Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router

by Jurnal Komitek

Submission date: 25-Des-2021 10:29AM
(UTC+0900)**Submission ID:** 1637584426
File name: dian-novianto.doc (574.5K)
Word count: 2979
Character count: 18264

Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi
Penerbit ADM
RUMAH PENGETAHUAN

Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router

Implementasi Sistem Keamanan Jaringan Menggunakan Metode Simple Port Knocking Pada Router Berbasis Mikrotik

Dian Novianto [1)]; Lukas Tommy [2)]; Yohanes Setiawan Japriadi[2)]
[1,2)] **Teknik Informatika, ISB Atma Luhur**
Email: [1)] diannovianto@atmaluhur.ac.id; [2)] lukastommy@atmaluhur.ac.id; [2)] ysetiawanj@atmaluhur.ac.id

How to Cite :
Novianto, D., Tommy, L., Japriadi, Y. S. (2021). Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router. JURNAL Komitek, *1*(2). DOI: https://doi.org/10.53697/jkomitek.v1i2

ARTICLE HISTORY
Received [26 November 2021]
Revised [9 Desember 2021]
Accepted [24 Desember2021]

KEYWORDS
Knocking Port, PPDIOO, Mikrotik.

ABSTRAK

Salah satu permasalahan dalam remote akses terhadap sistem adalah tindakan hacking untuk mendapatkan hak akses secara ilegal terhadap sebuah sistem. Oleh karena itu perlunya sebuah mekanisme tambahan dalam autentikasi pengguna selain parameter username dan password. Metode port knocking merupakan pilihan yang dapat diimplementasikan dalam permasalahan tersebut. Port knocking adalah sistem keamanan yang berfungsi untuk membuka atau menutup akses menuju port tertentu dengan menggunakan firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi yang digunakan dapat berupa protokol TCP, UDP, maupun ICMP. Metode pengembangan sistem jaringan yang digunakan dalam penelitian ini adalah metode PPDIOO yang dikembangkan oleh CISCO, dimana urutan siklusnya antara lain: . prepare (persiapan), Plan (perencanaan), Design (Desain), Implement (Implementasi), Operate (Operasi) dan Optimize (Optimasi). Hasil dari penerapan metode Port Knocking pada sebuah sistem di jaringan komputer yaitu sistem akan menolak apabila aktivitas login pada sistem tidak atau salah mengirimkan parameter tambahan, selain itu admin jaringan dapat mengetahui aktivitas di sistem jaringan jika ada seseorang dari luar gagal saat akan mengakses sistem melalui port tertentu, sehingga dapat dilakukan tindakan sesuai dengan kebutuhan keamanan sistem.

ABSTRACT

One of the problems in remote access to the system is the act of hacking to illegally gain access rights to a system. Therefore the need for an additional mechanism in user authentication in addition to the username and password parameters. The port knocking method is an option that can be implemented in this problem. Port knocking is a security system that functions to open or close access to certain ports by using a firewall on network devices by sending certain packets or connections. The connection used can be in the form of TCP, UDP, or ICMP protocols. The network system development method used in this research is the PPDIOO method developed by CISCO, where the cycle sequence includes: . prepare (preparation), Plan (planning), Design (Design), Implement (Implementation), Operate (Operation) and Optimize (Optimization). The result of implementing the Port Knocking method on a system on a computer network is that the system will refuse if the login activity on the system does not or sends additional parameters incorrectly, besides that the network admin can find out the activity on the network system if someone from outside fails when accessing the system through the port. so that actions can be taken according to system security requirements..

PENDAHULUAN

Jaringan komputer saat ini mengalami perkembangan yang sangat pesat, saat ini teknologi jaringan sudah memasuki era generasi kelima atau 5G yang berpengaruh terhadap kecepatan internet itu sendiri, sehingga berbagai informasi dapat kita dapatkan dengan mudah, cepat, dan akurat. Dilihat dari pesatnya perkembangan teknologi jaringan kompter yang ada saat ini, salah satu hal yang harus diperhatikan oleh pengelola jaringan adalah keamanan dari jaringan itu sendiri. Karena jaringan komputer digunakan oleh hampir semua orang tanpa terkecuali, termasuk para cracker. Adanya maksud dan tujuan tertentu para cracker melakukan penyusupan melalui port-port yang terdapat pada jaringan sehingga dapat merugikan para pemilik server yang didalamnya terdapat data – data penting ataupun jaringan komputer yang didalamnya terdapat sistem pengelolaan jaringan di sebuah instansi atau organisasi. Banyak organisasi yang menggunakan jaringan komputer untuk saling bertukar informasi. Sehingga menjadi kebutuhan yang sangat penting dalam mendukung kegiatan sebuah organisasi, baik yang berupa organisasi komersial dalam hal ini perusahaan, organisasi pendidikan, lembaga milik pemerintahan, maupun individu (pribadi). Dengan demikian yang harus diperhatikan oleh para pengelola jaringan ialah meningkatkan keamanan pada jaringan supaya celah - celah yang terdapat pada jaringan tidak dapat dilihat ataupun diketahui oleh orang yang tidak bertanggung jawab seperti Cracker.

Sistem keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer. Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun logik. Yang dimaksud ancaman fisik itu adalah yang merusak bagian fisik komputer atau hardware komputer sedangkan ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun seseorang [1].

Sebagian besar para cracker melakukan serangan terhadap sistem jaringan dengan cara mengeksploit port-port yang terbuka pada sistem tersebut. Contoh serangan ini adalah dos atau ddos (Distributed Denial of Service), serangan ini dilakukan dengan membanjiri host atau komputer target dengan paket dalam jumlah besar yang berasal dari host- host berbeda. Agar serangan ini dapat berhasil maka para cracker harus mengetahui port yang terbuka dan menjadi tujuan. Adapun tahapan yang dilakukan penyerang dalam melakukan penyerangan ialah melakukan identifikasi komputer target atau tahap port scanning, dimana penyerang dapat mengambil informasi port-port yang terbuka pada mesin target. Lalu tahap OS Finger Printing, dalam tahan ini penyerang dapat mengetahui sistem operasi apa yang digunakan target. Oleh karena itu diperlukan upaya untuk meningkatkan keamanan pada jaringan supaya celah-celah yang terdapat pada jaringan tidak dapat dilihat oleh orang yang tidak bertanggung jawab seperti cracker.

Salah satu metode yang dapat digunakan untuk meningkatan keamanan sistem jaringan komputer adalah metode simple port knocking. Simple port knocking diterapkan agar sistem yang dibangun mampu mendeteksi dan menghindari serangan yang berbahaya terhadap jaringan dan langsung memberikan peringatan kepada pengelola jaringan (administrator) tentang kondisi jaringan yang sedang berjalan pada saat kejadian berlangsung, Penerapan simple port knocking menggunakan media router mikrotik yang berfungsi untuk merubah konfigurasi setting dan proteksi router sehingga tatap aman dari serangan cracker [2].

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 berupa protokol TCP, UDP, maupun ICMP. Sehingga untuk masuk dan menggunakan akses ke port tertentu yang telah dibatasi, maka user harus mengetuk terlebih dahulu dengan memasukan rule yang harus dilakukan terlebih dahulu. Rule yang mana hanya diketahui oleh pihak penyedia jaringan (administrator jaringan). Sebuah sistem harus memiliki keseimbangan antara keamanan dan fleksibilitas. Satu cara untuk mencapai sistem seperti demikian yaitu dengan menggunakan akses firewall. Dengan menggunakan firewall maka secara tidak langsung kita dapat mendefiniskan user yang dapat dipercaya dan yang tidak dapat dipercaya dengan menggunkan alaat IP sebagai kriteria filter

LANDASAN TEORI

Jaringan Komputer

Jaringan Komputer Jaringan komputer merukapan sebuah kebutuhan yang tidak dapat dielakan lagi, dan secara umum, yang disebut jaringan komputer adalah sekumpulan atau kelompok dari beberapa

komputer yang saling berhubungan satu dengan lainnya menggunakan protokol komunikasi dengan bantuan melalui media komunikasi untuk dapat saling berbagi informasi, aplikasi, dan juga perangkat keras secara bersama sama. Disamping itu jaringan komputer dapat diartikan juga sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri lebih dari satu komputer yang saling berhubungan [5].

Firewall

Firewall adalah sebuah sistem aplikasi di dalam sistem komputer yang berfungsi untuk melindungi komputer yang terkoneksi dalam jaringan komputer dari berbagai macam ancaman atau gangguan dari user yang tidak bertanggung jawab. Firewall juga dapat memblokir traffic data serta melakukan pencatatan bilamana traffic data yang masuk berisikan paket data yang mencurigakan. The Rule-set untuk firewall tersebut kemudian dikonversi menjadi sintaks khusus untuk mesin firewall yang digunakan oleh perangkat komputer [6] .

Metode Port Knocking

Port Knocking merupakan sebuah metode otorisasi user berdasarkan firewall untuk melakukan komunikasi melalui port yang tertutup. Metode port knocking menggunakan sistem authentication yang secara khusus dibuat untuk koneksi client dan server [15].

Port Knocking merupakan salah satu metode keamanan jaringan yang memungkinkan akses ke router hanya setelah menerima upaya koneksi berurutan pada satu set port tertutup yang ditentukan sebelumnya. Setelah urutan upaya koneksi yang benar diterima, RouterOS secara dinamis menambahkan IP sumber host ke daftar alamat yang diizinkan maka akan dapat menghubungkan router [7].

Mikrotik

MikroTik adalah perusahaan Latvia yang didirikan pada tahun 1996 untuk mengembangkan router dan sistem ISP nirkabel. MikroTik sekarang menyediakan perangkat keras dan perangkat lunak untuk konektivitas Internet di sebagian besar negara di dunia[8]. Mikrotik digunakan untuk menjadikan komputer ke router network sebagai fitur yang dibuat untuk IP network dan jaringan wireless.

METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah PPDIOO, adapun tahapan yang dilakukan antara lain:

***Prepare* (Persiapan)**

Pada tahap persiapan ini peneliti akan menyiapkan beberapa perlengkapan baik perangkat keras maupun perangkat lunak yang dibutuhkan dalam penerapan sistem keamanan pada jaringan dengan metode *Simple Port Knocking.* Perangkat yang dibutuhkan dapat dilihat di tabel 3.1 berikut ini:

Tabel 1 Kebutuhan Perangkat Keras

No	Perangkat Keras	Keterangan	Jumlah
1	Mikrotik RB750	Mikrotik sebagai media penghubung dan pemantau lalulintas jaringan	1
2	Kabel UTP	Penghubung	2
3	Laptop (*Server*)	OS Windows + *Winbox*	1

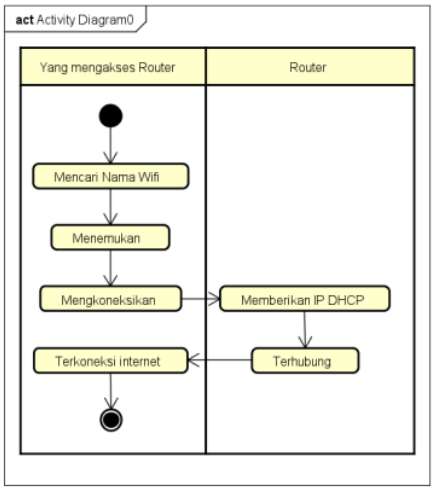
Pada bagian menjelaskan perangkat lunak yang digunakan dalam pembangunan *server Port Knocking*. Perangkat yang digunakan dapat dilihat pada tabel 3.2 berikut ini:

Tabel 2. Kebutuhan Perangkat Lunak

Software	Keterangan
Sistem Operasi Windows	Sistem operasi yang digunakan pada laptop
Winbox	Digunakan untuk konfigurasi
Putty	Digunakan untuk menguji akses
Astah	Digunakan untuk membuat Diagram
Cisco packet tracer	Digunakan untuk membuat topologi jaringan

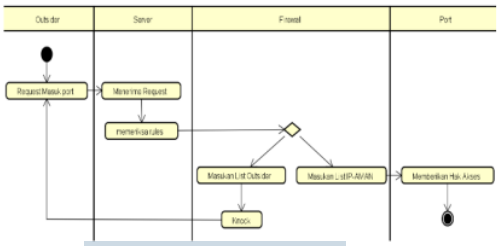
***Plan* (Perencanaan)**

Pada tahap perencanaan ini peneliti melakukan analisa sistem berjalan dan membuat sistem usulan pada jaringan yang digunakan, analisa ini berfungsi sebagai acuan dalam pembuatan desain jaringan dalam penerapan metode *Simple Port Knocking.* Berdasarkan proses bisnis yang ditemukan pada sistem berjalan, maka dibuat *activity diagram* sistem berjalan yang biasanya terjadi di sebuah instansi atau organisasi yang ditunjukkan pada gambar 3.1:



Gambar 1 *Activity Diagram* Jaringan Awal

Adapun *activity* sistem usulan untuk pemecahan masalah yang telah diuraikan pada latar belakang ditunjukkan pada gambar 2 berikut ini:



Gambar 2. *Activity diagram usulan*

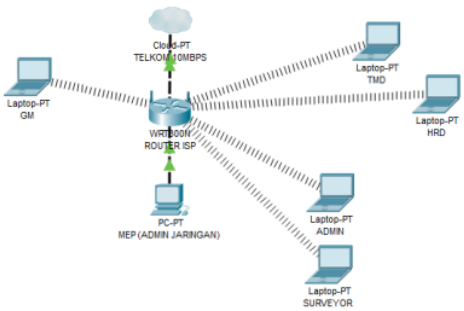
Dari gambar 2. terlihat paket data masuk lalu dicek oleh *firewall* dan *Port* untuk mendeteksi ada yang ingin mengakses *port* dan membaca *rules* lalu melakukan *Knock* sebelum membuka *port* yang ditentukan, oleh karena itu kegunaan *log* bisa mengetahui *ip outsider* dan tanggal *outsider* ingin mencoba membuka *port.*

Penerbit ADM RUMAH PENGETAHUAN
Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi

***Design* (Desain)**

Pada tahap ini dimana peneliti akan mendesain topologi alur kerja dari sistem keamanan jaringan *Simple Port Knocking* yang akan di terapkan.

Secara umum, sebuah jaringan yang berjalan pada sebuah instansi atau organisasi kecil sampai menengah kebanyakan hanya menggunakan sistem yang standar, dimana sistem jaringan yang digunakan berupa modem yang berasal dari *provider*, kemudian dihubungkan ke sebuah router sebagai pengatur lalu lintas data, adapun skema yang digunakan dalam penelitian ini, terlihat pada gambar 3.3 dibawah ini:

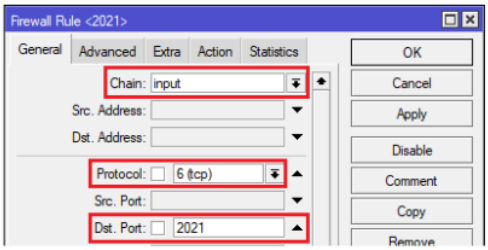


Gambar 3 Desain simulasi jaringan

Dapat dilihat pada skema jaringan diatas dalam ujicoba ini hanya menggunakan sebuah *wireless router* untuk menghubungkan akses internet dari ISP *(Internet Service Provider)* yang melayani komunikasi menggunakan media bebas yang terbuka, maka *wireless router* dapat dikatakan perangkat yang terbuka bebas. Perangkat jaringan yang tidak diverifikasi dan di kontrol dengan baik akan dapat menjadi sebuah pintu masuk bagi para *cracker* untuk melakukan tindakan ilegal yang dapat merugikan pengguna dijaringan tersebut.

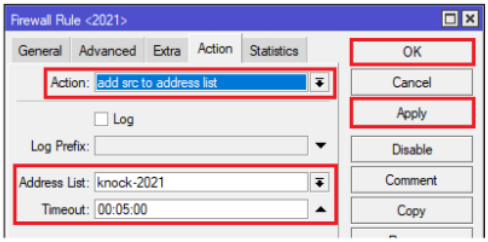
***Implement* (Implementasi)**

Pada tahap ini peneliti akan menerapkan sistem yang akan direncanakan pada tahap-tahapan sebelumnya dengan melakukan simulasi berbasis router mikrotik guna tercapainya hasil yang maksimal ketika diterapkan langsung menggunakan alat-alat yang asli pada sistem yang berjalan. Pada tahapan keempat dalam siklus PPDIOO adalah implementasi, dimana dalam tahapan ini dilakukan konfigurasi *port knocking* pada router, adapun tahapan yang dilakukan dalam konfigurasi router berbasis mikrotik dengan cara membuat beberapa rule pada *firewall*. Rule yang pertama adalah memasukan ip address yang mencoba masuk kedalam router kedalam *address list*, rule ini bertujuan jika ada koneksi dari luar ke dalam mengetuk port 2021 dengan protokol tcp maka akan dimasukan kedalam kelompok *address list "knock-2021"* selama 5 menit. Rule pertama ditunjukkan pada gambar 4.



Gambar 4. *Firewall General Rule* 1

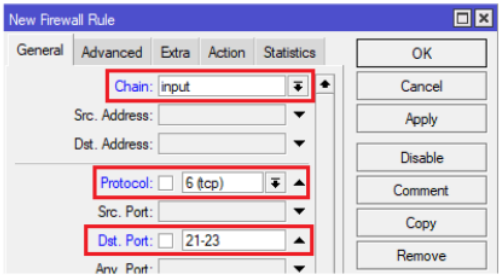
Implementasi rule pertama dengan cara mengisi c*hain firewall* dengan input yang berarti koneksi yang masuk ke dalam router, protokol yang digunakan adalah tcp, dan destination port di isi 2021.



Gambar 5. Action Rule 1

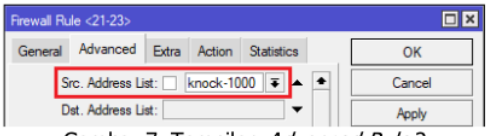
Pada tab action dipilih "add src to address lists" dengan fungsi ip yang tertangkap akan di masukan pada *address list* yang diberi nama "knock-2021" dengan *timeout* 5 menit.

Selanjutnya membuat rule kedua pada *firewall*, yang bertujuan jika ada koneksi dari luar ke dalam berada pada kelompok address list "*knock*" mengetuk port 21-23 dengan protokol tcp maka ip tersebut akan dimasukan kedalam kelompok address list "aman" selama 30 detik.



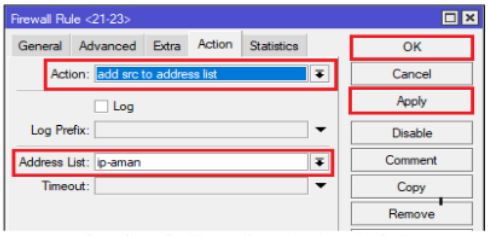
Gambar 6. *Firewall General Rule* 2

Chain diisi input karena *traffic* yang masuk ke dalam router, protokol yang digunakan adalah tcp, dan *destination port* di isi 21-23.



Gambar 7. Tampilan *Advanced Rule* 2

Pada tab *advanced* – *Src. Address List* pilih *knock-1000* adalah grup yang telah di buat pada rule pertama.

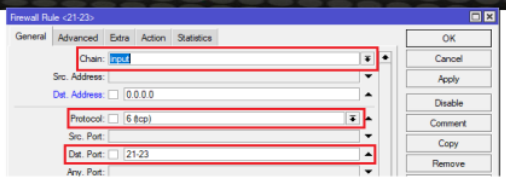


Gambar 8. Tampilan *Action Rule* 2

Pada tab action dipilih "add src to address lists" dengan fungsi akan di masukan seperti group. Pada Address list diberi nama "ip-aman".

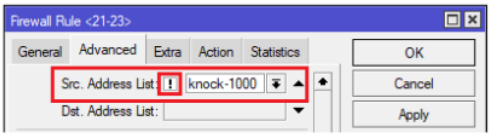
Membuat *Rule* 3 pada *firewall*, yang bertujuan jika ada koneksi dari luar kedalam yang membuka port 21-23 kecuali ada pada kelompok address list "*knock*" maka ip tersebut akan dimasukan kedalam kelompok address list "penyusup" selama 3 menit.

Penerbit ADM
RUMAH PENGETAHUAN
Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi



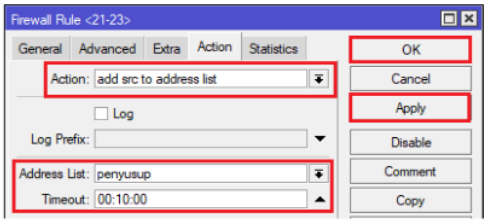
Gambar 9. *Firewall General Rule* 3

Chain di isi *input* karena trafik yang masuk ke dalam router, protokol yang digunakan adalah tcp, dan *destination port* di isi 21-23.



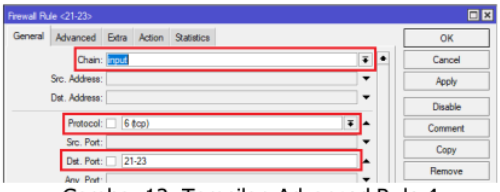
Gambar 10. Advanced Rule 3

Pada tab *advanced* – *Src. Address List* pilih knock-1000, dan klik kotak sampai bertanda seru yang arti nya logika *not* karena yang akan ditangkap adalah trafik data dari selain IP yang sudah terdaftar.



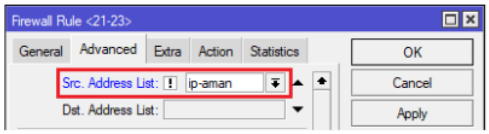
Gambar 11. Tampilan Action Rule 3

Membuat Rule keempat pada *firewall*, yang bertujuan jika ada koneksi dari luar ke dalam yang membuka port 21-23 kecuali atau yang bukan ada pada kelompok *address list* "ip-aman" maka ip tersebuat akan di blok atau tidak di izinkan mengakses.



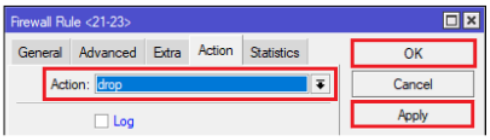
Gambar 12. Tampilan Advanced Rule 4

Chain di isi input karena trafic yang masuk ke dalam router, protokol yang digunakan adalah tcp, dan destination port di isi 21-23.



Gambar 13. Tampilan Advanced Rule 4

Pada tab advanced – Src. Address List pilih "ip-aman", dan klik kotak sampai bertanda seru yang arti nya logika *not* karena yang akan ditangkap adalah traffic data dari selain IP yang sudah terdaftar.



Gambar 14. Tampilan Action Rule 4

Pada tab action pilih "drop" dengan fungsi memblock.

***Operate* (Operasi)**

Pada tahap ini peneliti akan melakukan operasi pada sistem yang telah dirancang pada tahap *Implement* (menerapkan) dimana pada tahap ini peneliti akan memantau jaringan yang telah diterapkan mulai dari kinerja jaringan, konfigurasi dan stabilitas jaringan.

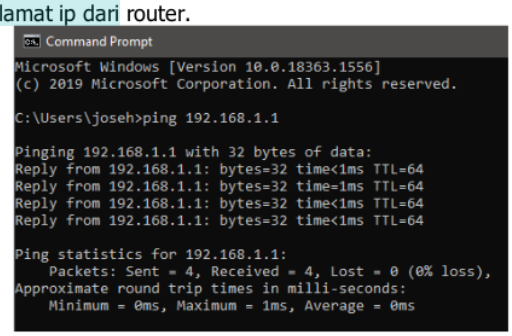
***Optimize* (Optimasi)**

Pada tahap ini dimana peneliti akan melakukan analisa dari hasil perolehan data dan melakukan identifikasi terhadap sistem yang sudah diterapkan apakah sistem sudah berjalan sesuai dengan apa yang di inginkan atau masih perlu perbaikan lagi untuk lebih meningkatkan keamanan jaringan yang diterapkan.

HASIL DAN PEMBAHASAN

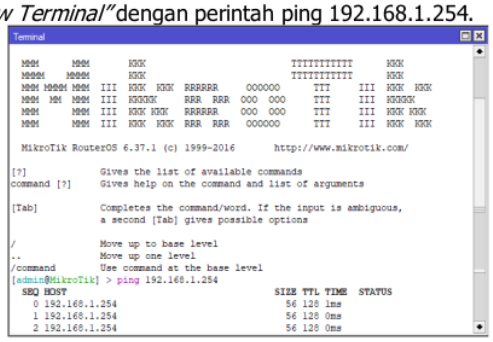
Hasil

Untuk mengetahui hasil dari konfigurasi yang telah dibuat perlu dilakukan pengujian, pengujian dilakukan dengan cara mencoba masuk kedalam router dengan dan tanpa proses *port knocking*. Langkah yang pertama untuk memastikan konektivitas antara klien dan router perlu dilakukan testing dengan melakukan ping melalui CMD *(Command Prompt)* dengan perintah "ping 192.168.1.1, dimana 192.168.1.1 merupakan alamat ip dari router.



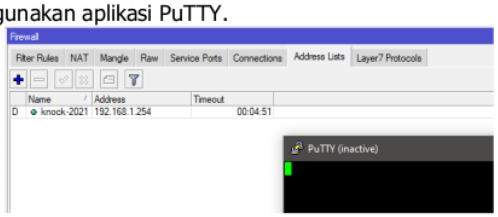
Gambar 15. Hasil Pengujian PING ke Router

Lalu cek ip yang terhubung dari *RouterBoard* ke Laptop dengan menggunakan aplikasi *Winbox*, dengan menggunakan "*New Terminal*" dengan perintah ping 192.168.1.254.



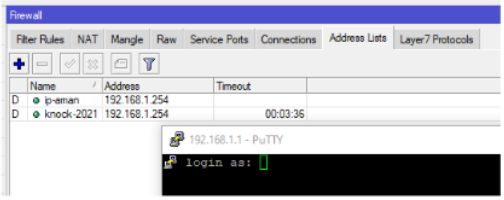
Gambar 16. Hasil Pengujian Ping Laptop

Sekarang uji coba *Rule* pertama yaitu dengan mengetuk *"port-2021"* ketujuan ip *ether1* yaitu 192.168.1.1 dengan menggunakan aplikasi PuTTY.



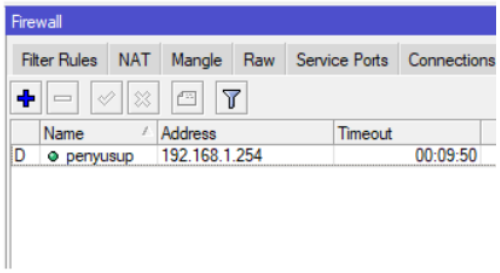
Gambar 17. Hasil Pengujian Pertama

Hasil pengujian pertama yang telah dilakukan menunjukkan ip yang melakukan port knocking berhasil masuk ke address list dengan nama *knock-2021*, yang artinya ada percobaan akses ke router dengan mengetuk *"port-2021"*.



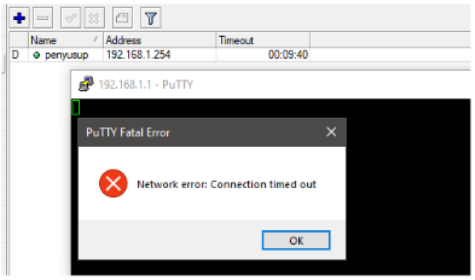
Gambar 18. Hasil Pengujian Kedua

Hasil pengujian kedua yaitu apabila setelah mengetuk *"port-2021"* dan alamat ip sudah berada didalam *address list* dengan nama "*knock-2021"* maka akan dianggap sebagai "ip-aman" dan apabila sudah tercatat sebagai ip yang melakukan *knocking*, maka alamat ip akan diizinkan mengakses router. Terlihat dari gambar 4.15 menunjukkan aplikasi putty dapat digunakan untuk masuk kedalam router, yang berarti router telah menjalankan *rule* yang telah dibuat.



Gambar 19. Hasil Pengujian Ketiga

Hasil pengujian ketiga yaitu apabila siapapun yang mencoba masuk ke port 21-23 tanpa melakukan rule pertama yaitu dengan mengetuk *"port-2021"* maka akan dimasukan ke *address lists* dengan nama "penyusup". Nama ini digunakan untuk membedakan alamat ip yang masuk kedalam address list sehingga administrator akan mengetahui alamat dari cracker yang mencoba masuk kedalam sistem secara ilegal.



Gambar 20. Hasil Pengujian keempat

Hasil pengujian keempat, yaitu mencoba masuk kedalam router tanpa pengetukan *port 2021* koneksinya akan di tolak atau di blok oleh router, hal ini dibuktikan saat ingin mengakses port 22, aplikasi PuTTY merespon dengan notifikasi *network error/connection time out.*

KESIMPULAN DAN SARAN

Kesimpulan

1. Rule *filtering* akses yang dikonfigurasi pada router berbasis mikrotik telah berjalan dengan baik, terbukti dengan mampu mengizinkan alamat ip yang terdaftar sebagai ip-aman, dan mampu memfilter alamat ip yang dianggap sebagai penyusup.
2. Dengan penerapan *Port Knocking* pada sebuah jaringan, pengelola jaringan dapat mengetahui jika ada seseorang dari luar ingin mencoba mengakses *port* yang bisa dilihat dari *address-list*.

Saran

1. Perlu dilakukan penerapan pada port yang lain sehingga tidak perlu terlalu banyak port yang terbuka untuk jalan masuknya serangan hacking.
2. Perlu penyesuaian waktu untuk pencatatan alamat ip didalam ip address.
3. Perlu menambahkan konfigurasi keamanan lainnya agar semakin kecil celah bagi cracker untuk masuk kedalam sistem secara ilegal

DAFTAR PUSTAKA

L. Jurnal Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak Ryan Permana, D. Ramadhani, and I. Lestari, "Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak," Int. J. Nat. Sci. Eng., vol. 3, no. 1, pp. 37–43, 2019, [Online]. Available: https://ejournal.undiksha.ac.id/index.php/IJNSE.

Amarudin, "Mikrotik Router Os Menggunakan Metode Port," 2018.

A, Saputro, N. Saputro, H. Wijayanto, and P. S. Informatika, "Metode Demilitarized Zone Dan Port Knocking Untuk Demilitarized Zone and Port Knocking Methods for Computer," vol. 3, no. 2, pp. 22–27, 2020.

Dian Novianto, Ellya Helmud. Implementasi Failover dengan Metode Recursive Gateway Berbasis Router Mikrotik Pada STMIK Atma Luhur Pangkalpinang. JURNAL ILMIAH INFORMATIKA GLOBAL VOLUME 10 No. 1 Juli 2019

Sugiyono, "Sistem keamanan jaringan komputer menggunakan metode watchguard firebox pada pt guna karya indonesia," J. CKI, vol. 9, no. 1, pp. 1–8, 2016.

S. Khadafi, S. Nurmuslimah, and F. K. Anggakusuma, "Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server," Nero, vol. 4, no. 3, pp. 181–188, 2019.

Mikrotik, "Port Knocking," wiki, 2015. https://wiki.mikrotik.com/wiki/Port_Knocking.

https://mikrotik.com/aboutus

Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router

ORIGINALITY REPORT

22%	22%	6%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	4%
2	nero.trunojoyo.ac.id Internet Source	2%
3	nandiantechno.wordpress.com Internet Source	2%
4	zucinetwork.wordpress.com Internet Source	2%
5	jurnal.uts.ac.id Internet Source	1%
6	inponow.blogspot.com Internet Source	1%
7	Submitted to Universitas Brawijaya Student Paper	1%
8	Submitted to SDM Universitas Gadjah Mada Student Paper	1%
9	Submitted to Konsorsium Turnitin Relawan Jurnal Indonesia	1%

	Student Paper	
10	at-siregar.blogspot.com Internet Source	1 %
11	Submitted to Sriwijaya University Student Paper	1 %
12	download.garuda.kemdikbud.go.id Internet Source	<1 %
13	ojs.unikom.ac.id Internet Source	<1 %
14	Submitted to Universitas Negeri Makassar Student Paper	<1 %
15	adoc.pub Internet Source	<1 %
16	pt.scribd.com Internet Source	<1 %
17	search.unikom.ac.id Internet Source	<1 %
18	repositori.usu.ac.id Internet Source	<1 %
19	ejournal.widyamataram.ac.id Internet Source	<1 %
20	ejurnal.itenas.ac.id Internet Source	<1 %
21	eprints.iain-surakarta.ac.id	

	Internet Source	<1%
22	drblattner.deliriumcg.com Internet Source	<1%
23	eprints.undip.ac.id Internet Source	<1%
24	jurnalmahasiswa.unesa.ac.id Internet Source	<1%
25	mum.mikrotik.com Internet Source	<1%
26	penerbitadm.com Internet Source	<1%
27	repository.atmaluhur.ac.id Internet Source	<1%
28	repository.uncp.ac.id Internet Source	<1%
29	techin.id Internet Source	<1%
30	www.slideshare.net Internet Source	<1%

Exclude quotes	On	Exclude matches	< 1 words
Exclude bibliography	On		

Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10