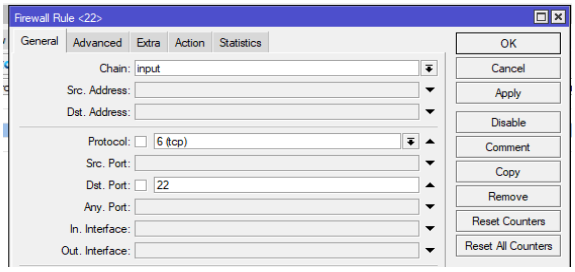
Gambar 9. *Rule* Telnet *Knocking* 1

Dari gambar 9 diketahui bahwa alamat *host* yang dapat melakukan telnet bersumber dari *address list* yang bernama ICMP *PORT KNOCKING*.



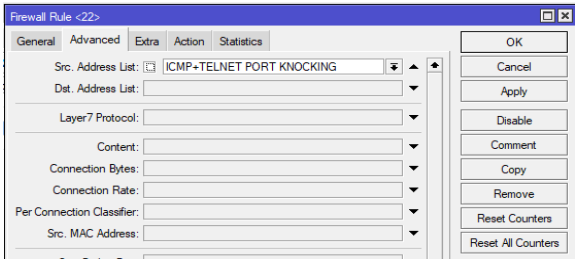
Gambar 10. *Rule* Telnet *Knocking* 2

Pada gambar 10 menunjukkan alamat yang telah melakukan *knocking* icmp dan telnet akan disimpan ke *address list* dengan nama baru, yaitu ICMP + TELNET *PORT KNOCKING*. Dimana alamat yang tersimpan dapat melanjutkan untuk *knocking* menggunakan SSH.

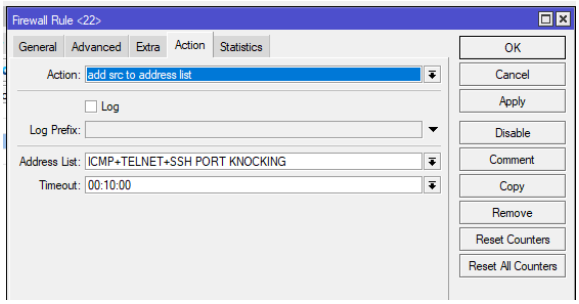


Gambar 11. *Rule* SSH *Knocking*

Pada menu *firewall*, chain yang ditambahkan adalah input, dan *protocol* yang dipilih TCP dan *port* yang digunakan ssh adalah *port* 22.



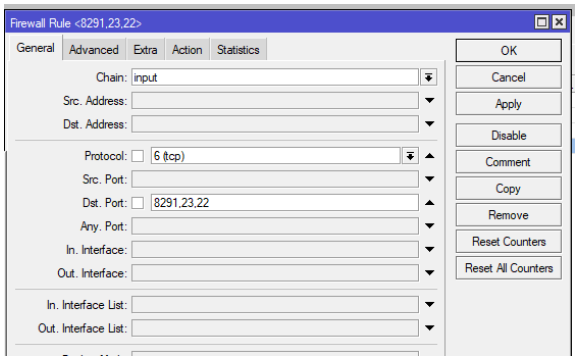
Gambar 12. *Rule* SSH *Knocking*



Gambar 13. *Rule* SSH *Knocking*

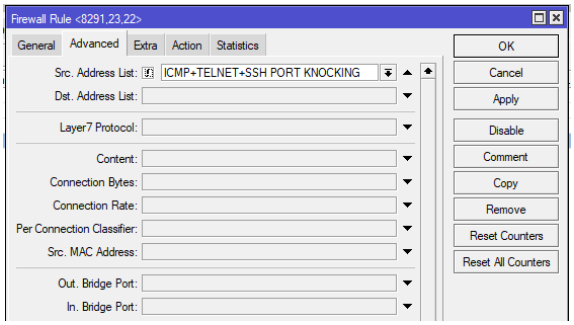
Dari gambar 12 dan 13 dapat dijelaskan bahwa *knocking* menggunakan SSH baru dianggap valid apabila alamat ip bersumber dari *address list* yang bernama ICMP + TELNET *PORT KNOCKING*, dan hasil *knocking* dari SSH akan disimpan pada *address list* dengan nama ICMP + TELNET + SSH *PORT KNOCKING*, dengan lama waktu 10 menit.

Setelah konfigurasi *port knocking* dilakukan, langkah selanjutnya adalah melakukan konfigurasi *port blocking* sesuai dengan desain activity diagram pada tahap sebelumnya. Konfigurasi pada *port blocking* dalam penelitian ini bertujuan untuk menutup *port* yang biasanya digunakan untuk remot akses ke *router*, yaitu winbox (8291), telnet (23), dan ssh (22).



Gambar 14. *Port blocking*

Chain yang digunakan input, *protocol* yang digunakan untuk mengakses ketiga service tadi menggunakan protokol TCP, dan destination *port*nya 8291, 23, dan 22.

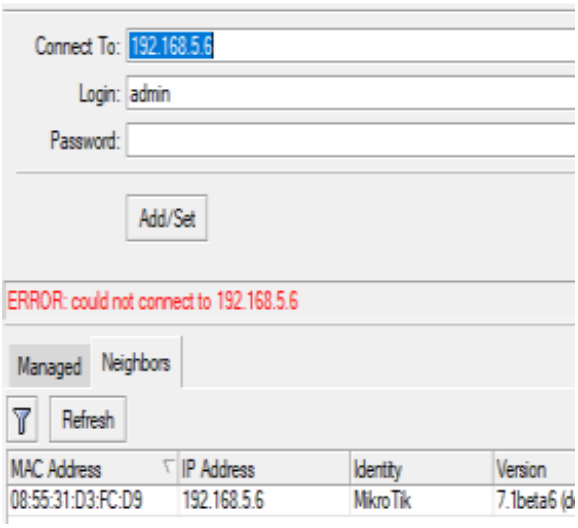


Gambar 15. *Port blocking* 1

Source *address list* dengan tanda ! menunjukan bahwa selain alamat ip yang terdaftar pada *address list* dengan nama ICMP + TELNET + SSH *PORT KNOCKING*, *router* harus menolak alamat permintaan untuk mengakses ketiga service tadi. Karena hanya yang sudah melakukan *knocking* sesuai dengan urutan yang ditentukan yang dapat mengakses *router* melalui ketiga service tersebut.

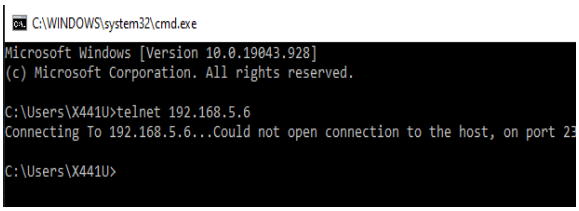
III. HASIL DAN PEMBAHASAN

Pada tahapan kelima dari model pengembangan jaringan PPDIOO, yaitu tahapan operasi, maka pada bagian ini akan di jelaskan hasil dari penerapan multiple *port knocking* dan *port blocking* untuk meningkatkan sistem keamanan akses terhadap *router*



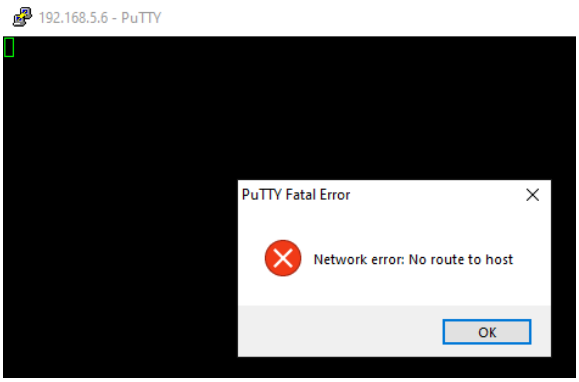
Gambar 16. Tampilan login winbox

Gambar 16 menunjukan bahwa *host* tidak dapat masuk ke dalam sistem *router* secara langsung melalui winbox tanpa melakukan *knocking* terlebih dahulu, hal ini sesuai dengan konfigurasi yang telah dilakukan pada tahapan sebelumnya.



Gambar 17. Tampilan login telnet

Gambar 17 menunjukkan bahwa saat percobaan *remote* akses menggunakan service telnet menuju *router*, *router* menolak membuka akses untuk koneksi tersebut. Hal ini juga berlaku saat *remote* akses dilakukan menggunakan service ssh yang terlihat pada gambar 18, meskipun koneksi dari ssh ini lebih aman karena koneksi yang terenkripsi, dan dilakukan menggunakan aplikasi putty, *remote* akses juga gagal dilakukan. Hal ini menunjukkan bahwa *port blocking* sudah bekerja dengan baik dalam menutup *port* koneksi untuk ketiga service tersebut.



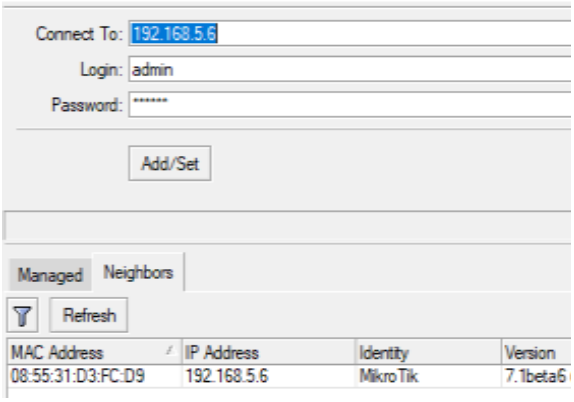
Gambar 18. Tampilan login ssh

Selanjutnya untuk memastikan bahwa kegagalan *remote* akses ketiga *port* dikarenakan *filter* dari *firewall*, penulis melakukan pemindaian menggunakan aplikasi nmap. Gambar 19 menunjukkan bahwa ketiga *port* memang sudah ter*filter* dengan baik.

Gambar 19. Tampilan pemindaian nmap

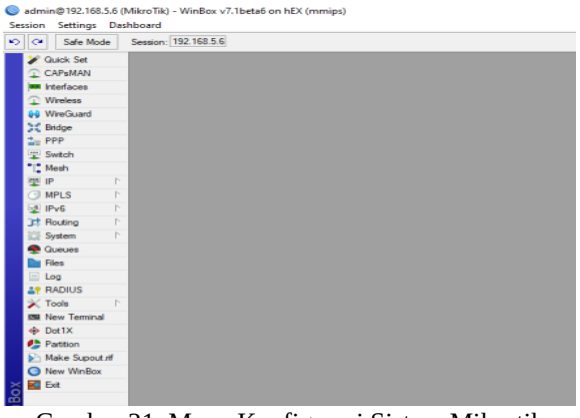
Pada bagian selanjutnya, dilakukan *port knocking* secara berurutan, dimulai dari ICMP menggunakan perintah ping ke alamat *router*, dilanjutkan dengan *remote* akses melalui telnet pada *port* 23 menggunakan aplikasi putty, dan *remote* akses melalui ssh pada *port* 22 menggunakan aplikasi putty.

Hasil dari *port knocking* yang benar akan mendaftarkan alamat ip dari *host* yang melakukan *knocking* ke dalam *address list*, sehingga *router* akan membuka koneksi terhadap *port* dari service winbox *port* 8291, telnet *port* 23, dan ssh *port* 22.



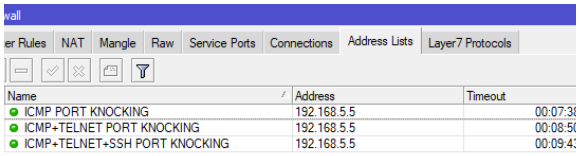
Gambar 20. Login Winbox

Dari gambar 20 terlihat bahwa saat *host* yang telah melakukan *knocking* dengan benar dan mencoba masuk kedalam sistem *router*, maka *router* akan memberikan akses tersebut seperti yang terlihat pada gambar 21.



Gambar 21. Menu Konfigurasi Sistem Mikrotik

Setelah berhasil masuk kedalam sistem *router* mikrotik, administrator bisa melakukan konfigurasi sesuai dengan kebutuhan, salah satunya adalah melihat *address list* yang berisi alamat ip *host* yang berhasil melakukan *knocking*. Seperti yang terlihat pada gambar 22.



Gambar 22. Hasil *Knocking*

Gambar 22 menunjukan bahwa alamat ip *host* yang melakukan *knocking* sudah tercatat dengan nama yang berbeda, dimana alamat ipnya adalah 192.168.5.5, alamat ip ini sesuai dengan skema topologi yang telah di desain pada tahapan sebelumnya. Selama alamat tersebut masih terdaftar didalam *address list*, maka *host* tersebut dapat masuk kedalam sistem *router*, namun bila alamat *host* sudah hilang dari *address list*, maka *host* diharuskan melakukan *knocking* ulang dengan pola yang benar.

IV. KESIMPULAN

Setelah dilakukan penelitian ini, penulis dapat mengambil beberapa kesimpulan metode *port knocking* dan *port blocking* bisa mengamankan akses ke *router* mikrotik dengan cara terlebih dahulu mengirimkan paket *knocking* berupa ping ke IP Address, telnet, dan ssh. Terbukti, dengan adanya *rule knocking* yang tepat, maka administrator jaringan bisa mengakses dan mengelola jaringan di *router* mikrotik dengan aman. Service *port* yang terbuka dalam *router* mikrotik dapat diamankan dengan melakukan *blocking port* sehingga menjadi ter-*filter*ed. Terbukti dapat menambah keamanan terhadap hak akses administrator menuju sistem *router*, dan terhindar dari serangan brute force meskipun tidak praktis dibandingkan dengan hanya mengandalkan penggunaan *password* saja.

DAFTAR PUSTAKA

[1] https://www.cnnindonesia.com/teknologi/20210421113409-185-632702/waspada-serangan-bruteforce-di-ri-dan-cara-mengatasinya

[2] A. Z. Mardiansyah, Y. M. Abdussyakur, and A. H. Jatmika, "OPTIMASI *PORT KNOCKING* DAN HONEYPOT MENGGUNAKAN Security)," vol. 3, no. 2, 2

[3] Amarudin, "Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik *Router* Menggunakan Metode *Port knocking*," Semin. Nas. Sains dan Teknol. 2018, pp. 1–7, 2018.

[4] U. B. Darma, T. Brades, T. Komputer, F. Vokasi, and U. B. Darma, "PEMANFATAAN METODE *PORT KNOCKING* DAN *BLOCKING*," pp. 99–107.

[5] Imam Solikin. 2017. Penerapan Metode PPDIOO dalam Pengembangan LAN dan WLAN. TEKNOMATIKA, Vol.07, No.01, hal 65-73.

[6] Dian Novianto, Tri Sugihartono. 2020. Sistem Deteksi Kualitas Buah Jambu Air Berdasarkan Warna Kulit Menggunakan Algoritma Principal Component Analysis (Pca) dan K-Nearest Neigbor (K-NN). JURNAL ILMIAH INFORMATIKA GLOBAL VOLUME 11 No. 2 Desember 2020

[7] R. Rizal, R. Ruuhwan, and K. A. Nugraha, "Implementasi Keamanan Jaringan Menggunakan Metode *Port blocking* dan *Port knocking* Pada Mikrotik RB-941," J. ICT Inf. Commun. Technol., vol. 19, no. 1, pp. 1–8, 2020, doi: 10.36054/jict-ikmi.v19i1.119.

[8] D. Desmira and R. Wiryadinata, "Rancang Bangun Keamanan *Port* Secure Shell (SSH) Menggunakan Metode *Port knocking*," J. Ilmu Komput. dan Sist. Inf., vol. 5, no. 1, pp. 28–33, 2022, doi: 10.55338/jikomsi.v5i1.242.

[9] J. Al Amien, "Implementasi Keamanan Jaringan Dengan Iptables Sebagai *Firewall* Menggunakan Metode *Port knocking*," J. Fasilkom, vol. 10, no. 2, pp. 159–165, 2020.

[10] M. Julkarnain and A. J. Afahar, "Implementasi *Port knocking* Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar," J. Inform. Teknol. dan Sains, vol. 3, no. 2, pp. 326–335, 2021, [Online]. Available: http://www.jurnal.uts.ac.id/index.php/JINTEKS/article/view/1016.

[11] A. Z. Mardiansyah, Y. M. Abdussyakur, and A. H. Jatmika, "OPTIMASI *PORT KNOCKING* DAN HONEYPOT MENGGUNAKAN Security)," vol. 3, no. 2, 2021.