JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK) VOL 14, No.2, September 2023, pp. 318 - 329
p-ISSN : 2087-0868 (media cetak)
e-ISSN : 2598-9707 (media online)
http://ejurnal.provisi.ac.id/index.php/JTIKP

IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE PORT KNCOKING STUDI KASUS SMP ISLAM AL BISYRI

Joko winarno[1],Jeffri Alfa Razaq, M.kom[2]
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Stikubank
e-mail:joko.cah22@gmail.com[1], mrjf@edu.unisbank.ac.id[2]
Jalan Tri Lomba juang Semarang Telp. (024)8451976

ARTICLE INFO

Article history:

Received : 5 – Juli - 2023
Received in revised form : 20 – Juli - 2023
Accepted : 3– Agustus - 2023
Available online : 1 – September - 2023

ABSTRACT

Security of access to the intended device is a key element in network services. However, the problem that occurs is that open ports or access cannot be accessed without authentication, which can allow unauthorized users to access the server. This is the basis for increasing access to servers that have been built without having to close the ports used. Port knocking is a security system that has the ability to perform tasks that stop unwanted access. Basically, this method successfully closes all ports on the server. If users need access to a server, they are "knocking" to use the service. When finished, the port is closed again. Five ports were used by the systems built in the study: port 22 (SSH), port 23 (Telnet), port 80 (Webfig), and port 21 (FTP), port 445 (filesharing)

Keywords: *port kncoking, winbox,*

Received 5 – Juli - 2023; Revised 20 – Juli - 2023 ; Accepted : 3 - Agustus – 2023.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

1. PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer atau network security sangat berhubungan dengan keamanan data,oleh karena itu keamanan jaringan sangat penting untuk melindungi data dari berbagai serangan yang tidak bertanggung jawab.Serangan tersebut dapat di tujukan terhadap instansi perusahaan atau lembaga tertentu, tidak terkecuali SMP Islam AL Bisyri yang dapat terdampak pada serang tersebut

Serangan dilakukan pada celah di jaringan komputer, salah satunya menggunakan port-port yang terbuka. Orang yang tidak memiliki hak akses dapat dengan mudah mengontrol port-port ini.

Dalam situasi ini, pengguna masuk ke antarmuka router dengan menavigasi ke alamat IP-nya menggunakan browser, HTTP (port 80), SSH (port 22),Telnet (port 23), dan file sharing ,Untuk mengatasi serangan terhadap port -port pada sistem jaringan komputer maka menggunakan metode Port Knoking yang merupakan suatu sistem keamanan yang dibuat secara khusus untuk sebuah jaringan. Pada dasarnya cara kerja dari port knocking adalah menutup semua port yang ada, dan hanya pengguna tertentu saja yang dapat mengakses sebuah port yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu, dan akan di tambahkan fitur firwall untuk mengidentifikasi serangan apa saja yang masuk dan port mana saja yang di serang.

Berdasarkan latar belakang tersebut, maka peneliti mengangkat permasalahan ini kedalam penelitian yang berjudul " IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN METODE PORT KNOCKING STUDI KASUS SMP ISLAM AL BISYRI

2. TINJAUAN PUSTAKA

Pustaka Terkait Penelitian

Tahap tinjauan pustaka ini merupakan bagian dari sebuah penelitian yang bertujuan untuk mengumpulkan informasi atau referensi yang terkait dengan permasalahan yang akan diteliti. Tinjauan pustaka dapat dilakukan dengan mengumpulkan informasi dari berbagai sumber seperti buku, jurnal ilmiah, dan dokumen lain yang berkaitan dengan topik penelitian. Ini dapat membantu dalam memahami konteks penelitian serta dapat menghubungkannya dengan masalah yang sedang diteliti.

Pada tahap ini menjelaskan mengenai tinjauan pustaka yang digunakan dalam menunjang proses pembuatan **"IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE PORT KNCOKING STUDI KASUS SMP ISLAM AL BISYRI".** Berikut beberapa penelitian terdahulu yang memiliki kemiripan pembahasan dengan penelitian yang sedang diteliti sebagai berikut:

Sebuah penelitian yang dilakukan oleh **Nugroho Adhi Santoso,Khaediar Bagus Affandi,Rifki dwi kurniawan** Keamanan jaringan perlu ditingkatkan untuk mengurangi penyalahgunaan jaringan hacker, port Knocking digunakan pada penelitian ini untuk melakukan penelitian tentang pembuatan jaringan komputer yang aman. Berdasarkan hasil analisis dan pengujian implementasi sistem, dapat disimpulkan bahwa sistem dapat beroperasi dengan baik , dibandingkan dengan keamanan non-jaringan, keamanan jaringan bawaannya dapat ditingkatkan. keamanan dengan menggunkan port knocking.

Sebuah penelitian yang dilakukan oleh **Andik Saputro,Daniel Tunggono, Saputro Dwi Remawat (2022),**Keamanan jaringan sangat vital untuk jaringan komputer. Kelemahan keamanan pada ,Di masa pandemi ini, seluruh kegiatan belajar mengajar dan ujian dilakukan secara daring.Dengan ujian online, SMAN 5 Surakarta menyediakan server khusus untuk diberikan kepada siswa.Di sisi lain, Sementara server harus tetap terhubung ke internet, berbagai serangan dapat terjadi pada server. Serangan ini dapat melakukannya melalui IP server dan port, yang dapat mengakibatkan kebocoran data rahasia, pertanyaan yang akan diuji, dan data dari peserta, atau bahkan serangan ini dapat membuat server turun.

Sebuah penelitian yang dilakukan oleh **Paradika Dwi Oktaviansyah(2022)** layanan jaringan untuk keamanan jaringan yang dapat diakses oleh semua perangkat yang masalah yang terjadi adalah port atau akses terbuka tidak dapat diakses tanpa otentikasi,yang dapat memungkinkan pengguna yang tidak diinginkan untuk mengakses server. Port knocking adalah sistem keamanan yang memiliki kemampuan untuk melakukan fungsi yang memblokir akses yang tidak diinginkan.

Sebuah penelitian yang dilakukan oleh **Rosalia Ernawati1, Ikhwan Ruslianto2, Syamsul Bahri3** Keamanan *Server* memiliki akses layanan yaitu *port* 22 yang menjadi titik paling penting yang harus diamankan karena sering kali terjadi akses ilegal pada sistem. Firewall berfungsi sebagai dinding penghalang untuk mengatasi masalah tersebut. Namun,

p-ISSN : 2087-0868 e-ISSN : 2598-9707

karena cara kerjanya yang menutup semua akses tanpa memperhatikan siapa pun yang terhubung ke jaringan, penggunanya sendiri masih kurang efektif. Untuk mengatasi hal-hal tersebut, metode port knocking diterapkan pada keamanan server.

Perbedaan antara Penelitian Terkini dan Penelitian Sebelumnya

Pada tinjauan pustaka ini, dijelaskan perbedaan antara penelitian yang dilakukan dengan penelitian terdahulu yang terkait dengan penerapan QR Code dalam proses pemesanan makanan dan minuman. Penelitian yang dilakukan berbeda dari segi metode penelitian dan tujuan dari penelitian itu sendiri

Tabel 1. perbedaan antara Penelitian Terkini dan Penelitian Sebelumnya

Nomer jurnal	*Penulis Jurnal*	*Metode*	*Hasil Penelitian*
1.	(Nugroho Adhi Santoso, Khaediar Bagus Affandi, Rifki Dwi Kurniawan 2022) Implementasi Keamanan Jaringan Menggunakan Port Knocking	*literatur sistematis (SLR)*	Metode port knocking digunakan untuk menetapkan parameter sehingga peralatan komputer tidak memiliki port komunikasi terbuka yang bebas untuk diakses, tetapi tetap dapat dijangkau dari luar. Ini mencegah serangan yang dilakukan dalam keadaan port terbuka.
2	(Andik Saputro, Daniel Tunggono Saputro, Dwi Remawat 2022) Implementasi *Port Knocking* Untuk Keamanan Jaringan Komputer Dengan Metode *Demilitarized Zone*	Demilitarized Zone	Hasil pengujian menunjukkan data loging server saat terjadi DDoS attack dari tiga jenis pengujian DoS attack sebelum dan sesudah implementasi server. teknik DMZ
3	(Paradika Dwi Oktaviansyah 2022) Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode Port Knocking	knocking	Sebuah metode dimana menutup beberapa akses yang tidak terpakia ,agar tidak terjadi serangan kepada port yang dituju
4	(Rosalia Ernawati, Ikhwan Ruslianto, Syamsul Bahri 2022) IMPLEMENTASI METODE PORT KNOCKING PADA SISTEM KEAMANAN SERVER UBUNTU VIRTUAL BERBASIS WEB MONITORING	Berbasis web/data	Data pendukung penelitian yang akan dimasukkan ke dalam sistem disimpan di basis data. MYSQL digunakan untuk penelitian database. Berikut adalah perancangan database yang akan dibuat pada sistem..

p-ISSN : 2087-0868 e-ISSN : 2598-9707

3. METODE PENELITIAN

3.1Metodologi Pengumpulan Data

Dalam penelitian ini, metode berikut digunakan untuk mengumpulkan data:

1.Pengamatan (Observasi)

Untuk memastikan bahwa data dan informasi yang dikumpulkan dari penelitian ini adalah data asli, penulis melakukan pengamatan atau eksperimen langsung pada objek yang ditinjau.

2.Pengujian (Testing)

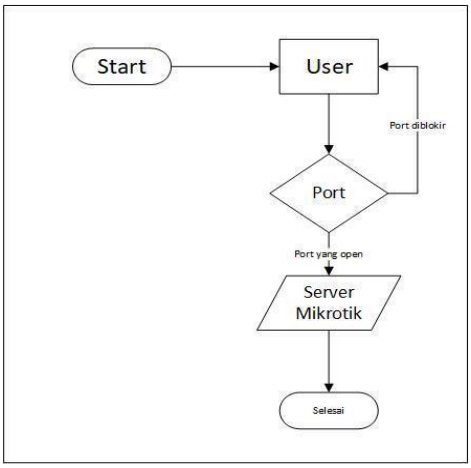
Penulis melakukan pengujian langsung pada berbagai objek. Pertama, merekamenguji port knocking sederhana pada routing dinamis; kemudian, mereka menguji jaringan normal; jaringan putus dengan port yang diblokir (dikenal sebagai bloking port); dan terakhir, mereka menguji jaringan open access port yang sebelumnya diblokir dengan ketukan.

3.Studi Pustaka (Literatur)

Metode ini memungkinkan penulis mendapatkan data dan informasi tentang subjek melalui penggunaan buku, jurnal, dan internet yang relevan

Analisis Keamanan jaringan

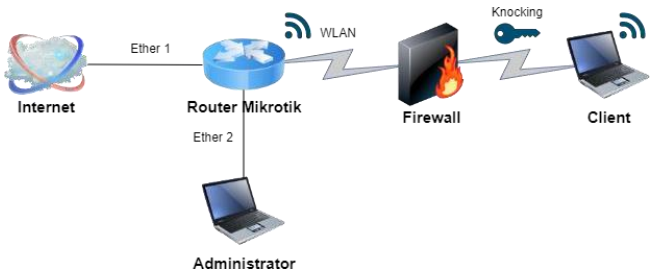
Sistem keamanan port knocking memungkinkan pengguna atau user dapat berinteraksi dengan server mikrotik pada jaringan local yang mana user yang terhubung sudah melalui verifikasi dari keamamnan mikrotik,dan terjadi nya serangan melalui port port yang terbuka seperti ssh(22),telnet(23),webfig(80),filesharing(445). Adapun untuk diagram dalam penelitian ini seperti gambar1



Gambar 1

3.3 Desain topologi

Untuk desain perancangan jaringan yang akan dibuat untuk autentikasi port knocking, diperlukan satu penyedia layanan internet (ISP), satu router Mikrotik, satu laptop administrator, dan satu laptop penguji.. Internet ISP yang dipakai menggunakan internet sekolah . 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



Gambar 2 topologi jaringan

p-ISSN : 2087-0868 e-ISSN : 2598-9707

3.4 Prepare (Persiapan)

Pada tahap persiapan ini peneliti akan menyiapkan beberapa alat-alat yang dibutuhkan dalam penerapan sistem keamanan port knocking diantaranya

No.	Perangkat Keras	Keterangan
1.	Router Mikrotik rb941	Router Mikrotik Sebagai alat penghubung dan pemantau lalulintas jaringan
2.	Kabel UTP Category 6	Media penghubung antara router dan pc
3.	Laptop/pc	Window 10

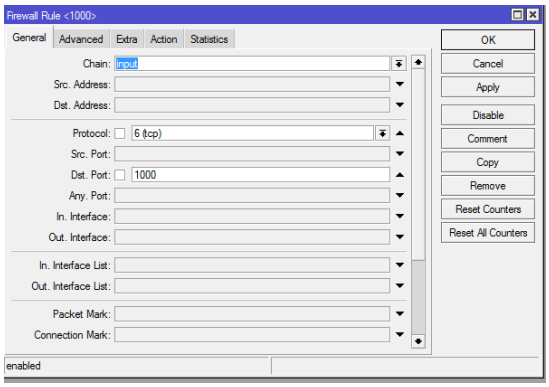
Tabel 2. alat dan bahan yang digunakan

4. Hasil dan pembahasan

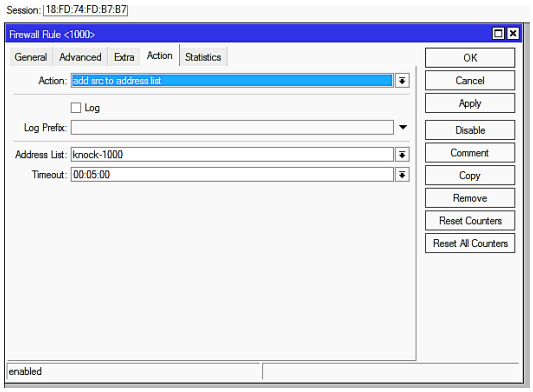
4.1 konfigurasi port kncoking

Setelah menyelesaikan konfigurasi di bagian setting ISP, yang bermanfaat untuk mendapatkan jaringan internet yang akan disebarkan ke perangkat mikrotik, dan setting DHCP Server, yang berfungsi sebagai gateway untuk klien yang terhubung ke WLAN dan memberikan IP otomatis kepada klien yang terhubung ke WLAN agar mereka dapat menggunakan jaringan internet dari router mikrotik. Selanjutnya, konfigurasi port knocking akan dilakukan pada keempat layanan yang terhubung.

Konfigurasi port knocking pada ssh (22),telnet(23),webfig(80).file sharing(445), ftp(21) Pertama pada bagian Chain pilih “input”, setelah itu pada bagian “Protocol pilih “tcp” dan pada Dst.port isikan port “1000”, port 1000 ini untuk pemicu pertama dalam mengamankan port . Selanjutnya, pilih tab Action dan pilih opsi untuk "menambahkan src ke daftar address." Pada bagian address list , ketikkan "knock-1000". dengan Timeout “5 menit” untuk mengaksesnya, seperti gambar 3 dan 4 dibawah.



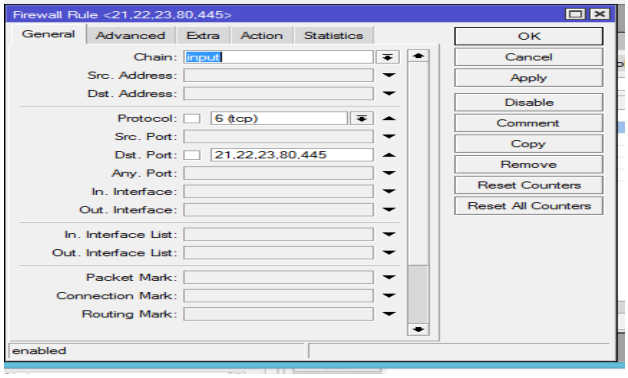
Gambar 3. konfigurasi rule pertama 1000



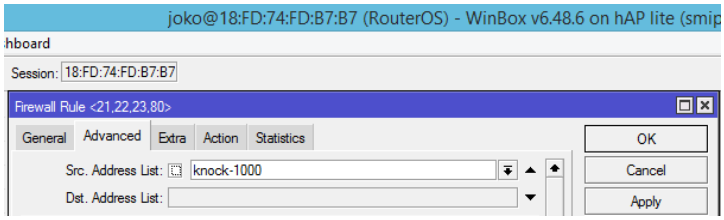
Gambar 4. **Action rule port 1000**

Konfigurasi rule ke 2 knocking , pada bagian Chain pilih “input”, setelah itu pada bagian Protocol pilih “tcp” dan pada Dst.port isikan port 21,22,23,80,445 port ini untuk pemicu kedua dalam mengamankan port 22 (SSH). 23 (talnet) 21(FTP) 80(webfig), 445 (fileshering). Lalu beralih ke tab Advanced pada bagian Src Address list pilih “knock-1000”. Kemudian beralih pada tab Action pilih “add src to address list” dan pada bagian Address List isi dengan “safe ip” dengan Timeout“none dynamice” untuk mengaksesnya, seperti gambar 5, 6 dan 7 dibawah.

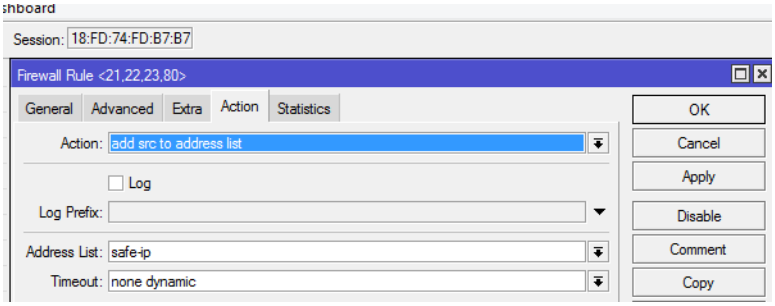
p-ISSN : 2087-0868 e-ISSN : 2598-9707



Gambar 5. Konfigurasi rule ke 2

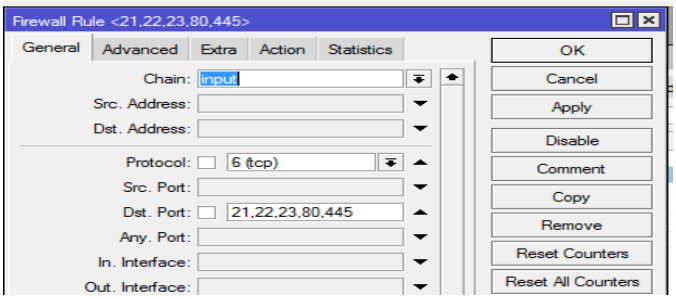


Gambar 6. Konfigurasi rule ke 2



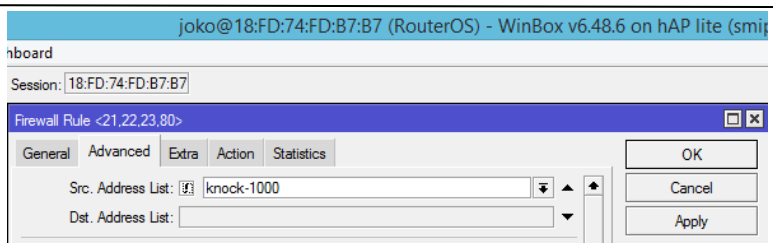
Gambar 7. Konfigurasi rule ke 2

Konfigurasi rule ke 3 knocking , pada bagian Chain pilih “input”, setelah itu pada bagian Protocol pilih “tcp” dan pada Dst.port isikan port 21,22,23,80, port ini untuk pemicu ketiga dalam mengamankan port 22 (SSH). 23 (talnet) 21(FTP) 80(webfig), 445 (fileshering). Lalu beralih ke tab Advanced pada bagian Src Address list pilih “safe-ip” klik centang pada kotak kecil (mengecualikan). Kemudian beralih pada tab Action “pilih drop” gambar 8, 9 dan 10 dibawah.

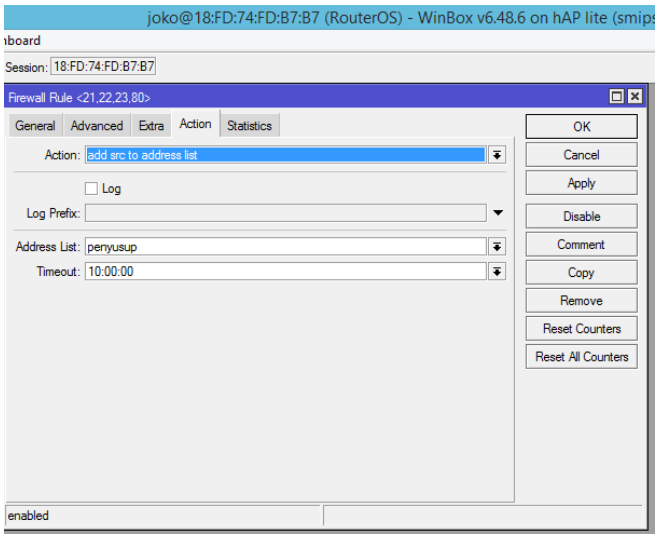


Gambar 8. Konfigurasi rule ke 3 tab general

p-ISSN : 2087-0868 e-ISSN : 2598-9707

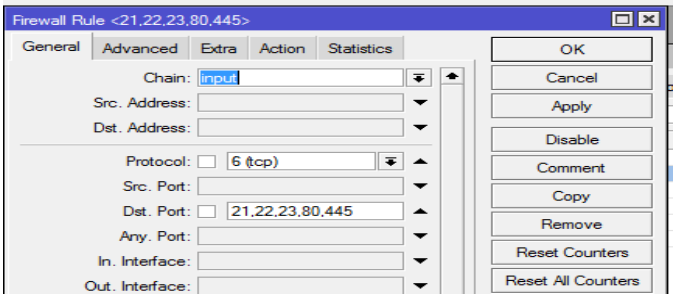


Gambar 9.konfigurasi rule ke 3 tab advanced

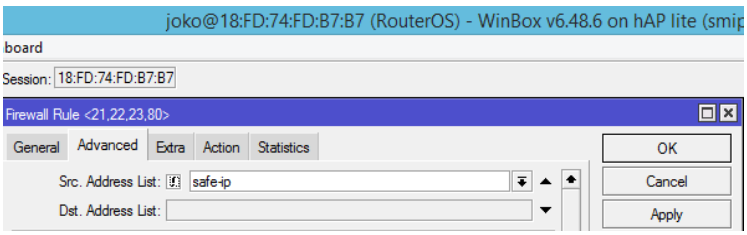


Gambar 10.konfigurasi rule ke 3 tab action

Konfigurasikan rule ke 3 . Pada bagian Chain, pilih "input", lalu pada protocol pilih "tcp". Isi port 21,22,23,80,445 sebagai port pemicu ketiga dalam mengamankan port 22 (SSH). 23 (talnet) 21(FTP) 80(webfig). Pada bagian advanced pilih Srcaddresstolist,"safe-ip" dan klik centang pada kotak kecil "mengecualikan".Kemudian beralih pada tab Action "pilih drop" gambar 11, 12 dan 13 dibawah.

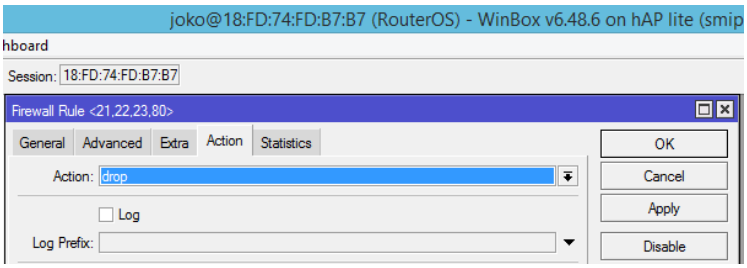


Gambar 11. Konfigurasi rule ke 4 general



Gambar 12. Konfigurasi rule ke 4 advanced

p-ISSN : 2087-0868 e-ISSN : 2598-9707

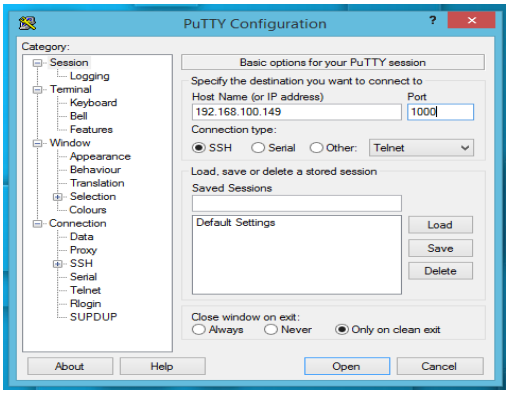


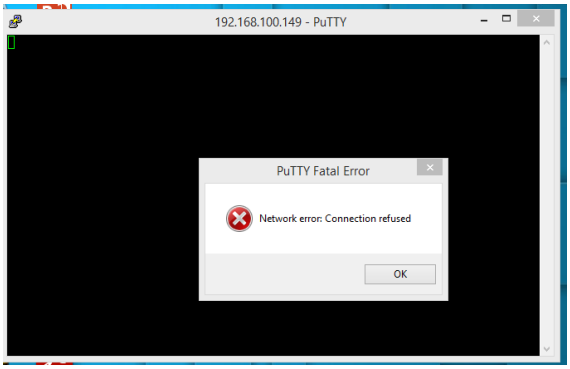
Gambar 13. Konfigurasi rule ke 4 action

4.2 Hasil dan pengujian port knocking

Untuk menguji akses port ini, knocking akan digunakan secara langsung. Pengujian ini dilakukan ketika firewall rules telah aktif. Pengujian akan tidak berhasil jika Anda tidak dapat mengakses port yang sesuai dengan aturan. Ini akan kembali ke filter aturan pertama.. Dalam pengujian , klien harus melakukan knocking port 1000 sebelum dapat mengakses port 22(SSH),23(TELNET)21(FTP),80(WEBFIG),445(FILE SHEARING)

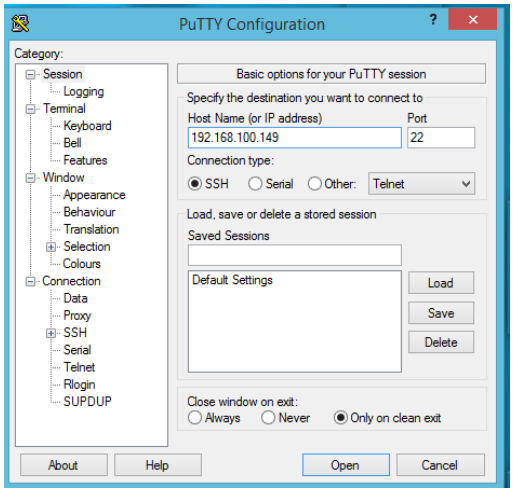
Setelah melakukan knocking, klien dapat mengakses port tersebut. Mereka dapat diamati pada gambar 14,15,16,17,18,19,20,21,22,23.





Gambar 14. Akses port 1000

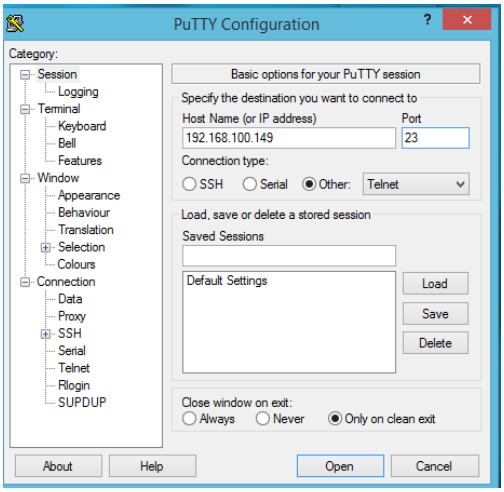
Gambar 15. Akses port 1000



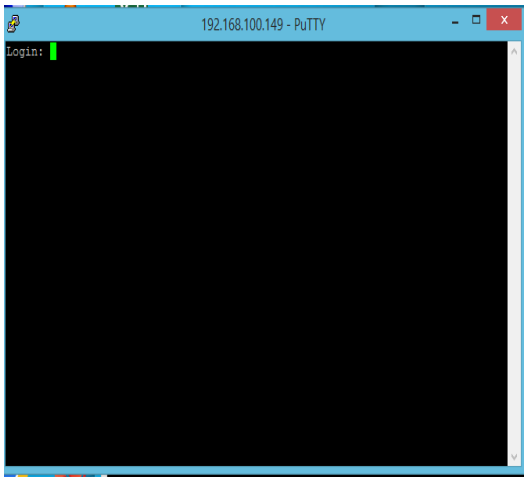
Gambar 16. Akses port 22(SSH)

Gambar 17. Akses port 22(SSH)

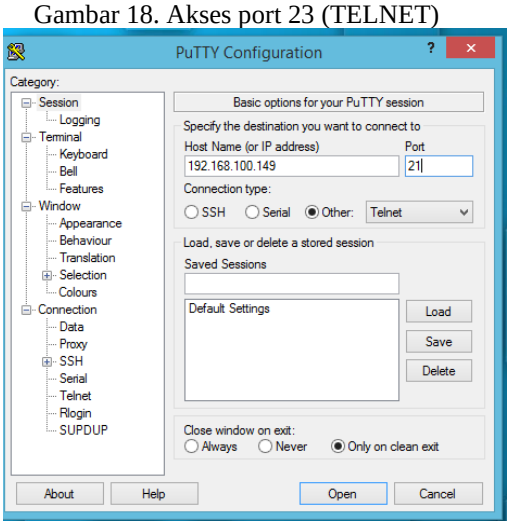
p-ISSN : 2087-0868 e-ISSN : 2598-9707



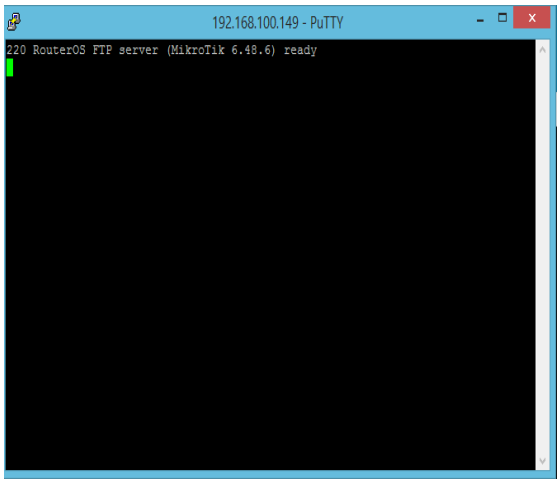
Gambar 18. Akses port 23 (TELNET)



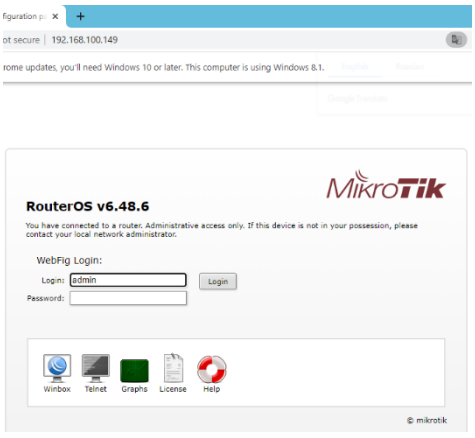
Gambar 19. Akses port 23 (TELNET)



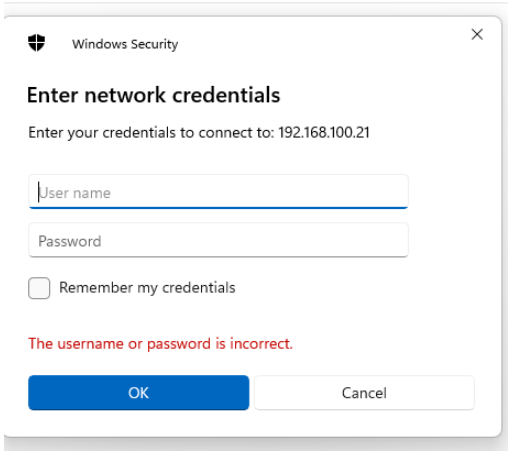
Gambar 20. Akses port 21 (FTP)



Gambar 21. Akses port 21 (FTP)



Gambar 22. Akses port 80(webfig)



Gambar 23. Akses port 445(file sharing)

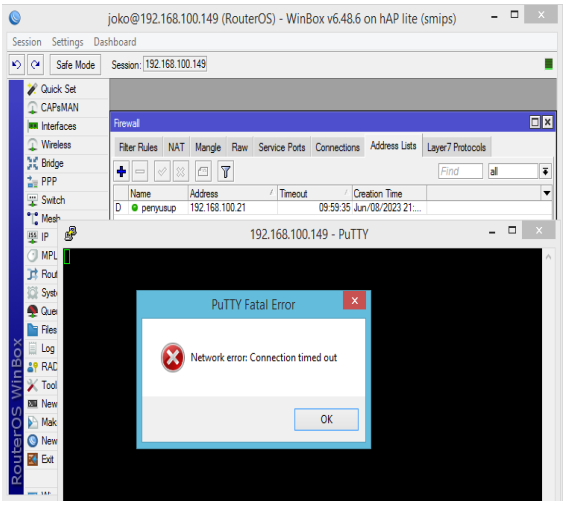
p-ISSN : 2087-0868 e-ISSN : 2598-9707

NO	Pengujian pertama menggunakan knocking	Keterangan
1	Akses ke ssh (22)	Berhasil
2	Akses ke ftp(21)	Berhasil
3	Akses ke webfig(80)	Berhasil
4	Akses ke telnet(23)	Berhasil
5	Akses ke file sharing (445)	Berhasil

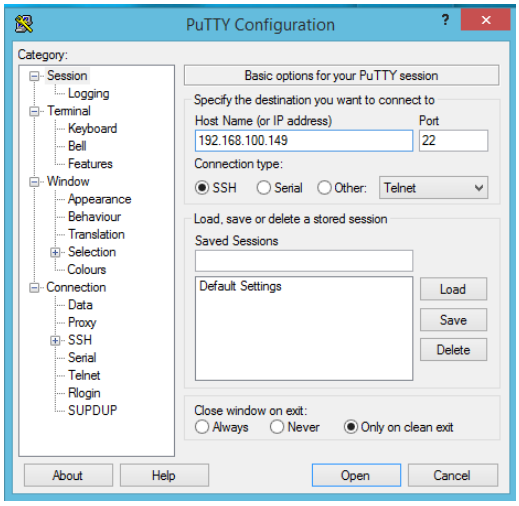
Tabel 3. Tabel pengujian port yang berhasil

4.3 hasil pengujian IP penyusup

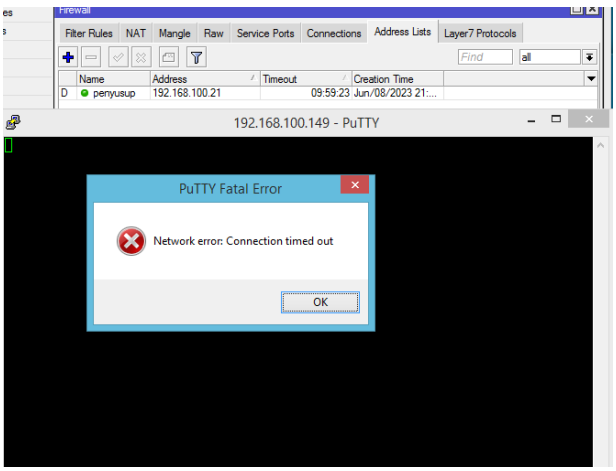
Hasil dari pengujian ketiga menunjukkan bahwa seseorang yang masuk ke port 21,22,23,80,445 tanpa mengetuk port 1000 maka akan di angap penyusup dan ip yang sudah masuk ke addres list penyusup akan di blok selama 10 jam .seperti yang terlihat pada gambar 24,25,26,27,28,29.



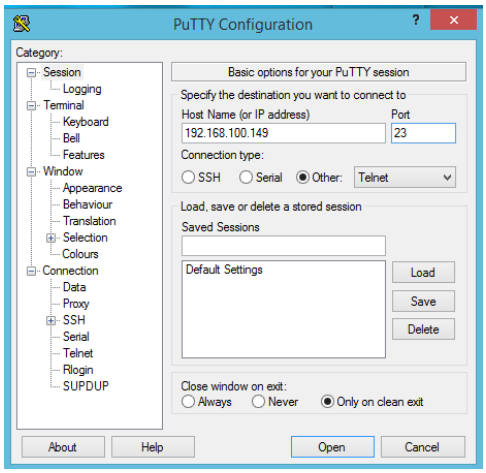
Gambar 24. Akses ke ssh yang di blok



Gambar 25. Akses ke ssh yang di blok

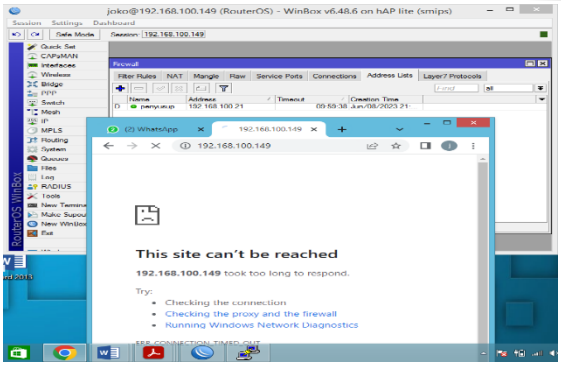


Gambar 26. Akses ke telnet (23) yang di blok

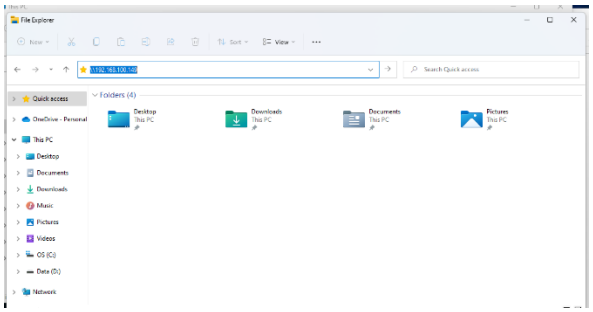


Gambar 27. Akses ke telnet yang di blok

p-ISSN : 2087-0868 e-ISSN : 2598-9707



Gambar 28. Akses ke webfig (80) yang di blok



Gambar 29. Akses ke file sharing (445) yang di blok

NO	Pengujian kedua tanpa knocking	Keterangan
1	Akses ke ssh (22)	Tidak berhasil
2	Akses ke ftp(21)	Tidak berhasil
3	Akses ke webfig(80)	Tidak berhasil
4	Akses ke telnet(23)	Tidak berhasil
5	Akses ke file sharing (445)	Tidak berhasil

Tabel 4. Tabel pengujian port yang di blok

5. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan yang menilai keamanan Router Mikrotik RB-941 bab ini mencakup kesimpulan dan rekomendasi dari penelitian tersebut.

1.) Penelitian ini melakukan analisis untuk mengidentifikasi cela keamanan pada Router Mikrotik Rb-941
2.) Hasil analisis yang dilakukan pada Router Mikrotik Rb-941 menunjukkan bahwa ada celah keamanan pada port-port yang terbuka
3.) Dari celah keamanan yang terjadi selama , peneliti mencoba melakukan penyerangan dengan brute force.
4.) Setelah memastikan bahwa keamanan jaringan masih rentan, peneliti menambah metode port knocking pada Router Rb-951
5.) Setelah menambahkan metode port knocking, keamanan server dan user telah teratasi dari serangan brute force .

6. SARAN

Dari hasil kesimpulan di atas, terdapat beberapa saran yang peneliti berikan untuk pihak-pihak yang terkait maupun untuk untuk penelitian selanjutnya

1) mengembangkan strategi serangan untuk Router Mikrotik dengan menggunakan metode serangan lainnya, seperti dengan sistem operasi dan alat yang lebih baru.
2) Untuk penelitian mendatang, implementasi ini diharapkan dapat meningkatkan keamanan jaringan, terutama untuk Mikrotik Router dan Mikrotik OS.

DAFTAR PUSTAKA

[1]-Ernawati, R., Ruslianto, I., & Bahri, S. (2022). Implementasi Metode *Port Knocking* Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring. *Jurnal Komputer Dan Aplikasi*, *10*(01), 158–169.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

[2]-Oktaviansyah, P. D. (2022). Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode *Port Knocking*. *Journal of Network and Computer Applications*, *1*(2), 13–24.
[3]Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). Implementasi Keamanan Jaringan Menggunakan *Port Knocking Network Security Implementation Using Port Knocking*. *Jurnal Janitra Informatika Dan Sistem Informasi*, *2*(2), 90–95. https://doi.org/10.25008/janitra.v2i2.156
[4]Saputro, A., Saputro, D. T., & Remawat, D. (2022). Implementasi *Port Knocking* Untuk Keamanan Jaringan Komputer Dengan Metode *Demilitarized Zone*. *INFORMA Politeknik Indonusa Surakarta*, *8*.