ANALISA DAN PENERAPAN KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN METODE DETEKSI *PORT SCANNING* BERBASIS*FIREWALL*

Ady Aryantho[1], Rr Yuliana Rachmawati Kusumaningsih[2], Joko Triyono[3]
Jurusan Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email: Aryanthodaniel@gmail.com[1], yuliana@akprind.ac.id[2], jack@akprind.ac.id[3]

Abstract

Analysis and Application of Mikrotik Network Security Using a Firewall-Based Port Scanning Detection Method is a method used for mikrotik network security in a small scope generally found in a LAN-based internet network (Local Area Network). Due to the rapid development of technology today, technology plays an important role in everyday life. Along with the development of information technology today which is always changing, making the security of an information very important. Likewise with data communication, ranging from connections between two computers to computer networks.In general, attacks that are usually carried out related to computer networks based on mikrotik are trying to gain access to mikrotik directly and also to find out information about network data used through open ports. Which actually has the main goal to be able to manipulate the network data used and control the network. Therefore, the purpose of this research is to provide security on the mikrotik network and the ports connected to the mikrotik itself. You do this by securing access to the proxy using the Port Knocking method, this security method has a function to provide access to network administrators or users by following the steps or rules that have been made. These rules will be the key to gain access to the proxy, so that only users or administrators who know the pattern of the lock can enter and access the proxy. Meanwhile, to secure the ports contained in the proxy, the Port Scanning security method is used.The function of Port Scanning itself is to secure and disguise the ports contained in the proxy, so that when scanning is carried out from irresponsible users, the task of this security method will be to disguise these ports so that they are not detected by attackers. The research method is carried out by implementing and testing to get results and find out the functions and uses of each of these network security methods. The results given will be in the form of experimental data when an attack is carried out or a trial attack from each of these security methods. In the end, the use of these two security methods is expected to be able to assist network administrators in securing mikrotik-based computer networks in a small area or Local Area Network.

Keywords: *Mikrotik, Firewall, Port Knocking, Port Scanning, Local Area Network*

Abstrak

Analisa Dan Penerapan Keamanan Jaringan *Mikrotik* Menggunakan Metode Deteksi *Port Scanning* Berbasis *Firewall* adalah metode yang digunakan untuk keamanan jaringan *mikrotik* dalam lingkup kecil umumnya terdapat dalam jaringan internet berbasis LAN (*Local Area Network*). Karena pesatnya perkembangan teknologi saat ini membuat teknologi sangat berperan penting dalam kehidupan sehari-hari. seiring dengan perkembangan teknologi Informasi saat ini yang selalu berubah, menjadikan keamanan suatu informasi sangatlah penting. Begitu juga dengan komunikasi data, mulai dari koneksi antar dua komputer hingga jaringan computer. Pada umumnya serangan yang biasa dilakukan yang berhubungan dengan jaringan komputer berbasis pada *mikrotik* yaitu mencoba untuk mendapatkan akses kedalam *mikrotik* secara langsung dan juga untuk mengetahui informasi tentang data jaringan yang digunakan melalui port-port yang terbuka. Yang sebenarnya memiliki tujuan utama untuk dapat memanipulasi data jaringan yang digunakan serta

menguasai jaringan tersebut. Oleh sebab itu tujuan dari penelitian ini adalah untuk memberikan keamanan pada jaringan *mikrotik* dan port-port yang terhubung dengan *mikrotik* itu sendiri. Caranya dengan melakukan pengamanan akses ke dalam *mikrotik* dengan menggunakan metode *Port Knocking*, metode keamanan ini memiliki fungsi untuk memberikan akses ke administrator jaringan atau user dengan mengikut langkah-langkah atau aturan yang telah dibuat. Aturan-aturan tersebut yang nantinya merupakan kunci untuk mendapatkan akses kedalam *mikrotik*, sehingga hanya user atau administrator yang mengetahui pola kunci tersebut yang dapat masuk dan mengakses *mikrotik*. Sedangkan untuk mengamankan port-port yang terdapat dalam *mikrotik*, maka digunakan metode keamanan *Port Scanning*. Fungsi dari *Port Scanning* sendiri yaitu untuk mengamankan dan menyamarkan port-port yang terdapat dalam *mikrotik*, sehingga saat dilakukan scanning dari user yang tidak bertanggung jawab, maka tugas dari metode keamanan ini akan menyamarkan port-port tersebut agar tidak terdeteksi oleh penyerang. Metode penelitian yang dilakukan yaitu dengan melakukan *Implementasi* serta pengujian untuk mendapatkan hasil dan mengetahui fungsi beserta kegunaan dari masing-masing metode keamanan jaringan tersebut. Hasil yang diberikan nantinya berupa data hasil percobaan saat dilakukan serangan atau uji coba serangan dari masing-masing metode keamanan tersebut. Pada akhirnya penggunaan kedua metode keamanan ini diharapkan mampu membantu adminstrator jaringan dalam mengamankan jaringan komputer berbasis *mikrotik* dalam lingkup area yang kecil atau *Local Area Network*.

Kata kunci: *Mikrotik*, *Firewall*, *Port Knocking*, *Port Scanning*, *Local Area Network*.

Pendahuluan

Dengan pesatnya perkembangan teknologi saat ini membuat teknologi sangat berperan penting dalam kehidupan sehari-hari. seiring dengan perkembangan teknologi Informasi saat ini yang selalu berubah, menjadikan keamanan suatu informasi sangatlah penting. Begitu juga dengan komunikasi data, mulai dari koneksi antar dua komputer hingga jaringan komputer. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan komputer mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian secara bersama baik penggunaan data, perangkat lunak dan peralatan. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien. Tentunya dalam pembangunan jaringan komputer kualitas akan keamanan jaringan merupakan hal yang paling utama. Segala bentuk ancaman yang datang baik langsung maupun tidak langsung akan mengganggu kegiatan yang sedang berlangsung dalam jaringan komputer. Banyak serangan sering dilakukan pada suatu port–port yang dalam keadaan terbuka, sehingga nantinya akan membuat orang–orang yang tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengendalikan port–port yang telah ia masuki. Maka untuk melakukan keamanan pada jaringan komputer dalam mengatasi serangan dapat dilakukan dengan beberapa cara yaitu menggunakan keamanan yang berbasis pada *Firewall*, dan menggunakan metode *Port Scan Detection*. Dari kedua keamanan tersebut memiliki fungsi dan cara kerja yang dapat digunakan untuk mengamankan suatu jaringan internet berbasis mikrotik. *Port Scanner* merupakan aplikasi yang digunakan untuk melihat informasi atau status dari protokol dan port yang terbuka (open) dari sebuah perangkat. Dengan aplikasi ini bisa jadi merupakan sebuah awal dari dimulainya serangan terhadap sebuah resource di jaringan.

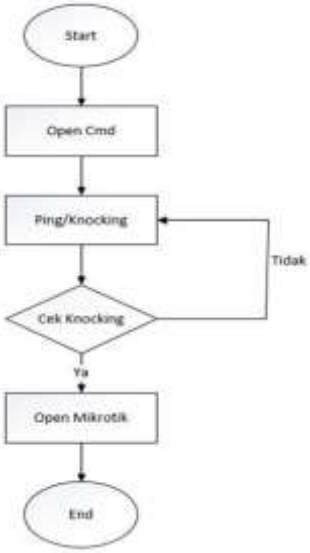
Ketika informasi protokol atau port sudah didapat maka *Hacker* atau penyerang bisa memanfaatkan untuk melakukan eksploitasi dari protokol atau port tersebut. Misal, salah satu contoh untuk serangan *Distributed Denial of Service (DDoS).* Banyak aplikasi yang bisa digunakan untuk melakukan port scanner yang umumnya seperti *Nmap*, *Netcut*, dan *Unicornscan.* Berbeda dengan cara kerja dari *Firewall*, cara kerja dari *Firewall* adalah menutup semua port tanpa memperdulikan apapun meskipun user tersebut memiliki hak untuk mengakses port tersebut. Sehingga user yang memiliki hak akses tersebut juga tidak bisa untuk mengaksesnya. Tetapi selain dari cara kerja tersebut, *Firewall* memiliki kelebihan lain dari keamanan yang disediakan yaitu terletak pada metode *Port Knocking,* yang dimana meskipun semua port yang ada telah ditutup, tetapi user yang memiliki hak akses dan mengetahui Knocking untuk membuka suatu port maka user tersebut tetap dapat menggunakan port yang telah dibuka sebelumnya. Dalam penelitian ini,

akan dijabarkan mengenai sistem keamanan jaringan komputer yang berbasis pada metode yang terdapat dalam *Firewall* dan metode *Port Scan Detection* untuk mengurangi serangan pada jaringan komputer lokal.

Metodologi Penelitian

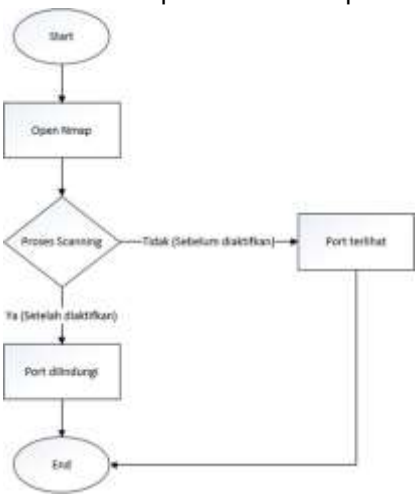
Metode pengumpulan data yang digunakan dalam pengembangan jaringan menggunakan mikrotik OS adalah metode observasi, metode studi pustaka, dan metode eksperimen. Metode analisa data yang digunakan dalam penelitian ini adalah dengan melakukan analisa dan perbandingan dalam melakukan penerapan atau implementasi dari metode keamanan *Port Knocking* dan *Port Scan Detection*, yang dimana metode *Port Knocking* memiliki fungsi untuk melindungi akses ke dalam mikrotik dengan menerapkan aturan- aturan berupa ketukan pada port kunci yang telah ditentukan, sedangkan untuk *Port Scan Detection* mempunyai fungsi untuk melindungi port-port yang aktif dalam mikrotik dari serangan-serangan dari pihak yang tidak bertanggung jawab. Sebenarnya, kedua keamanan ini memiliki keterkaitan satu sama lain. Oleh sebab itu, hasil dari penerapan kedua keamanan ini akan dianalisa dan nantinya hasil dari penelitian ini akan dilihat bagaimana fungsi dan kelebihan dari setiap keamanan jaringan yang digunakan

Diagram alir proses kncoking dalam penelitian ini dapat dilihat pada Gambar 1



Gambar 1 Flow Chart Proses Knocking

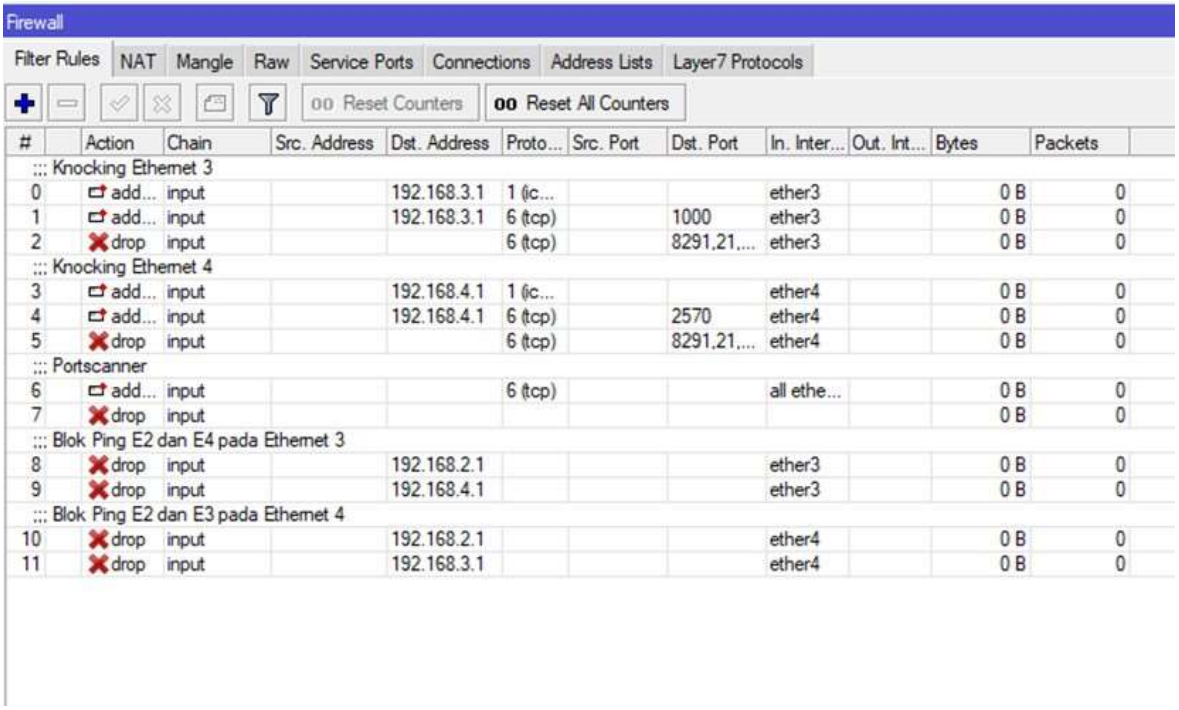
Diagram alir port scanner dalam penelitian ini dapat dilihat pada Gambar 2



Gambar 2 Port Scan Detection

Hasil dan Pembahasan

Pada Gambar 3 merupakan tampilan keseluruhan dari keamanan jaringan mikrotik yang dibuat pada Firewall Rule. Pada tampilan ini meliputi penerapan Port Knocking pada Ethernet 3 dan Ethernet 4, tampilan Port Scan Detection dan tampilan Rule Blokir Ip dalammetode Firewall Rule



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Knocking Ethernet 3											
0	add...	input		192.168.3.1	1 (ic...			ether3		0 B	0
1	add...	input		192.168.3.1	6 (tcp)		1000	ether3		0 B	0
2	drop	input			6 (tcp)		8291,21,...	ether3		0 B	0
;;; Knocking Ethernet 4											
3	add...	input		192.168.4.1	1 (ic...			ether4		0 B	0
4	add...	input		192.168.4.1	6 (tcp)		2570	ether4		0 B	0
5	drop	input			6 (tcp)		8291,21,...	ether4		0 B	0
;;; Portscanner											
6	add...	input			6 (tcp)			all ethe...		0 B	0
7	drop	input								0 B	0
;;; Blok Ping E2 dan E4 pada Ethernet 3											
8	drop	input		192.168.2.1				ether3		0 B	0
9	drop	input		192.168.4.1				ether3		0 B	0
;;; Blok Ping E2 dan E3 pada Ethernet 4											
10	drop	input		192.168.2.1				ether4		0 B	0
11	drop	input		192.168.3.1				ether4		0 B	0

Gambar 3 Tampilan Sistem Keamanan di Firewall Rule

Dari Gambar 3 merupakan tampilan keseluruhan dari rules keamanan yang diterapkan dalam penelitian ini, terlihat dalam Filter Rules terdapat rule Portknocking dari Ethernet 3 dan Ethernet 4. Dalam penelitian ini rule Portknocking hanya diterapkan pada Ethernet 3 dan Ethernet 4, karena hanya pada kedua Ethernet tersebutlah yang nantinya akan digunakan sebagai jaringan publik. Kemudian terdapat juga rule Portscanner dan rule pembatalan Ping yang akan diterapkan juga pada Ethernet 3 dan Ethernet 4 di dalam penelitian ini.

Tabel Rangkuman Dan Analisis Perbandingan Hasil Penelitian

Berikut ini merupakan tabel rangkuman dan analisis perbandingan yang dilakukan dalam penelitian ini. Pada tabel-tabel ini merupakan hasi dari percobaan yang dilakukan berkali- kali dalam waktu tertentu sehingg dapat diketahui perbandingan dari setiap percobaan dan hasil yang dapat diberikan serta dijelaskan seperti pada tabel-tabel berikut.

Portkncking

Ethernet 3

Tabel 1. Percobaan mengakses mikrotik beserta port-port di dalam mikrotik oleh user/administrator jaringan secara langsung sebelum melakukan rule portknocking dengan benar pada ethernet 3

Pembahasan	Keterangan	Hasil
Percobaan mengakses mikrotik secara langsungoleh user/administrator jaringan	Sebelum user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Tidak diizinkan untuk mengakses mikrotik secaralangsung dan gagal untuk masuk ke dalam mikrotik

Percobaan mengakses port 21 menggunakan aplikasi Putty oleh user/administrator jaringan secara langsung	Sebelum user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Tidak diizinkan untuk mengakses port yang ditujusecara langsung dan gagaluntuk masuk ke dalam mikrotik
Percobaan mengakses port 22 menggunakan aplikasi Putty oleh user/administrator jaringan secara langsung	Sebelum user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Tidak diizinkan untuk mengakses port yang ditujusecara langsung dan gagaluntuk masuk ke dalam mikrotik
Percobaan mengakses port 23 menggunakan aplikasi Putty oleh user/administrator jaringan secara langsung	Sebelum user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Tidak diizinkan untuk mengakses port yang ditujusecara langsung dan gagaluntuk masuk ke dalam mikrotik
Percobaan mengakses port 8291 atau alamat webfig oleh user/administrator jaringansecara langsung	Sebelum user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Tidak diizinkan untuk mengakses port yang ditujusecara langsung dan gagaluntuk masuk ke dalam mikrotik

Tabel 4 Percobaan Kembali Mengakses Mikrotik Dan Port-Port Di Dalam Mikrotik Oleh User/Adminsitrator Jaringan Secara Langsung Setelah Melakukan Rule Portknocking Dengan Benar Pada Ethernet 4

Pembahasan	Keterangan	Hasil
Percobaan kembali mengakses mikrotik secara langsung oleh user/administrator jaringan	Setelah user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Sukses dan diizinkan untuk mengakses mikrotik
Percobaan kembali mengakses port 21 menggunakan aplikasi Putty oleh user/administrator jaringan secara langsung	Setelah user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Sukses dan diizinkan untuk mengakses mikrotik serta port yang dituju yang terdapat didalam mikrotik
Percobaan kembali mengakses port 22 menggunakan aplikasi Putty oleh user/administrator jaringan secara langsung	Setelah user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Sukses dan diizinkan untuk mengakses mikrotik serta port yang dituju yang terdapat didalam mikrotik

Percobaan kembali mengakses port 23 menggunakan aplikasi Putty oleh user/administrator jaringan secara langsung	Setelah user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Sukses dan diizinkan untuk mengakses mikrotik serta port yang dituju yang terdapat didalam mikrotik
Percobaan kembali mengakses port 8291 oleh user/administrator jaringan secara langsung	Setelah user/ administrator jaringan tersebut melakukan rule knocking dengan benar yaitu dengan melakukan ping ke ip dan melakukan ketukan dengan port yang telah ditentukan	Sukses dan diizinkan untuk mengakses mikrotik serta port yang dituju yang terdapat didalam mikrotik

Port Scan Detection

Percobaan penyerangan dari Ethernet 3 ke Ethernet lain

Tabel 5. Percobaan serangan atau scanning dari ethernet 3 ke ethernet lain sebelummengaktifkan rule port scan detection pada mikrotik

Pembahasan	Keterangan	Hasil
Serangan yang dilakukan dengan cara melakukan scanning dari Ethernet 3 ke Ip Ethernet 4 untuk mengetahui data dan informasi dari Ethernet 4 menggunakan software Nmap	Sebelum mengaktifkan rule PortScan Detection di mikrotik	Dapat mengetahui informasi mengenai jaringan Ethernet 4 dan port apa saja yang aktif dan terdapat dalam Ethernet 4
Serangan yang dilakukan dengan cara melakukan scanning dari Ethernet 3 ke Ip Ethernet 2 untuk mengetahui data dan informasi dari Ethernet 2 menggunakan software Nmap	Sebelum mengaktifkan rule PortScan Detection di mikrotik	Dapat mengetahui informasi mengenai jaringan Ethernet 2 dan port apa saja yang aktif dan terdapat dalam Ethernet 2

Tabel 6. Percobaan kembali melakukan serangan atau scanning dari ethernet 3 keethernet lain setelah mengaktifkan rule port scan detection pada mikrotik

Pembahasan	Keterangan	Hasil
Serangan yang kembali dilakukan dengan cara melakukan scanning dari Ethernet 3 ke Ip Ethernet 4 untuk mengetahui data dan informasi dari Ethernet 4 menggunakan software Nmap	Setelah mengaktifkan rule PortScan Detection di mikrotik	Informasi mengenai Ethernet 4dan port yang aktif sudah tidakterlihat dan Ip penyerang sudah terblokir
Serangan yang kembali dilakukan dengan cara melakukan scanning dari Ethernet 3 ke Ip Ethernet 2 untuk mengetahui data dan informasi dari Ethernet 2 menggunakan software Nmap	Setelah mengaktifkan rule PortScan Detection di mikrotik	Informasi mengenai Ethernet 2dan port yang aktif sudah tidakterlihat dan Ip penyerang sudah terblokir

Percobaan penyerangan dari Ethernet 4 ke Ethernet lain

Tabel 7 Percobaan Serangan Atau Scanning Dari Ethernet 4 Ke Ethernet Lain Sebelum Mengaktifkan Rule Port Scan Detection Pada Mikrotik

Pembahasan	Keterangan	Hasil
Serangan yang dilakukan dengan cara melakukan scanning dari Ethernet 4 ke Ip Ethernet 3 untuk mengetahui data dan informasi dari Ethernet 3 menggunakan software Nmap	Sebelum mengaktifkan rule Port Scan Detection di mikrotik	Dapat mengetahui informasi mengenai jaringan Ethernet 3 dan port apa saja yang aktif dan terdapat dalam Ethernet 3
Serangan yang dilakukan dengan cara melakukan scanning dari Ethernet 4 ke Ip Ethernet 2 untuk mengetahui data dan informasi dari Ethernet 2 menggunakan software Nmap	Sebelum mengaktifkan rule Port Scan Detection di mikrotik	Dapat mengetahui informasi mengenai jaringan Ethernet 2 dan port apa saja yang aktif dan terdapat dalam Ethernet 2

Tabel 8 Percobaan Kembali Melakukan Serangan Atau Scanning Dari Ethernet 4 KeEthernet Lain Setelah Mengaktifkan Rule Port Scan Detection Pada Mikrotik

Pembahasan	Keterangan	Hasil
Serangan yang kembali dilakukan dengan cara melakukan scanning dari Ethernet 4 ke Ip Ethernet 3 untuk mengetahui data dan informasi dari Ethernet 3 menggunakan software Nmap	Telah mengaktifkan rule Port Scan Detection di mikrotik	Informasi mengenai Ethernet 3 dan port yang aktif sudah tidak terlihat dan Ip penyerang sudah diblokir
Serangan yang kembali dilakukan dengan cara melakukan scanning dari Ethernet 4 ke Ip Ethernet 2 untuk mengetahui data dan informasi dari Ethernet 2 menggunakan software Nmap	Telah mengaktifkan rule Port Scan Detection di mikrotik	Informasi mengenai Ethernet 2 dan port yang aktif sudah tidak terlihat dan Ip penyerang sudah diblokir

Pembatalan Ping

Percobaan Serangan Ping dari Ethernet 3 ke Ethernet lain.

Tabel 9 Percobaan Serangan Dengan Cara Ping Dari Ethernet 3 Ke Ethernet LainSebelum Mengaktifkan Rule Pembatalan Ping Pada Mikrotik

Pembahasan	Keterangan	Hasil
Ping dari Ethernet 3 ke Ip Ethernet 4	Sebelum mengaktikan rule pembatalan ping atau metode block ping	Ping masih dapat berjalan keIp tujuan
Ping dari Ethernet 3 ke Ip Ethernet 2	Sebelum mengaktikan rule pembatalan ping atau metode block ping	Ping masih dapat berjalan keIp tujuan

Tabel 10 Percobaan Kembali Melakukan Serangan Dengan Ping Dari Ethernet 3 KeEthernet Lain Setelah Mengaktifkan Rule Pembatalan Ping Pada Mikrotik

Pembahasan	Keterangan	Hasil
Serangan kembali dilakukan dengan cara Ping dari Ethernet 3 ke Ip Ethernet 4	Setelah mengaktifkan rule pembatalan ping	Ip yang dituju sudah tidak dapat terhubung dan menunjukan status RTO
Serangan kembali dilakukan dengan cara Ping dari Ethernet 3 ke Ip Ethernet 2	Setelah mengaktifkan rule pembatalan ping	Ip yang dituju sudah tidak dapat terhubung dan menunjukan status RTO

Percobaan Serangan Ping dari Ethernet 4 ke Ethernet lain

Tabel 11 Percobaan Serangan Dengan Cara Ping Dari Ethernet 4 Ke Ethernet LainSebelum Mengaktifkan Rule Pembatalan Ping Pada Mikrotik

Pembahasan	Keterangan	Hasil
Ping dari Ethernet 4 ke Ip Ethernet 3	Sebelum mengaktikan rule pembatalan ping atau metode block ping	Ping masih dapat berjalan ke Ip tujuan
Ping dari Ethernet 4 ke Ip Ethernet 2	Sebelum mengaktikan rule pembatalan ping atau metode block ping	Ping masih dapat berjalan ke Ip tujuan

Tabel 12 Percobaan Kembali Melakukan Serangan Dengan Ping Dari Ethernet 4 KeEthernet Lain Setelah Mengaktifkan Rule Pembatalan Ping Pada Mikrotik

Pembahasan	Keterangan	Hasil
Serangan kembali dilakukan dengan cara Ping dari Ethernet 4 ke Ip Ethernet 3	Setelah mengaktifkan rule pembatalan ping	Ip yang dituju sudah tidak dapat terhubung dan menunjukan status RTO
Serangan kembali dilakukan dengan cara Ping dari Ethernet 4 ke Ip Ethernet 2	Setelah mengaktifkan rule pembatalan ping	Ip yang dituju sudah tidak dapat terhubung dan menunjukan status RTO

Kesimpulan

Dari hasil penilitian Analisa Dan Penerapan Keamanan Jaringan Mikrotik Menggunakan Metode Deteksi *Port Scanning* Berbasis *Firewall*, dapat disimpulkan sebagai berikut:

1. Dengan menerapkan keamanan jaringan mikrotik menggunakan metode keamanan *Port Knocking* dan metode keamanan *Port Scan Detection*, maka dari hasil penerapan penelitian ini berhasil dilakukan pengamanan dari percobaan akses kedalam mikrotik dengan menerapkan aturan-aturan dari metode keamanan *Port Knocking*. Sehingga, user atau adminitrator jaringan yang mencoba untuk mengakses ke dalam mikrotik harus melewati aturan-aturan atau tahapan keamanan sebelum diberikan izin masuk dan mengakses mikrotik. Dan untuk keamanan port-port yang terbuka berhasil diamankan dengan cara disamarkan agar tidak terlihat disaat ada user yang tidak bertanggung jawab yang mencoba mengakses atau menyerang jaringan mikrotik dengan cara melakukan scanning dan menggunakan port-port yang terbuka sebagai alat untuk menyerang dan mengetahui jaringan internet tersebut.
2. Hasil pengujian akses kedalam mikrotik menggunakan aturan-aturan keamanan *Port Knocking* terlihat bahwa user yang mengetahui langkah-langkah beserta kunci dalam aturan yang telah dibuat dari masing-masing Ethernet, yaitu Ethernet 3 dan Ethernet

4 yang mengarah ke jaringan publik yang bisa masuk dan mengakses mikrotik. Sedangkan untuk user yang mencoba mengetahui informasi jaringan internet dari salah satu jaringan publik yang ada dengan cara melakukan scanning, maka saat metode keamanan *Port Scan Detection* diaktifkan maka Ip penyerang atau Ip user tersebut akan langsung terbaca sebagai Ip yang melakukan scanning, kemudian oleh aturan keamanan yang dibuat, Ip tersebut akan langsung di drop atau diblokir dalam jangka waktu yang telah ditentukan.

3. Setelah melakukan percobaan untuk mendapatkan akses kedalam mikrotik, user atau administrator harus melakukan Ping ke Ip dari Ethernet yang terhubung. Kemudian, untuk mendapatkan akses tidak bisa sebatas melakukan Ping ke Ip Ethernet yang dituju saja, tetapi harus melakukan Ping ke Port kunci atau aturan ke dua yang telah dibuat. Untuk Port kunci telah ditetapkan untuk masing-masing Ethernet yang mengarah ke jaringan publik, yaitu untuk Ethernet 3 dengan Port kunci 1000, sedangkan Ethernet 4 dengan Port Kunci 2570. Kemudian saat aturan tersebut berhasil dijalankan, maka akan terlihat pada *Addres List* bahwa Ip yang melakukan knocking sudah tercatat dan dinyatakan aman. Untuk percobaan scanning, saat metode keamanan *Port Scan Detection* belum diaktifkan, Ip penyerang akan melakukan scanning dengan menggunakan aplikasi Nmap, disini Ip terget akan discanning dan akan terbaca port apa saja yang aktif dan terbuka. Kemudian saat metode keamanan *Port Scan Detection* diaktifkan maka saat Ip penyerang melakukan scanning kembali, akan terlihat bahwa port-port yang aktif tadi sudah disamarkan atau tidak terbaca lagi. Dan pada *Addres List* dalam *Firewall* mikrotik, Ip dari penyerang akan di blokir dan akan terbaca sebagai user yang melakukan scanning.
4. Dari hasil penelitian ini juga dapat disimpulkan bahwa penggunaan metode *Port Knocking* dan *Port Scan Detection* saling terhubung satu sama lain. Saat metode Port Knocking mengamankan dari segi akses kedalam mikrotik dengan memblokir beberapa port yang terhubung kedalam mikrotik saat user atau administrator jaringan belum memiliki hak akses ke dalam jaringan mikrotik, dari sisi yang lain metode Port Scan Detection melindungi port-port tersebut agar tidak terdeteksi oleh user atau penyerang yang ingin mengetahui informasi dari jaringan yang digunakan saat user tersebut belum mendapatkan akses kedalam mikrotik. Kelebihan dari kedua sistem keamanan ini adalah memeberikan keamanan yang berlapis sehingga jaringan mikrotik bisa lebih aman saat terhubung ke jaringan publik.

Daftar Pustaka

[1] H. Orlando *et al.*, “Edukasi Pentingnya Keamanan Komputer Kepada Siswa SMK Dua Mei,” vol. 3, pp. 90–92, 2022.

[2] R. 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, p. 37, 2019, doi: 10.23887/ijnse.v3i1.22175.

[3] Z. Munawar and N. I. Putri, “Keamanan Jaringan Komputer Pada Era Big Data,” *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 1–7, 2020.

[4] M. I. Irawan, U. Y. K. s. Hediyanto, and R. R. Saedudin, “Implementasi Keamanan Jaringan Pada Cloudfri Dengan Metode Hardening,” vol. 9, no. 2, pp. 644–649, 2022.

[5] B. P. Firdaus and I. M. Suartana, “Implementasi Keamanan Jaringan Intrusion Detection/Prevention System Menggunakan Pfsense,” *J. Manaj. Inf.*, vol. 4, no. 1, pp. 1–9, 2021.

[6] F. Panjaitan, A. Aprilo, U. B. Darma, J. Jenderal, A. Yani, and N. Palembang, “Analisis manajemen risiko keamanan jaringan menggunakan framework nist,” vol. 24, no. 1, pp. 71–81, 2022

[7] Y. Kuspandi Putra, M. Sadali, and M. Mahpuz, “Penerapan Mikrotik Dalam Mengembangkan Infrastruktur Jaringan Pada Kantor Desa Rumbuk Kecamatan Sakra,” *Infotek J. Inform. dan Teknol.*, vol. 3, no. 2, pp. 182–193, 2020, doi: 10.29408/jit.v3i2.2350.

[8] E. S. R. O. B. Langobelen, Y. Rachmawati, and C. Iswahyudi, “Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta,” *J. JARKOM*, vol. 7, no. 2, pp. 95–102, 2019.

[9] N. Akbar, “Pengenalan Winbox Dan Fungsinya Dan Cara Penggunaannya,” 2019. [Online]. Available: biloketam88.wordpress.com/pengenalan-winbox-dan- fungsinya-dan-cara-penggunaannya/

[10] D. B. Rendro, Ngatono, and W. N. Aji, “Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang),”

PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput., vol. 7, no. 2,pp. 108–115, 2020.

[11] Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router Os," *J. Teknoinfo*, vol. 12,no.2,pp.72–75,2018,[Online].Available: http://ejurnal.teknokrat.ac.id/index.php/teknoinfo/article/view/121/91

[12] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, pp. 115–123, 2020, doi: 10.37034/jsisfotek.v2i4.32.