SCIENTIST
Journal of Security, Computer, Information, Embedded, Network, and Intelligence System

P-ISSN : 3024-8701
E-ISSN : 3024-8329

(SCIENTIST) Journal of Security, Computer, Information, Embedded, Network, and Intelligence System
Vol. 1, No. 1, 2023

Implementasi Metode Port Knocking pada MikroTik RouterOS untuk Mendukung Keamanan Jaringan

Fadhlirrahman Baso*
Jurusan Teknik Informatika dan Komputer
Universitas Negeri Makassar
Makassar, Indonesia
fadhlirrahman.baso@unm.ac.id

Muhammad Ardiansyah
Jurusan Teknik Informatika dan Komputer
Universitas Negeri Makassar
Makassar, Indonesia
muhardizzz14@gmail.com

ARTICLE INFO

Received : 10 April 2023
Accepted : 19 June 2023
Published : 20 June 2023

ABSTRACT

This study aims to implement the Port Knocking security method in a local network using MikroTik RouterOS. The Port Knocking method is employed to enhance system security by closing access to specific ports in the network and only allowing access to these ports when a predefined sequence of port knocks is performed. The research encompasses several stages, including the analysis of the port data to be tested, the configuration of the MikroTik router, and the security system testing. The results of this study demonstrate the successful securing of the Winbox and WWW ports on the MikroTik server using the Port Knocking method. Users are required to execute the predetermined port knocking sequence before accessing these services. Furthermore, the Port Knocking method effectively blocks ping access to the MikroTik server for users who have not completed the authentication process. These findings indicate that the implementation of the Port Knocking method significantly enhances the local network security on the MikroTik server.

Keywords : Port Knocking; Network Security; MikroTik RouterOS; Authentication.

ABSTRAK

Penelitian ini bertujuan untuk mengimplementasikan metode keamanan *Port Knocking* pada jaringan lokal dengan menggunakan *MikroTik RouterOS*. Metode *Port Knocking* digunakan untuk meningkatkan keamanan sistem dengan menutup akses ke *port* tertentu pada jaringan dan hanya mengizinkan akses ke *port* tersebut jika urutan ketukan (*port knocks*) yang telah ditentukan dilakukan. Penelitian ini melibatkan beberapa tahap, termasuk analisis data *port* yang akan diuji, konfigurasi *router MikroTik*, dan pengujian sistem keamanan. Hasil dari penelitian ini menunjukkan bahwa metode *Port Knocking* berhasil mengamankan *port Winbox* dan www pada *server MikroTik*. Pengguna harus melakukan urutan ketukan yang telah ditentukan sebelum dapat mengakses layanan tersebut. Selain itu, metode *Port Knocking* juga berhasil memblokir akses *ping* ke *server MikroTik* bagi pengguna yang belum melewati proses autentikasi. Hasil ini menunjukkan bahwa implementasi metode *Port Knocking* dapat meningkatkan keamanan jaringan lokal pada *server MikroTik* dengan efektif.

Kata Kunci : Port Knocking; Network Security; MikroTik RouterOS; Autentikasi.

I. PENDAHULUAN

Keamanan jaringan adalah aspek yang sangat penting dalam implementasi jaringan komputer. Penelitian sebelumnya telah membahas metode keamanan jaringan yang dapat digunakan untuk meningkatkan keamanan jaringan komputer. Salah satu metode yang dikembangkan adalah Port *Knocking*. Metode ini digunakan untuk menutup akses ke *port* tertentu dan hanya mengizinkan akses jika urutan ketukan *port* yang telah ditentukan dilakukan. Mengimplementasikan metode *Port Knocking* pada *MikroTik RouterOS* dapat menjadi solusi untuk meningkatkan keamanan jaringan [1].

Metode *Port Knocking* memiliki beberapa keunggulan. Meskipun *port-port* ditutup, pengguna masih dapat mengaksesnya melalui penyadapan. Metode ini sangat efisien dalam melindungi sistem jaringan dan banyak digunakan untuk memastikan keamanan jaringan. Namun, terkadang pemblokiran *firewall* menjadi kurang fleksibel ketika perlu terhubung dengan seseorang di dalam jaringan. Oleh karena itu, mengimplementasikan metode *Port Knocking* pada *MikroTik RouterOS* dapat membantu mengatasi masalah ini dan meningkatkan keamanan jaringan [2].

Dalam penelitian yang dilakukan, metode *Port Knocking* telah diimplementasikan untuk mengamankan *Router* dari akses yang tidak sah. Metode ini dapat membantu mengamankan *MikroTik Routerboard* dalam sistem jaringan komputer [3]. Selain itu, metode *Port Knocking* juga dapat digunakan untuk melindungi *port* dari klien yang tidak diizinkan untuk melakukan akses jarak jauh [4]. Dengan menggunakan metode *Port Knocking*, administrator dapat memastikan bahwa hanya pengguna yang diotorisasi yang dapat mengakses *port-port* tertentu.

Sistem *firewall* yang lebih kompleks diperlukan untuk meningkatkan penggunaan *firewall* pada *MikroTik RouterOS*. Sangat mungkin untuk meningkatkan keamanan jaringan komputer dengan sistem *firewall* yang diperbarui. Konfigurasi *firewall* yang berbeda termasuk dalam sistem ini, termasuk pemblokiran akses ke Internet, pemblokiran akses ke jaringan lokal, dan pembatasan *bandwidth*. Selain itu, sistem *firewall* ini memiliki fungsi pemantauan dan log untuk memudahkan pengguna memantau akses jaringan [5].

Implementasi metode *Port Knocking* menawarkan beberapa keunggulan dalam hal keamanan jaringan. Dengan menutup akses ke *port-port* tertentu, menjadi lebih sulit bagi para penyerang potensial untuk mendapatkan akses tidak sah ke jaringan. Metode ini juga memberikan lapisan keamanan tambahan dengan mensyaratkan urutan ketukan *port* tertentu, sehingga sulit bagi para penyerang untuk menebak atau menghindari langkah-langkah keamanan. Selain itu, metode *Port Knocking* dapat membantu melindungi dari serangan *spoofing*, di mana para penyerang berusaha untuk menyamar sebagai pengguna atau perangkat yang sah [6].

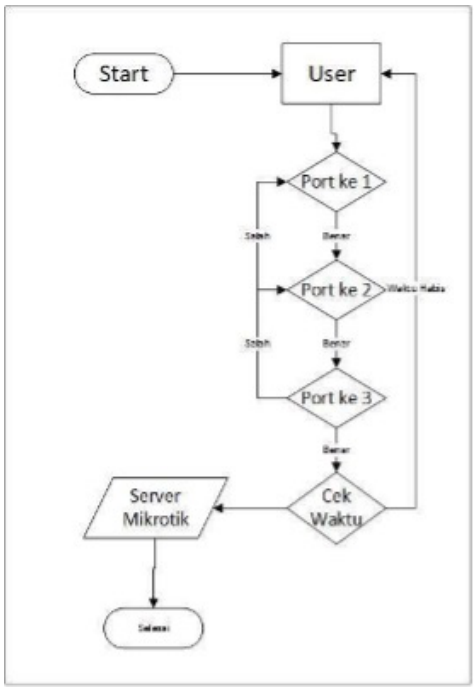
Untuk memastikan keberhasilan implementasi metode *Port Knocking*, penting untuk memiliki sistem *firewall* yang tangguh. *Firewall* berperan sebagai penghalang antara jaringan internal dan eksternal, memantau dan mengontrol lalu lintas jaringan yang masuk dan keluar [7]. Dengan mengintegrasikan metode *Port Knocking* dengan sistem *firewall*, administrator jaringan dapat meningkatkan keamanan jaringan lebih lanjut dengan mengizinkan akses terpilih ke *port-port* tertentu berdasarkan urutan ketukan *port*. Kombinasi antara metode *Port Knocking* dan teknologi *firewall* ini memberikan pendekatan komprehensif terhadap keamanan jaringan.

II. METODE PENELITIAN

Sistem keamanan rute *port* memungkinkan pengguna atau pengguna untuk terhubung ke server di jaringan lokal di mana pengguna yang terhubung telah melewati otentikasi keamanan. Adapun *framework* pada penelitian ini ditunjukkan pada Gambar 1 yang menjelaskan implementasi dan hasil pengujian pada jaringan keamanan lokal dengan menggunakan metode metode *port*. Penelitian ini bertujuan untuk menerapkan metode *port knocking* pada jaringan lokal.

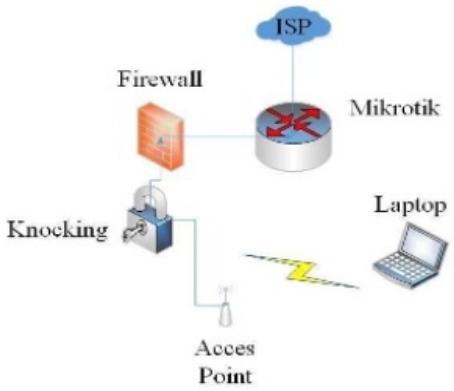
Gambar 1. Diagram Alir Penelitian

Struktur diagram blok hit *port* dapat dilihat pada diagram blok *port* pada Gambar 2. Arsitektur sistem keamanan jaringan terdiri dari beberapa komponen perangkat lunak dan perangkat keras. Tahap selanjutnya adalah merancang sistem keamanan jaringan lokal dengan menggunakan metode *port knock*. Sistem yang diusulkan dalam penelitian ini menggunakan protokol TCP untuk melakukan autentikasinya, dan menutup *state* awal dari *port* layanan pada server sehingga dapat memastikan bahwa layanan pada server tidak dapat diakses oleh siapapun yang mencoba mengakses layanan jaringan pada server terlebih dahulu harus diautentikasi, dengan tujuan *Open closed port*, sehingga dapat dilihat proses autentikasi pada *port-port* tersebut, seperti terlihat pada gambar 2.



Gambar 2. Autentikasi Port Knocking

Awalnya, server diamankan dengan mengaktifkan *firewall* pada *routerboard Mikrotik* menggunakan filter IP dengan tujuan agar alamat IP yang diketahui dapat mengakses layanan di server. Pada metode ini, pengguna (klien) terlebih dahulu harus mengimplementasikan metode *port* agar dapat mengakses layanan jaringan yang ada pada *server*, dan pada metode pemblokiran *port*, pengguna (klien) tidak dapat mengakses server meskipun paket tertentu dikirim ke alamat IP *mikrotik*. Gambar 3 menunjukkan topologi jaringan yang digunakan untuk mengimplementasikan metode *port knocking*.



Gambar 3. Topologi Jaringan *Port Knocking*

III. Hasil dan Pembahasan

Tiga tahapan utama dilakukan dalam percobaan penelitian ini, yaitu: menganalisis data *port* yang akan diuji, mengkonfigurasi *MikroTik* untuk metode penutupan dan pemblokiran *port*, dan pengujian. Tahap analisis *port* data yang akan diuji dilakukan dengan menentukan kebutuhan *port* data yang digunakan dalam implementasi sistem keamanan jaringan lokal menggunakan *MikroTik Routerboard*. Data relevan metode *port knocking* ditunjukkan pada Tabel 2. Berdasarkan hasil Tabel 2, implementasi percobaan keamanan jaringan *port knocking* pada *router MikroTik* berhasil mengamankan *port Winbox* dan www dengan autentikasi, di mana setiap autentikasi memiliki batas waktu yang ditetapkan dan ditentukan..

Tabel 1. Kebutuhan Data Port Knocking

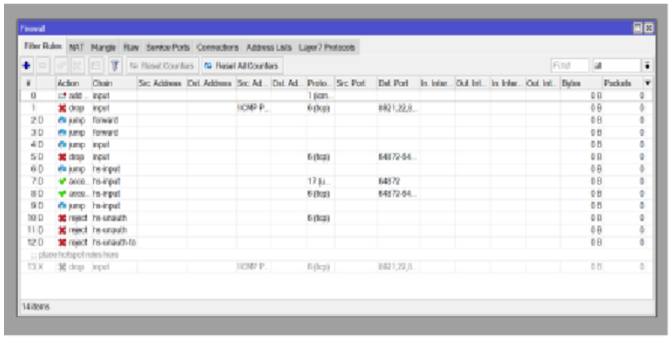
Layanan *Port*	*Port Knocking*	Kunci	Waktu
Port 8921, 22,80,23	1 2	Kunci 1 Kunci 2	10 Detik 10 Detik

Selanjutnya, konfigurasikan *Port Knocking* pada *MikroTik* untuk *first hit* dengan Port 2001. Masukkan "Chain: Input" dan atur protokol ke "TCP/IP", lalu pilih *port* 2001 sebagai *port* yang akan diamankan untuk *Winbox*. Lalu buka tab tindakan dan tambahkan tindakan "tambahkan src ke daftar alamat", lalu masukkan "hit pertama" di daftar alamat dengan batas waktu 10 detik. Selanjutnya, konfigurasikan serangan kedua dengan *port* 2002. Masukkan protokol "Chain: Input" dan "TCP/IP", lalu tentukan *port* 2002 sebagai *port* aman untuk *Winbox*. Buka tab tindakan dan tambahkan tindakan "tambahkan src ke daftar alamat", lalu masukkan "hit pertama" di daftar alamat dengan batas waktu 10 detik. Terakhir, konfigurasikan aturan

pemogokan ketiga dengan *port* 2003. Masukkan protokol "Chain: Input" dan "TCP/IP", lalu pilih *port* 2003 sebagai *port* aman untuk *Winbox*. Buka tab tindakan dan tambahkan tindakan "tambahkan src ke daftar alamat" lalu masukkan "serangan ke-2" di daftar alamat dengan batas waktu 1 jam.

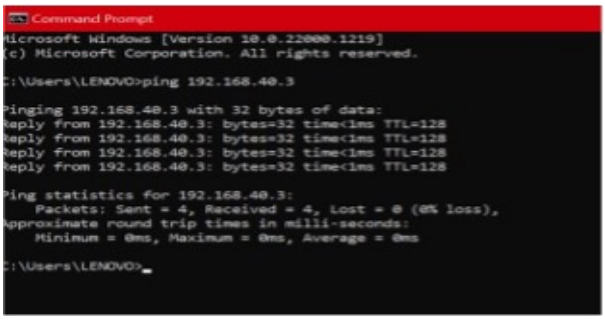
Langkah selanjutnya adalah mengkonfigurasi prosedur aturan pemilihan *port* untuk hit *MikroTik*. Pertama masukkan "Chain: Input" dan setel protokol ke "TCP/IP". Kemudian pilih port yang akan diamankan untuk *Winbox* dan www yaitu 8921, 22, 80, 23. Selanjutnya beralih ke tab *advanced* dan isi alamat src.list dengan *third strike*, dan terakhir di tab *action*, masukkan "drop". Selanjutnya, konfigurasikan tindakan aturan akses *ping* pada *port* yang rusak. Konfigurasi ini dimaksudkan untuk memblokir akses bagi pengguna yang belum menyelesaikan tahapan aturan *port knocking* yang telah ditentukan sebelumnya. Untuk membuat konfigurasi ini, masukkan "Rantai: Input" dan setel protokol ke "ICMP" di tab "Umum". Selanjutnya, di tab Lanjut, masukkan "serangan ketiga" di bagian direktori src, dan terakhir masukkan "DROP" di action.

Setelah semua konfigurasi selesai, hasil konfigurasi ditunjukkan pada Gambar 13. Semua pengaturan metode port untuk memblokir port www/80 dan *Winbox*/8291 ditunjukkan pada Gambar 4.



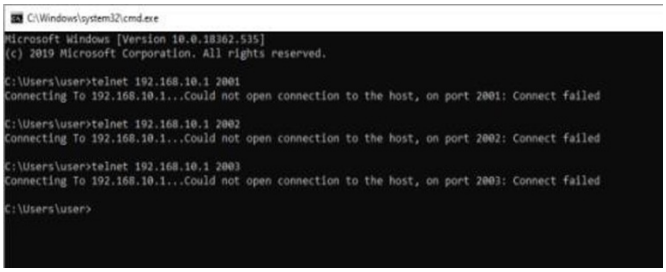
Gambar 4. Konfigurasi Port Knocking

Ada tiga aturan *knockout* dan dua tindakan *knockout*: aturan *knockout* pertama adalah *port* 2001, aturan kedua adalah 2002, dan aturan ketiga adalah 2003. Tindakan pemblokiran pertama memblokir akses ke server di *port winbox*, *port* 8291, dan www pada *port* 80. Untuk drop kedua memblokir akses *ping*, jika pengguna belum menjalankan aturan *knockout*, pengguna tidak akan dapat melakukan *ping*. Pada ara. 5 menunjukkan hasil permintaan gema sebelum aturan *knockout* diterapkan.



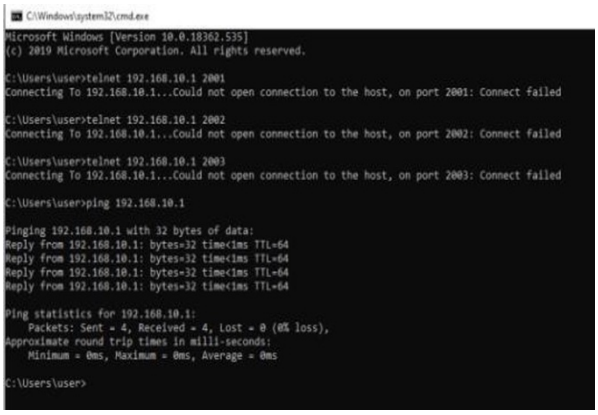
Gambar 13 Koneksi *PING* sebelum *Rule Knocking*

Pengujian *port knocking* dilakukan dengan cara *client* mengakses server dengan membuka *service winbox* pada *port* 8921,22,23 dan *service* www pada *port* 80 dimana *port winbox* dan *port* www sudah *pre-configured*, sehingga ketika user menginginkan untuk menggunakan layanan *Winbox* dan www perlu menjalankan aturan *knockout* terlebih dahulu. Kemudian jalankan *knock rule* yang dikonfigurasi untuk *port blow key* yaitu : *blow port* 1, *port* 2. Cara membuka blokir *knock rule* yang digunakan cmd dengan mengetikkan telnet diikuti dengan IP address seperti pada gambar 5.



Gambar 5. Melakukan *Rule Knocking*

Port knocking melibatkan pengiriman paket ke *port* yang telah ditentukan sebelumnya dalam urutan yang telah ditentukan. Jika urutan klik *port* cocok dengan yang ditentukan oleh aturan keamanan, *firewall* akan mendeteksi perintah dan membuka akses dengan benar ke *port* tertentu untuk pengguna atau perangkat yang mengklik. Itu kemudian melakukan percobaan untuk melakukan ping ke alamat IP *mikrotik*. Hasil *ping* yang didapat adalah status *response* yang artinya klik *port* berhasil. Hasil pengujian *ping* ditunjukkan pada Gambar 6.



Gambar 6. Ping berhasil ke *mikrotik*

Setelah semua alur penerapan konfigurasi metode *port knocking* di lakukan maka didapatkan data hasil pengujian *port knocking* dijelaskan pada Tabel 2.

Tabel 2. Hasil Pengujian *Black Box*

No	Komponen Uji	Keterangan
	Pengujian Pertama	
1	Ping ke *mikrotik*	Gagal
2	Akses *Winbox*	Gagal
3	Akses www	Gagal
	Pengujian Kedua	
1	Ping ke *mikrotik*	Berhasil
2	Akses *Winbox*	Berhasil
3	Akses www	Berhasil

Port Knocking diuji dengan memblokir secara permanen, kecuali untuk port *Winbox* dan port www. Dengan pemblokiran permanen, pengguna tidak dapat melakukan *remote* sepenuhnya ke *MikroTik* menggunakan layanan *Winbox* dan www. Namun, dengan pemblokiran terkecuali, pengguna dapat melakukan *remote* ke *MikroTik* menggunakan layanan *Winbox* dan www dengan alamat IP tertentu yang telah dikonfigurasi sebelumnya sebelum dilakukan proses *port knocking*.

IV. KESIMPULAN

Implementasi metode keamanan *Port Knocking* memungkinkan pengguna atau *user* untuk berinteraksi dengan server *MikroTik* pada jaringan lokal dengan syarat *user* telah melewati verifikasi keamanan dari *MikroTik*. Penelitian ini bertujuan untuk menerapkan metode *Port Knocking* pada jaringan lokal dengan menggunakan *MikroTik RouterOS*. Untuk mencapai tujuan tersebut, dibangun sebuah arsitektur blok diagram yang melibatkan beberapa komponen *software* dan *hardware* dalam sistem keamanan jaringan. Metode *Port Knocking* dilakukan dengan mengaktifkan *port* tertentu pada server setelah melakukan urutan ketukan yang telah ditentukan. Proses *port knocking* melibatkan pengiriman paket ke *port* yang telah ditentukan dalam urutan yang telah ditentukan juga. Namun, akses yang tidak sesuai dengan urutan ketukan akan gagal. Pengujian juga menunjukkan bahwa metode *port knocking* dapat mengamankan port *Winbox* dan www, serta dapat memblokir akses *ping* ke server *MikroTik*. Dengan demikian, hasil penelitian ini menunjukkan bahwa implementasi metode *port knocking* dapat meningkatkan keamanan jaringan lokal pada *server MikroTik*.

REFERENCES

[1] A. Amarudin, “Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking,” *J. Teknoinfo*, 2018, doi: 10.33365/jti.v12i2.121.

[2] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, “Implementasi Keamanan Jaringan Menggunakan Port Knocking,” *J. Janitra Inform. Dan Sist. Inf.*, 2022, doi: 10.25008/janitra.v2i2.156.

[3] Y. Mulyanto, M. Julkarnain, and A. J. Afahar, “Implementasi Port Knocking Untuk Keamanan Jaringan SMKN 1 Sumbawa Besar,” *J. Inform. Teknol. Dan Sains*, 2021, doi: 10.51401/jinteks.v3i2.1016.

[4] A. Harbani and M. Apriani, “Pengembangan Notifikasi Email Untuk Keamanan Port Menggunakan Metode Port Knocking,” *Teknois J. Ilm. Teknol. Inf. Dan Sains*, 2019, doi: 10.36350/jbs.v8i2.12.

[5] A. B. Pratomo, “Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros,” *Bull. Netw. Eng. Informatics*, 2023, doi: 10.59688/bufnets.v1i2.10.

[6] S. M. Bellovin, “Security Problems in the TCP/IP Protocol Suite,” *Acm Sigcomm Comput. Commun. Rev.*, 1989, doi: 10.1145/378444.378449.

[7] K. A. Scarfone and P. Hoffman, “Guidelines on Firewalls and Firewall Policy,” 2009, doi: 10.6028/nist.sp.800-41r1.