Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode Port Knocking

Paradika Dwi Oktaviansyah

Sistem Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya, Palembang, Indonesia

Penulis Korespondensi: Paradika Dwi Oktaviansyah (paradikadwio@gmail.com)

Diterima	:	01 Juni 2022	UR	RL :	https://jurnal.netplg.com/index.php/jnca/article/view/10
Disetujui	:	01 Juli 2022	ISS	SN :	2964-6669
Diterbitkan	:	20 Juli 2022			

ABSTRAK

Poin terpenting dalam layanan jaringan adalah keamanan akses di perangkat yang dituju. Namun masalah yang terjadi adalah port atau akses yang terbuka tidak dapat diakses dengan otentikasi yang dapat memfasilitasi pengguna yang tidak sah untuk diakses oleh server. Hal ini merupakan dasar untuk meningkatkan hak akses ke server yang dibangun tanpa harus menutup port yang digunakan. Port knocking adalah sistem keamanan yang dapat melakukan fungsi yang memblokir akses yang tidak diinginkan. Pada prinsipnya, port knocking berhasil menutup semua port di server. Jika pengguna membutuhkan akses ke server, pengguna melakukan: "ketukan" untuk menggunakan layanan tersebut, maka jika pengguna telah selesai mengakses port ditutup kembali. Itu Sistem yang dibangun pada penelitian ini menggunakan tiga buah port yaitu port 22 (SSH), port 23 (Telnet), port 80 (Webfig) dan port 8291 (Winbox). Waktu Akses Port masing-masing adalah 5 menit. Berdasarkan hasil analisis dan pengujian implementasi sistem yang dibangun dibangun dibandingkan dengan jaringan yang tidak menggunakan keamanan Port Knocking.

Kata Kunci : Network Security, Port Knocking, Mikrotik, Winbox, Port

ABSTRACT

The most important point in network services is the security of access on the intended device. But the problem that occurs is that the port or access that is open cannot be accessed by authentication which can facilitate unauthorized users to be accessed by the server. This is the basis for increasing access rights to the server that is built without having to close the port that is used. Port knocking is a security system that can perform a function that blocks unwanted access. In principle, port knocking succeeds in closing all ports on the server. If the user needs access to the server, the user does: "tap" to use the service, then if the user has finished accessing the port is closed again. The system built in this study uses three ports, namely port 22 (SSH), port 23 (Telnet), port 80 (Webfig) and port 8291 (Winbox). Port Access Time is 5 minutes each. Based on the results of the analysis and testing of the system implementation, the results of the system can run well and can increase the security of the network system that is built compared to a network that does not use Port Knocking security.

Keywords: Network Security, Port Knocking, Mikrotik, Winbox, Port

1. PENDAHULUAN

Keamanan jaringan adalah perlindungan infrastruktur jaringan yang mendasari dari akses yang tidak sah, penyalahgunaan, atau pencurian. Ini melibatkan pembuatan infrastruktur yang aman untuk perangkat, aplikasi, pengguna, dan aplikasi untuk bekerja dengan cara yang aman. Keamanan jaringan

menggabungkan beberapa lapisan pertahanan di tepi dan di dalam jaringan. Setiap lapisan keamanan jaringan menerapkan kebijakan dan kontrol. Pengguna yang berwenang mendapatkan akses ke sumber daya jaringan, tetapi pengguna jahat akan diblokir yang ingin melakukan eksploitasi dan ancaman.

Berbagai cara dan jumlah serangan pada suatu server semakin hari semakin meningkat. Itu pembukaan beberapa port yang menyimak secara tidak langsung akan mengundang para penyerang dan pihak-pihak tertentu yang tidak bertanggung jawab untuk membobol server melalui port itu. Hal yang sering dilakukan oleh penyerang adalah mencoba mengeksploitasi berbagai aplikasi yang berjalan melalui port yang terbuka di sisi server. Untuk mencegah hal-hal yang tidak diinginkan, biasanya administrator akan memasang firewall dan melakukan beberapa hal konfigurasi yang intinya adalah membatasi siapa saja yang akan mengakses server.

Jaringan nirkabel tidak seaman kabel. Tanpa tindakan keamanan yang ketat, memasang LAN nirkabel bisa seperti meletakkan port Ethernet di mana-mana, termasuk tempat parkir. Untuk mencegah eksploitasi terjadi, diperlukan produk yang dirancang khusus untuk melindungi jaringan nirkabel.

Pada penelitian ini adalah melakukan penerapan port knocking untuk mencegah eksploitasi dari pengguna yang ingin mengancam lalu lintas jaringan. Menggunakan rules firewall dengan 4 knock yaitu SSH (22), Telnet (23), Webfig (80) dan Winbox (8291) sebagai pintu atau knock terhadap pengguna yang tidak diizinkan untuk mengakses jaringan di router mikrotik. Tujuan utama penelitian ini adalah untuk melindungi para pelaku yang menyerang lalu lintas jaringan yang dapat berfungsi sebagai pengeksploitasian dengan melakukan pemindaian port dan pembatasan hak akses pengguna, sehingga hanya pengguna yang di terima oleh port saja (administrator) yang bisa mengakses secara penuh untuk membuka dan menutup akses port yang telah dikonfigurasi

2. TINJAUAN PUSTAKA

1.1. Mikrotik

Mikrotik adalah sistem operasi dari perangkat keras Mikrotik RouterBoard. Itu juga dapat diinstal pada PC dan akan mengubahnya menjadi router dengan semua fitur yang diperlukan - perutean, firewall, manajemen bandwidth, titik akses nirkabel, tautan backhaul, gateway hotspot, server VPN, dan banyak lagi. RouterOS adalah sistem operasi yang berdiri sendiri berdasarkan kernel Linux v2.6, dan tujuan Mikrotik adalah alat untuk menyediakan semua fitur ini dengan instalasi yang cepat dan sederhana serta antarmuka yang mudah digunakan[1].

1.2. Port Knocking

Port knocking merupakan teknologi baru yang menjanjikan untuk lebih mengamankan layanan jarak jauh. Teknologi ini dapat digunakan untuk menjaga semua port TCP tetap tertutup sampai pengguna mengautentikasi dengan port knock urutan. Selama urutan ketukan port tidak diketahui, semua port akan tetap tertutup, sehingga membuat server tidak terlihat oleh pemindaian port berbahaya. Setelah urutan ketukan yang valid diverifikasi oleh sistem, port TCP atau UDP yang telah ditentukan dapat memungkinkan koneksi standar untuk sebuah layanan yang telah ditentukan[2].

1.3. Firewall

Firewall merupakan pemfilteran paket dan menyediakan fungsi keamanan yang digunakan untuk mengelola aliran data ke router, dari router dan melalui router. Bersamaan dengan terjemahan alamat jaringan, ini yang berfungsi untuk mencegah akses tidak sah ke jaringan yang terhubung langsung dan router itu sendiri serta sebagai filter untuk lalu lintas keluar.

RouterOS memiliki fitur firewall stateful, yang berarti melakukan inspeksi paket stateful dan melacak status koneksi jaringan yang melintasinya. Ini juga mendukung sumber dan tujuan NAT (terjemahan alamat jaringan), pembantu NAT untuk aplikasi populer dan UPnP. Firewall menyediakan fitur untuk memanfaatkan koneksi internal, perutean, dan tanda paket. Hal itu dapat memfilter berdasarkan alamat IP, rentang alamat, port, rentang port, protokol IP, DSCP dan parameter lainnya, juga mendukung daftar alamat statis dan dinamis[1].

1.4. SSH (Secure Shell Connection)

SSH (biasa dikenal juga sebagai Secure Shell atau Secure Socket Shell) adalah protokol jaringan yang memberi pengguna, terutama administrator sistem, cara aman untuk mengakses komputer melalui jaringan yang tidak aman. SSH juga mengacu pada rangkaian utilitas yang mengimplementasikan protokol SSH. Secure Shell menyediakan otentikasi kata sandi yang kuat dan otentikasi kunci publik, serta

komunikasi data terenkripsi antara dua komputer yang terhubung melalui jaringan terbuka, seperti internet. Selain menyediakan enkripsi yang kuat,

SSH banyak digunakan oleh administrator jaringan untuk mengelola sistem dan aplikasi dari jarak jauh, memungkinkan mereka untuk masuk ke komputer lain melalui jaringan, menjalankan perintah, dan memindahkan file dari satu komputer ke komputer lain. SSH mengacu pada protokol jaringan kriptografi dan ke rangkaian utilitas yang mengimplementasikan protokol tersebut.

SSH menggunakan model client-server, menghubungkan aplikasi klien Secure Shell, yang merupakan akhir tempat sesi ditampilkan, dengan server SSH, yang merupakan akhir tempat sesi berjalan. Implementasi SSH sering kali menyertakan dukungan untuk protokol aplikasi yang digunakan untuk emulasi terminal atau transfer file[3].

1.5. IP Address

IP Address adalah address unik yang dapat mengidentifikasi perangkat di internet atau jaringan lokal. IP adalah singkatan dari "Internet Protocol," yang merupakan seperangkat aturan yang mengatur format data yang dikirim melalui internet atau jaringan lokal.

Intinya, IP Address adalah pengidentifikasi yang memungkinkan informasi dikirim antar perangkat di jaringan: alamat tersebut berisi informasi lokasi dan membuat perangkat dapat diakses untuk komunikasi. Internet membutuhkan cara untuk membedakan antara komputer, router, dan situs web yang berbeda. Setiap angka dalam set IP Address dapat berkisar dari 0 hingga 255. Jadi, rentang pengalamatan IP lengkap berkisar dari 0.0.0.0 hingga 255.255.255.255.

IP Address bukanlah nomor yang acak semata. Mereka secara matematis diproduksi dan dialokasikan oleh Internet Assigned Numbers Authority (IANA), sebuah divisi dari Internet Corporation for Assigned Names and Numbers (ICANN). ICANN adalah organisasi nirlaba yang didirikan di Amerika Serikat pada tahun 1998 untuk membantu menjaga keamanan internet dan memungkinkannya untuk digunakan oleh semua orang. Setiap kali seseorang mendaftarkan domain di internet, mereka melalui pendaftar nama domain, yang membayar sedikit biaya kepada ICANN untuk mendaftarkan domain tersebut[4].

1.6. WLAN (Wireless Local Area Network)

WLAN (Wireless Local Area Network) merupakan sekelompok komputer atau perangkat lain yang membentuk jaringan berdasarkan transmisi radio daripada koneksi kabel. Jaringan Wi-Fi adalah jenis WLAN; siapa pun yang terhubung ke Wi-Fi saat berselancar atau mencari sesuatu diinternet, itu bisa disebut menggunakan WLAN.

Cara kerja yaitu WLAN seperti Broadcast Media, WLAN mengirimkan informasi melalui gelombang radio. Data dikirim dalam bentuk paket. Paket berisi lapisan dengan label dan instruksi, bersama dengan alamat MAC (Media Access Control) unik yang ditetapkan ke titik akhir, memungkinkan perutean ke lokasi yang dituju[5].

3. METODELOGI PENELITIAN

3.1. Desain Topologi



Gambar 1. Rancangan Topologi

Gambar 1 diatas merupakan topologi pada penelitian ini. Untuk autentikasi port knocking diperlukannya internet ISP (Internet Service Provider), 1 Router Mikrotik, 1 laptop administrator dan 1 laptop penguji. Internet ISP yang dipakai menggunakan internet layanan rumah dari Router Fiberhome. Router Mikrotik dipakai sebagai server dan penyedia layanan port yang akan diamankan serta sebagai

autentikasi port knocking. Sedangkan 2 laptop digunakan sebagai administrator server dan penguji sebagai client.

3.2. Pengalamatan IP Topologi

Pertama, berikan IP Address pada perangkat dengan ketentuan IP Address di beberapa port seperti tabel dibawah.

Interface	IP Address	Default Gateway
WLAN Server	192.168.100.1/24	Suteriug
Ether 1	192.168.1.2/24	192.168.1.1
Ether 2	100.100.100.1/24	
FastEthernet0	100.100.100.2/24	100.100.100.1
WLAN Client	192.168.100.2/24-	192.168.100.1
	192.168.20.254/24	

Tabel 1.	IP	Address	Perangkat
----------	----	---------	-----------

Pemberian IP dilakukan router mikrotik (untuk bagian interface WLAN, Ether 1 dan Ether 2) yang digunakan untuk menghubungkan administrator dan client pada jaringan dengan mikrotik. Selain itu, pemberian IP dilakukan pada FastEthernet0 (Administrator) agar interface ini dapat mengakses router mikrotik. Sedangkan pada Client akan mendapatkan IP otomatis dari WLAN Client.

3.3. Data Implementasi Port Knocking

Pada tahap ini kebutuhan data untuk implementasi port knocking pada Mikrotik ini dapat dilihat pada tabel 2 Data Implementasi Port Knocking.

Layanan Service	Port	Autentikasi	Port Knocking	
CCII	22	Knock-satu	1001	
зэп	22	Knock-dua	2002	
Talpat	22	Knock-satu	1111	
Temet	25	Knock-dua	2222	
Wahfia	80	Knock-satu	1010	
weblig	80	Knock-dua	2020	
Winhow	8201	Knock-satu	1122	
windox	8291	Knock-dua	2233	

Tabel 2. Data Implementasi Port Knocking

Berdasarkan tabel 2 diatas pada penelitian ini implementasi port knocking dilakukan pada perangkat Mikrotik. Implementasi port knocking ini dilakukan untuk mengamankan port yang penting pada Mikrotik Seperti, SSH, Telnet, Webfig dan Winbox, yang memiliki jalur autentikasi pertama dan kedua, pada setiap jalur memiliki batas waktu yang tersedia. Pada setiap autentikasi memiliki batas waktu rata-rata 5 menit. Jika batas waktu telah habis sebelum autentikasi pada server layanan jaringan maka Client harus mengulangi dari autentikasi pertama.

4.1. Konfigurasi Port Knocking

4. HASIL PENELITIAN

Setelah selesai mengkonfigurasi pada bagian setting ISP yang berguna untuk mendapatkan jaringan internet yang nanti akan disebar ke perangkat yang terhubung dengan mikrotik, dan setting DHCP Server yang sebagai gateway dari Client yang terhubung ke WLAN dan memberikan IP otomatis kepada siapapun Client yang terhubung ke WLAN agar dapa menggunakan jaringan internet dari router mikrotik, selanjutnya akan dilakukan konfigurasi port knocking pada ke empat layanan yang tersedia yaitu SSH, Telnet, Webfig dan Winbox. Disini hanya akan diberi satu contoh konfigurasi dari satu layanan yaitu SSH, karena setiap cara konfigurasi port knocking dari ke empat layanan kurang lebih sama.

Konfigurasi port knocking pada ssh. Pertama pada bagian Chain pilih "input", setelah itu pada bagian "Protocol pilih "tcp" dan pada Dst.port isikan port "1001", port 1001 ini untuk pemicu pertama dalam mengamankan port 22 (SSH). Kemudian beralih pada tab Action pilih "add src to address list" dan pada bagian Address List isi dengan "ssh-satu" dengan Timeout "5 menit" untuk mengaksesnya, seperti gambar 2 dan 3 dibawah.

Firewall R	ule <1001>						
General	Advanced	Extra	Action	Statistics			ОК
	Chain	input			₹	•	Cancel
	Src. Address	:			•		Apply
	Dst. Address	:			•		Disable
	Protocol	: 🗌 🧕	(tcp)		∓▲		Comment
	Src. Port				•		Сору
	Dst. Port	: 🗆 🚺	001				Remove
	Any. Port	:			•		Reset Counters
	In. Interface	:			-		Reset All Counters
(Gambar	· 2. ŀ	Konfi	gurasi 1	ule p	erta	ma 1001

Firewall Rule <1001>	
General Advanced Extra Action Statistics	ОК
Action: add src to address list	Cancel
	Apply
Log Prefix:	Disable
Address List ssh-satu ₹	Comment
Timeout: 00:05:00	Сору
	Remove
	Reset Counters
	Reset All Counters

Gambar 3. Action rule pertama 1001

Konfigurasi rule knocking 2002, pada bagian Chain pilih "input", setelah itu pada bagian Protocol pilih "tcp" dan pada Dst.port isikan port "2002", port 2002 ini untuk pemicu kedua dalam mengamankan port 22 (SSH). Lalu beralih ke tab Advanced pada bagian Src Address list pilih "ssh-satu". Kemudian beralih pada tab Action pilih "add src to address list" dan pada bagian Address List isi dengan "ssh-dua" dengan Timeout "5 menit" untuk mengaksesnya, seperti gambar 4, 5 dan 6 dibawah.

Firewall Rule <2002>	
General Advanced Extra Action Statistics	ОК
Chain: input 🗸 🛧	Cancel
Src. Address:	Apply
Dst. Address:	Disable
Protocol: 🗌 6 (tcp) ∓ 🔺	Comment
Src. Port:	Сору
Dst. Port: 2002	Remove
Any. Port	Reset Counters
In. Interface:	Reset All Counters
	0000

Gambar 4. Konfigurasi rule kedua 2002

Firewall Rule <2002>	
General Advanced Extra Action Statistics	ОК
Src. Address List 📋 ssh-satu ∓ 🔺	Cancel
Dst. Address List	Apply
Gambar 5. Advanced rule kedu	a 2002
Firewall Rule <2002>	
General Advanced Extra Action Statistics	ОК
Action: add src to address list	Cancel
Log	Apply
Log Prefix:	Disable
Address List ssh-dua ∓	Comment
Timeout 00:05:00 ∓	Сору
	Remove
	Reset Counters
	Reset All Counters

Gambar 6. Action rule kedua 2002

Konfigurasi port 22, pada bagian Chain pilih "input" setelah itu pada bagian Protocol pilih "tcp" dan pada Dst.port isikan port "22", Lalu beralih ke tab Advanced pada bagian Src Address list pilih "sshdua". Kemudian beralih pada tab Action pilih "add src to address list" dan pada bagian Address List isi dengan "LOGIN_SSH" dengan Timeout "30 menit", seperti gambar 7, 8 dan 9 dibawah.

Firewall Rule <22>	<u> </u>
General Advanced Extra Action Statistics	ОК
Chain: input	Cancel
Src. Address:	Apply
Dst Address:	Disable
Protocol: 6 (tcp) ∓ 🔺	Comment
Src. Port	Сору
Dst. Port 🗌 22 🔺	Remove
Any. Port	Reset Counters
In. Interface:	Reset All Counters

Gambar 7. Konfigurasi port SSH 22

Firewall Rule <22>	
General Advanced Extra Action Statistics	ОК
Src. Address List 📋 ssh-dua ∓ 🔺	Cancel
Dst. Address List	Apply

Gambar 8. Advanced port SSH 22

Firewall Rule <22>	
General Advanced Extra Action Statistics	ОК
Action: add src to address list	Cancel
Log	Apply
Log Prefix:	Disable
Address List LOGIN_SSH	Comment
Timeout 00:30:00	Сору
·	Remove
	Reset Counters
	Reset All Counters

Gambar 9. Action port SSH 22

Konfigurasi drop pada port 22, pada bagian Chain pilih "input", setelah itu pada bagian Protocol pilih "tcp" dan pada Dst.port isikan port "22", lalu beralih ke tab Advanced pada bagian Src Address list pilih "LOGIN_SSH" dan klik centang pada kotak kecil (mengecualikan). Kemudian beralih pada tab Action pilih "drop" seperti gambar 10, 11 dan 12 dibawah.

Firewall Rule <22>	
General Advanced Extra Action Statistics	ОК
Chain: input ∓ 🗲	Cancel
Src. Address:	Apply
Dst. Address:	Disable
Protocol: 🗌 6 (tcp) ∓ 🔺	Comment
Src. Port	Сору
Dst. Port 22	Remove
Any. Port	Reset Counters
In. Interface:	Reset All Counters

Gambar 10. Konfigurasi drop SSH 22

Firewall Rule <22>											
General	Advanced	Extra	Action	Statistics		ОК					
5	Src. Address I	Cancel									
[Ost. Address I	list			_ ▼	Apply					
	Gan	ıbar	11. A	dvance	d drop SS	H 22					

wall R	ule <22>					×
neral	Advanced	Extra	Action	Statistics	ОК	٦

Gambar 12. Action drop SSH 22

Cancel Apply

4.2. Scanning Port Enable

Ge

Action: dro

Pengujian scanning port ini dilakukan dengan cara mengaktifkan konfigurasi port knocking. Dapat dilihat pada gambar 13 dibawah konfigurasi enable port knocking.

C* Safe Mode	Sessio	on: CC:2D	E0 7D 33 D	1										
auick Set	Firewall													
CAPsMAN	Filter R	ules NA	T Mangle	Raw	Service Po	rts	Connection	s Addr	ess Lists	Layer7 Protoco	ols			
m Interfaces				2	Denot Court	tore	OD Door	AT C	and a					
1 Wireless	-			0	Preset Cour	uers	OD Mese		10015					
Bridge	#	Action	Chain	Sr	c. Address	Dst	Address	Proto	Src. Por	t Dst. Port	In. Interf	Out Inte.	Bytes	Packets
	0 X	acc.	input		0.100.100.2		100.100.1	6 (tcp)		22,23,80,8.				
E PPP	=PO	RT KNOC	KING SSH											
Switch	1	Ef add	input					6 (tcp)		1001			520 B	
A Mesh	2	et add	input					6 (tcp)		2002			520 B	
in n	3	Ef add	input					6 (tcp)		22			6.9 KiB	
₽ ₩	4	T drop	input					6 (tcp)		22			08	
🖉 MPLS 🗈 🗅	EPU	RTKNUC	NING TELIN					C (trank					0.0	
🥂 Routing	6	er add	input					6 (tcp)		2000			00	
System	7		input					6 (tcp)		22			08	
		adda adda	input					E (top)		23			0.0	
Queues	PO	RTKNOC	KING WEBE	IG				o (acp)		2.5			00	
Files	9	rt add	input					6 (tcn)		1010			0.8	
Log	10	rt add	input					6 (tcp)		2020			08	
A Padius	11	t add	input					6 (tcp)		80			08	
Radius	12	¥ drop	input					6 (tcp)		80			260 B	
💦 Tools 🛛 🗋	= PO	RT KNOC	KING WINB	XC				1.000						
New Terminal	13	🖬 add	input					6 (tcp)		1122			2860 B	
Make Supout if	14	🖬 add	input					6 (tcp)		2233			2028 B	
a nanc Supourin	15	🖬 add	input					6 (tcp)		8291			17.3 KiB	1
Wew WinBox	16	X drop	input					6 (tcp)		8291			2521 B	1
Exit														

Gambar 13. Konfigurasi Filter Rules Enable

Kemudian untuk melakukan scanning masukkan IP wlan Mikrotik yaitu 192.168.100.1 pada bagian target dan akan masuk pada bagian command Nmap -T4 -A -v 192.168.100.1. Dan di dapatkan hasil dari scanning konfigurasi enable (mengaktifkan konfigurasi dari port knocking), pada port 22 (SSH), 23 (Telnet), 80 (Webfig), dan 8291 (Winbox) dalam keadaan filtered, menandakan konfigurasi firewall rule telah berhasil. Dilihat pada gambar 14 dibawah yaitu scanning port Mikrotik enable.

- Zenmap	- 0	×
Scan <u>T</u> ools <u>P</u> rofile	Help	
Target: 192.168.100.1	✓ Profile: Intense scan ✓ Scan Car	ncel
Command: nmap -T4	-A -v 192.168.100.1	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
OS 4 Host	nmap -T4 -A -v 192.168.100.1 🗸 🖉 Det	ails
	Completed MSE at 20:02, 6.108 elapsed Initiating MSE at 20:02 Completed MSE at 20:02, 00.07 elapsed Initiating MSE at 20:02, 00.0 elapsed Initiating MSE at 20:02, 00.0 elapsed Completed MSE at 20:02, 00.0 elapsed Not Size (0.0000, 00.0 elapsed Completed MSE at 20:02, 00.0 elapsed Completed MSE at 20:00, 00.0 elapsed Completed	
Filter Hosts	o:linux:linux_kernel:3	*

Gambar 14. Scanning Port Mikrotik Enable

4.3. Scanning Port Disable

Kemudian pengujian scanning port berikutnya ini dilakukan dengan cara mengnonaktifkan konfigurasi dari port knocking. Dapat dilihat pada gambar 15 dibawah konfigurasi disable port knocking.

C* Safe Mode	Sessio	on: CC:20	E0 7D:33 D2									
Guick Set	Firewall											
CAP\$MAN	Filter R	ules N	T Mangle	Raw Service P	orts Connection	s Addr	ess Lists	Layer7 Protoc	ols			
m Interfaces			o 🔊 🔽	BB Reset Cou	nara 00 Rese	t All Cour	dars					
Wireless				Di Hesercou	do riese	1701 COUR	Maris					
Bridge		Action	Chain	Src. Address	Dst Address	Proto	Src. Port	Dst. Port	In. Interf	Out Inte.	. Bytes	Packets
	0 X	✓ acc	input	100.100.100.2	100.100.100.1	6 (tcp)		22,23,80,8.			0 8	
Ca rrr	P0	RTKNO	KING SSH			0.000		1001			000 0	
Switch		Cr ad	1 input			6 (tcp)		1001			050 0	
3 Mesh	3 X	ET ad	input			6 (tcp)		2002			15 1 KFB	
ial IP	4 X	W dee	n input			6 (tcp)		22			88 F	
2 MOLO 1	PO	RT KNO	CKING TELNE	т								
WFL0	5 X	Et ad	1 input			6 (tcp)					88 B	
Routing	6 X	Et ad	1_ input			6 (tcp)		2222			88 B	
System 1	7 X	Et ad	d input			6 (tcp)		23			08	
Queues	8 X	3¢ dro	p input			6 (tcp)		23			176 B	
Files	.:: PO	RT KNO	CKING WEBFI	G								
1 100	9 X	Et ad	d input			6 (tcp)		1010			88 B	
E Log	10 X	ET ad	1 input			6 (tcp)		2020			88 B	
🥵 Radius	11 X	ET ad	d input			6 (tcp)		80				
Tools	12 X	J dro	p input			6 (tcp)		80			956 B	
New Terminal	12 Y	FT NNO	I isout	×		C (top)		1100			2049 0	
The second second	14 Y	et ad	input			6 (tcp)		2233			2028 8	
Make Supoutri	15 X	et ad	input			6 (tcp)		8291				1
🕘 New WinBox	16 X	1 du	p input			6 (tcp)		8291	-		2697 B	
Exit	14.11	44	p siput			o (rep)						

Gambar 15. Konfigurasi Filter Rules Disable

Selanjutnya untuk melakukan scanning masukkan IP wlan Mikrotik yaitu 192.168.100.1 pada bagian target dan akan masuk pada bagian command Nmap -T4 -A -v 192.168.100.1. Didapatkan hasil dari scanning konfigurasi disable (menonaktifkan konfigurasi dari port knocking) yaitu port pada Mikrotik dalam keadaan open atau terbuka. Dilihat pada gambar 16 dibawah yaitu scanning port Mikrotik disable.

Scan]	Tools Profile H	elp				
arget:	192.168.100.1	~	Profile:	Intense scan	~ Scar	Cance
Comma	nd: nmap -T4 -A	-v 192.168.100	1			
Host	s Services	Nmap Outp	ut Ports /	Hosts Topology Hos	t Details Scans	
S + H	lost 🔺	nmap -T4 -/	-v 192.168	.100.1	~	Detail
		Host is u Not show PORT 1/tcp 6.40.4 1 ftp-sys 2/tcp 1 stp-hos 1 824 (protocol 1 sth-hos 1 824 (protocol 1 1 824 (protocol 1 1 1 1 824 (protocol 1 1 1 1 1 1 1 1 1 1 1 1 1 1	p (0.005) j 993 clu STATE SEL open fty t: UNIX Min open ssl 2.0) tkey: 3b:47:31: 81:de:c6. open dor open tel open dor open tel these states tte: Rout thods: rted Nett open base unccoge	s latency). solatency). solate ports (ref VKVCE VERS) b Mikre croTik 6.40.4 Mikre continet Linue main (gen tp Mikre closs outer confi conds: GET HAD shuild the solatency main (continued the solatency) disclosed the solatency mikret conds: GET HAD shuild the solatency main (continued the solatency) mikret conds: GET HAD shuild the solatency mikret consolatency mikret consolatency mikret consolatency mikret consolatency mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret mikret m	set) INN STIK router ftp: STIK router ftp: STIK RouterOS s: (1):77:36:97:1a (1 (1):77:36:97:1a (1) (1):77:36:97:1a (1) (1):77:36:77:1a (1) (1):77:36:77:1a (1) (1):77:36:77:1a (1) (1):77:36:77:1a (1) (1):77:36:77:1a (1) (1):77:37:1a (1):77:37:1a (1) (1):77:37:1a (1):77:37:1a (1):77:37:37:1a (shd DSA) RSA) se: fig test you
	The state	fingerpri service : SF-Port53 windows-w SF:NSVers	-TCP:V=7 indows%r ionBindRe	tps://nmap.org/cgl .92%I=7%D=3/8%Time (D eqTCP,E,"\0\x0c\0\	<pre>l-bin/submit.cg =622756C0%P=164 x06\x81\x84\0\</pre>	L?new- 86-pc- 8\0\0 ♥

Gambar 16. Scanning Port Mikrotik Disable

4.4. Pengujian Akses Port Knocking

Pada pengujian akses port knocking disini akan langsung dilakukan dengan menggunakan knocking. Pengujian ini dilakukan dalam keadaan firewall rules telah aktif. Jika tidak mengikuti akses port sesuai dengan rules, maka pengujian tidak akan berhasil dan kembali lagi ke filter rules yang pertama.

Dalam pengujian pertama, sebelum Client mengakses remote pada port 22 (SSH), Client terlebih dahulu melakukan akses pada port knocking dengan kombinasi port 1001 dan 2002 (pada port SSH), dan setelah melakukan knocking maka Client dapat mengakses port 22 (SSH). Dapat dilihat gambar 17 rule knocking dan 18 address list yang masuk di port 22.



Gambar 17. Akses Port Rules SSH

Fire	ewall								
Fi	Iter Rules N	AT	Mangle	Raw	Service Ports	Connections	Address	Lists	Layer7 Protocols
+			2	7					
	Name		1	Addr	ess	Timeout		Creat	tion Time
D	LOGIN_S	SSH		192.1	68.100.254		00:27:33	Mar/0	08/2022 20:24:
D	ssh-dua			192.1	68.100.254		00:02:24	Mar/0	08/2022 20:24:
							00.00.40		0.0000.000.01

Gambar 18. Address List Rules SSH

Dalam pengujian kedua, sebelum Client mengakses remote pada port 23 (Telnet), Client terlebih dahulu melakukan akses pada port knocking dengan kombinasi yaitu port 1111 dan 2222 (pada port Telnet), dan setelah melakukan knocking maka Client dapat mengakses port 23 (Telnet). Dapat dilihat gambar 18 rule knocking dan 19 address list yang masuk di port 23.



Gambar 18. Akses Port Rules Telnet

Fire	Firewall												
Fi	lter Rules	NAT	Mangle	Raw	Service Ports	Connections	Address	Lists	Layer7 Protoc	ols			
	Name /			Addre	ess	Timeout		Crea	tion Time				
D	D OLOGIN_TELNET			192.1	68.100.254		00:29:41 N		Mar/08/2022 20:31:				
D	D @ telnet-dua			192.1	68.100.254		00:03:39	Mar/	08/2022 20:30:				
D	D @ telnet-satu				68.100.254		00:03:21 Mar/						

Gambar 19. Address List Rules Telnet

Dalam pengujian ketiga, sebelum Client melakukan akses remote pada port 80 (Webfig), Client terlebih dahulu melakukan akses pada port knocking dengan kombinasi port 1010 dan 2020 (pada port Webfig), dan setelah melakukan knocking maka Client dapat mengakses port 80 (Webfig). Dapat dilihat gambar 20 rule knocking dan 21 address list yang masuk di port 80.

@ 192.166.190.1	× @ 192.9	81001	× @ wat	F4	×	+		v - 0 X
← → C 0 A Her								🕑 🄄 🛛 🗳 🔹 🔹 🛸 🎒 E
🖀 Aass 🚯 Ourt 📮 Alas		y 🛛 Scopus 🛄						
RouterOS vices (walk)							Quin M	wanty Sevena 😝 🛃 -
								Home AP V Quick Set
where the second s								
NOT .								
					Wireles	8		Internet
Network Name	ini clicré					Address Acquisition	Static O/Automatic OPPPob	
Trequency	2112	w Merz				TP Address	192.198.1.2	
Band	20Hz-810 v					Netwask	255.255.255.0 (24) ¥	
Country	no_county_set	×				Cateway	192.198.1.1	
HAC Address	00:20 FX 70:33	68					* 192 168 1 1	
Use Access List (ACL)						DNS Servers	• 0888	
Will Decement	 madketts 	Citeda				MAC Address	CC201607033101	
					1000 1000	Firewall Router	8	
					and acres	MAC Server	•	
				Guest	t Wireless Networ	k MAC Websx		
Gaest Network	•							
					Wireless Client	S		
NAC Address	In ACI	Last TP	Uptime		Signal Strength			Local Network
DC141:49:40(FC:74	14	192.168.100.254	00:59:09	-27		IP Address	192.198.100.1	
						Network	255 255 255 0 (24) v	

Gambar 20. Akses Port Rules Webfig

Fire	ewall									
Fi	lter Rules	NAT	Mangle	Raw	Service Ports	Connections	Addres	is Lists	Layer7 Proto	cols
÷		> 😂	2	7						
	Name 🛆			Addres	SS	Timeout		Creatio	n Time	
D	LOGIN	I_WEB	FIG	192.16	8.100.254		00:29:58	Mar/08	/2022 20:48:	
D	webfig	j-dua		192.16	8.100.254		00:04:02	Mar/08	/2022 20:48:	
D	webfig	j-satu		192.16	8.100.254		00:03:42	Mar/08	/2022 20:47:	

Gambar 21. Address List Rules Webfig

Pengujian terakhir, sebelum Client melakukan akses remote pada port 8291 (Winbox), Client terlebih dahulu melakukan akses pada port knocking dengan kombinasi port 1122 dan 2233 (pada port Winbox), dan setelah melakukan knocking maka Client dapat mengakses port 8291 (Winbox). Dapat dilihat gambar 22 rule knocking dan 23 address list yang masuk di port 8291.

WinBox (6)	4bit) v3	32 (Addresses)						×
S WinBox (64	4bit) v3	32 (Addresses)						\times
S WinBox (6-	4bit) v3	.32 (Addresses)						×
File Tools								
Connect To	192.16	8 100 1 8291	_			M Keep	Pasewo	rd
Login	admin					🗌 Ope	n In New V	Vindow
Password						M Ada	Reconne	ct
				0.00	 			
Managed Net	Add/5	let		 Connect in	onnect			
Managed Net Refresh	Add(5 ghbors			 Connect in	onnect	Find	al	

Gambar 22. Akses Port Rules Winbox

Fire	ewall									
Fi	Iter Rules	NAT	Mangl	e Raw	Service Ports	Connections	Addr	ess Lists	Layer7 Pro	otocols
+	• - (*	2 😫		7						
	Name		- A	Address		Timeout		Creation	Time	
D	LOGIN	J_WINE	BOX	192.168.	100.254	00):29:49	Mar/08/20)22 20:42:	
D	winbo	x-dua		192.168.	100.254	00):04:49	Mar/08/20)22 20:41:	
D	winbo	x-satu		192.168.	100.254	00	04:47	Mar/08/20	022 20:41:	

Gambar 23. Address List Rules Winbox

5. KESIMPULAN

Mikrotik banyak dimanfaatkan untuk membangun sistem jaringan komputer skala kecil maupun besar. Semakin besar sistem jaringan yang terbagi, semakin banyak pula celah untuk dapat meretas atau mengakses mikrotik dari client yang tidak bertanggung jawab untuk mencuri data yang ada. Diperlukan cara pengamanan akses jaringan tersebut dengan salah satu cara yaitu mengamankan port jaringan.

Dengan adanya penelitian ini, peneliti dapat mengetahui cara melakukan keamanan jaringan dengan menggunakan metode port knocking dan dapat disimpulkan bahwa sistem keamanan jaringan telah berhasil dibuat dan sesuai dengan yang diharapkan. Kelebihan dari port knocking yaitu mengatur knock/ketukan port yang akan di set secara manual dan dapat mengakses server dimana saja selama masih terhubung ke dalam jaringan yang sama. Kekurangannya yaitu penyetingan yang cukup rumit dan adanya celah pembobolan server mikrotik dari serangan bruteforce.

DAFTAR PUSTAKA

- [1] A. Cameron, "What is MikroTik RouterOS? Part One," Feb. 2014. .
- [2] P. Lunsford and E. C. Wright, "Closed port authentication with port knocking," *ASEE Annu. Conf. Expo. Conf. Proc.*, no. June, pp. 1747–1754, 2005, doi: 10.18260/1-2--14788.
- [3] P. Loshin, "What is SSH (Secure Shell) and How Does it Work? Definition from TechTarget.".
- [4] "What Is an IP Address & What does it mean?".
- [5] "What Is a Wireless LAN (WLAN)? Cisco.".