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	URL	:	https://jurnal.netplg.com/index.php/jnca/article/view/10
Disetujui	:	01 Juli 2022	ISSN	:	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 dilakukan, hasil sistem dapat berjalan dengan baik dan dapat meningkatkan keamanan sistem jaringan yang 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.

Tabel 1. IP Address Perangkat

Interface	IP Address	Default Gateway
WLAN Server	192.168.100.1/24	
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	192.168.100.2/24–192.168.20.254/24	192.168.100.1

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.

Tabel 2. Data Implementasi Port Knocking

Layanan Service	Port	Autentikasi	Port Knocking
SSH	22	Knock-satu	1001
		Knock-dua	2002
Telnet	23	Knock-satu	1111
		Knock-dua	2222
Webfig	80	Knock-satu	1010
		Knock-dua	2020
Winbox	8291	Knock-satu	1122
		Knock-dua	2233

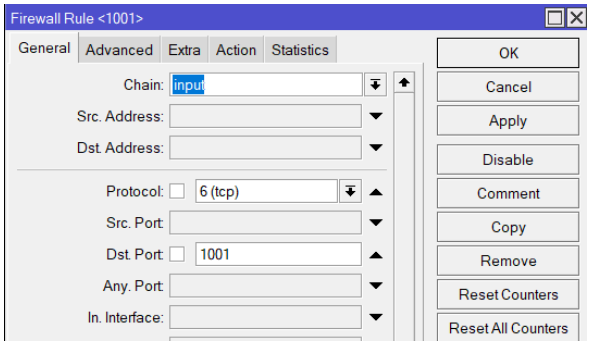
Berdasarkan tabel 2 diatas pada penelitian ini implementasi port knocking dilakukan pada perangkat Mikrotik. Implementasi port knocking ini dilakukan untuk mengamankan port yang penting pada Mikrotik Seperti, SSH, Telnet, Webfig dan Winbox, yang memiliki jalur autentikasi pertama dan kedua, pada setiap 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. HASIL PENELITIAN

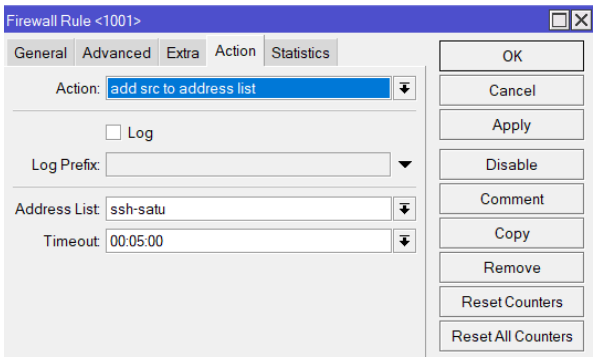
4.1. Konfigurasi Port Knocking

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.

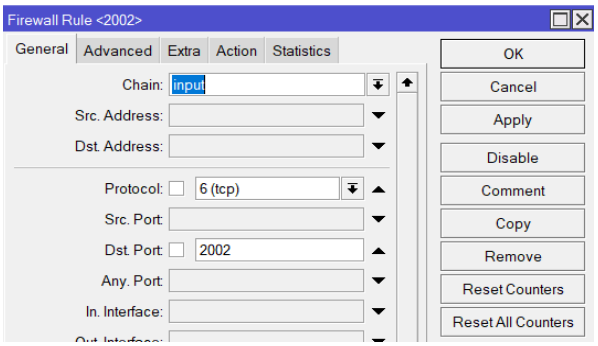


Gambar 2. Konfigurasi rule pertama 1001

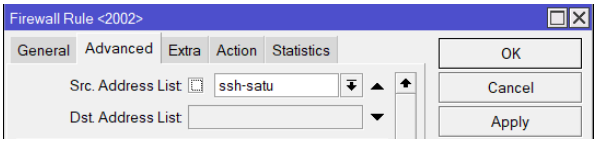


Gambar 3. Action rule pertama 1001

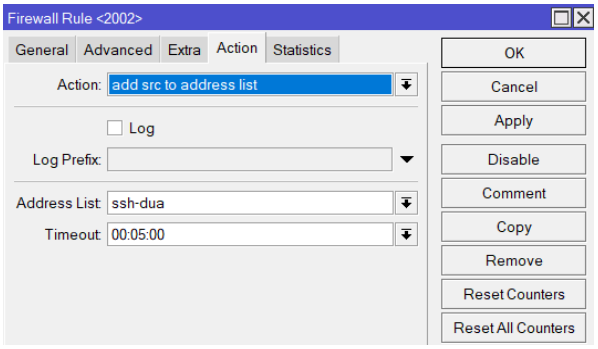
Konfigurasi rule knocking 2002, pada bagian Chain pilih “input”, setelah itu pada bagian Protocol pilih “tcp” dan pada Dst.port isikan port “2002”, port 2002 ini untuk pemicu kedua dalam mengamankan port 22 (SSH). Lalu beralih ke tab Advanced pada bagian Src Address list pilih “ssh-satu”. Kemudian beralih 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.



Gambar 4. Konfigurasi rule kedua 2002

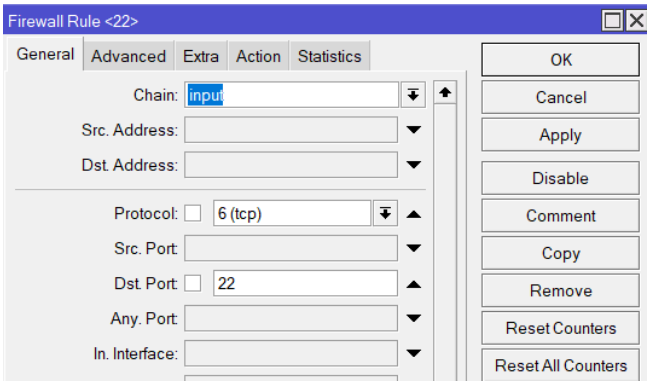


Gambar 5. Advanced rule kedua 2002

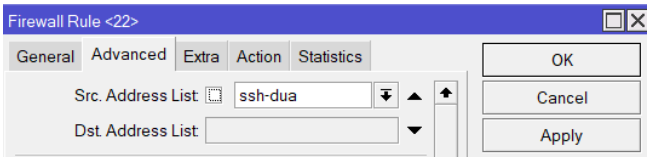


Gambar 6. Action rule kedua 2002

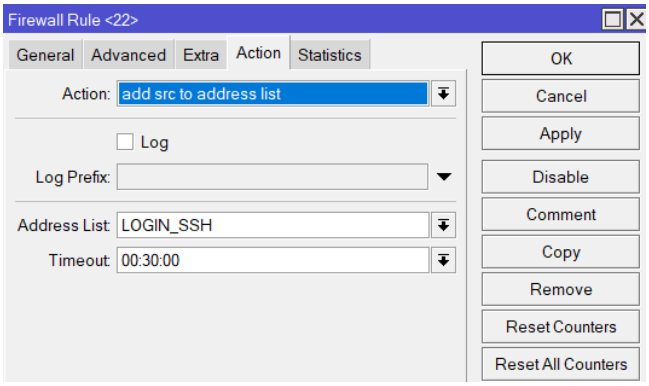
Konfigurasi port 22, pada bagian Chain pilih "input" setelah itu pada bagian Protocol pilih "tcp" dan pada Dst.port isikan port "22", Lalu beralih ke tab Advanced pada bagian Src Address list pilih "ssh-dua". Kemudian beralih pada tab Action pilih "add src to address list" dan pada bagian Address List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



Gambar 7. Konfigurasi port SSH 22

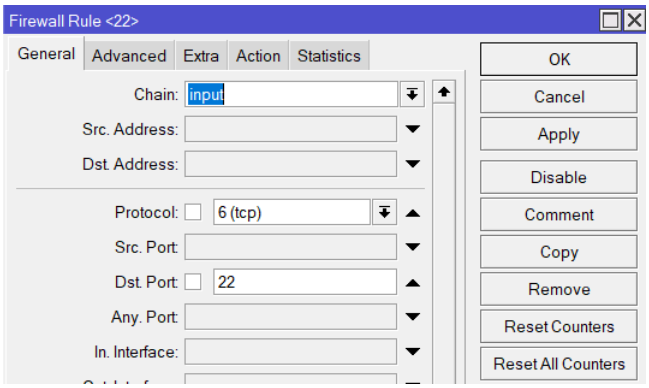


Gambar 8. Advanced port SSH 22

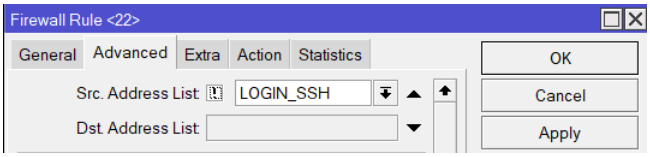


Gambar 9. Action port SSH 22

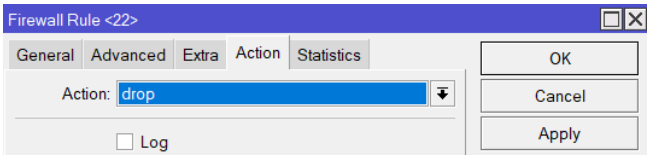
Konfigurasi drop pada port 22, pada bagian Chain pilih "input", setelah itu pada bagian Protocol pilih "tcp" dan pada Dst.port isikan port "22", lalu beralih ke tab Advanced pada bagian Src Address list pilih "LOGIN_SSH" dan klik centang pada kotak kecil (mengecualikan). Kemudian beralih pada tab Action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



Gambar 10. Konfigurasi drop SSH 22



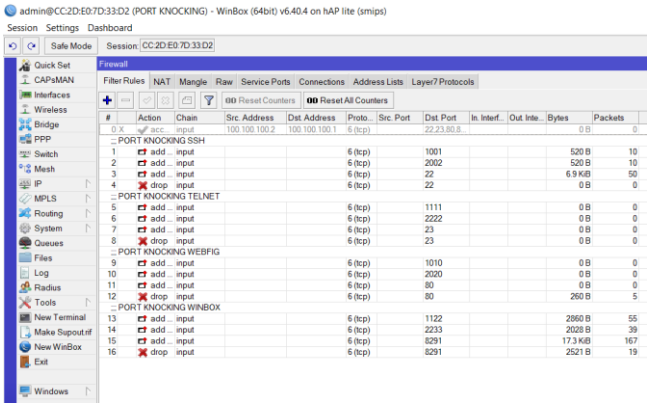
Gambar 11. Advanced drop SSH 22



Gambar 12. Action drop SSH 22

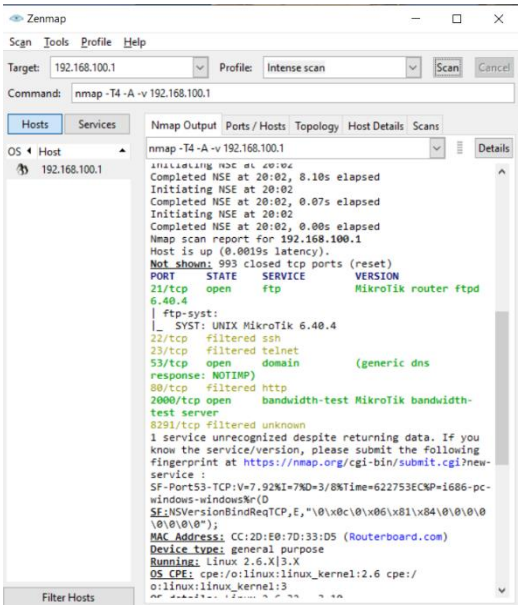
4.2. Scanning Port Enable

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



Gambar 13. Konfigurasi Filter Rules Enable

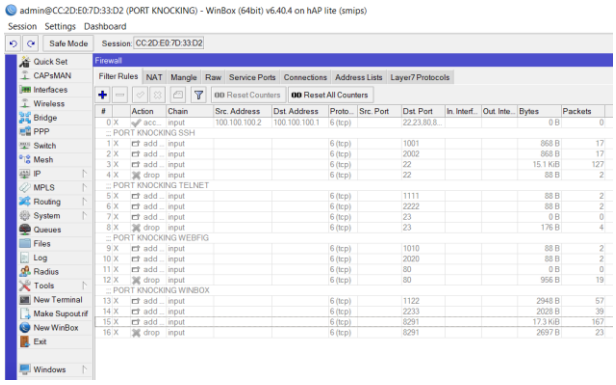
Kemudian untuk melakukan scanning masukkan IP wlan Mikrotik yaitu 192.168.100.1 pada bagian target dan akan masuk pada bagian command Nmap -T4 -A -v 192.168.100.1. Dan di dapatkan hasil dari scanning konfigurasi enable (mengaktifkan konfigurasi dari port knocking), pada port 22 (SSH), 23 (Telnet), 80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



Gambar 14. Scanning Port Mikrotik Enable

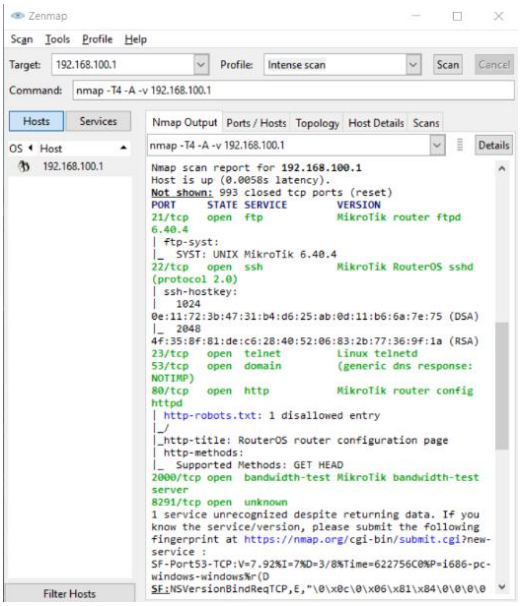
4.3. Scanning Port Disable

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



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.

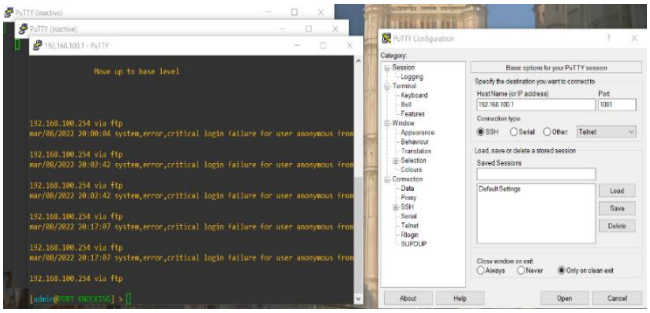


Gambar 16. Scanning Port Mikrotik Disable

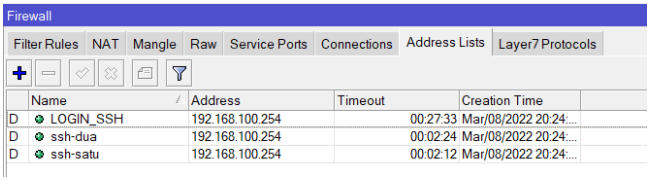
4.4. Pengujian Akses Port Knocking

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.

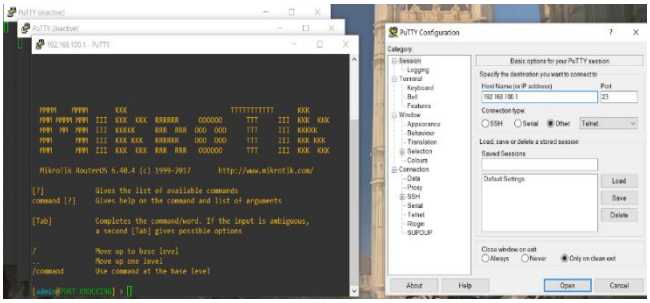


Gambar 17. Akses Port Rules SSH

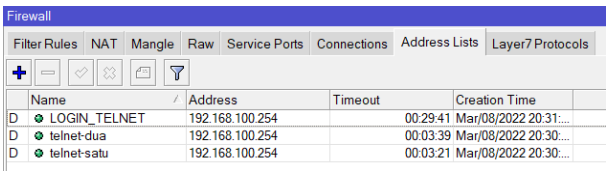


Gambar 18. Address List Rules SSH

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.

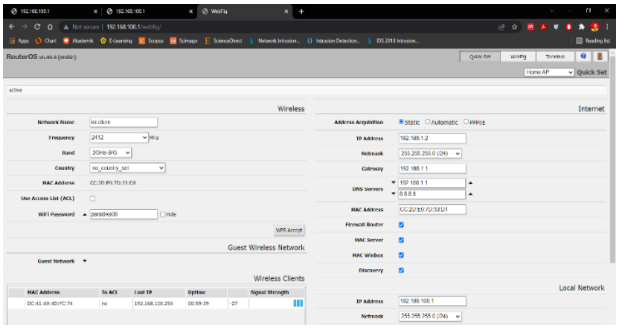


Gambar 18. Akses Port Rules Telnet

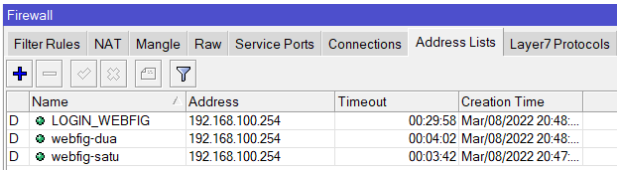


Gambar 19. Address List Rules Telnet

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.

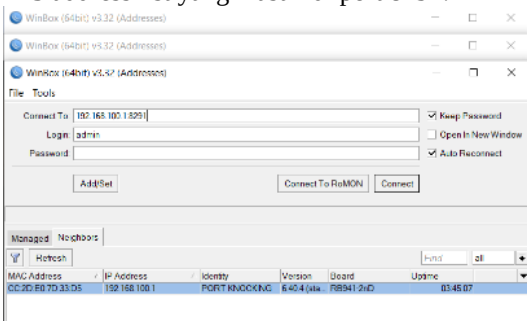


Gambar 20. Akses Port Rules Webfig

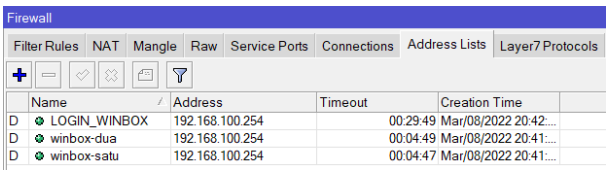


Gambar 21. Address List Rules Webfig

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.



Gambar 22. Akses Port Rules Winbox



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.” .