Volume 19 No.2 September 2022

Jurnal Ilmiah Fakultas Teknik
LIMIT'S

JURNAL ILMIAH FAKULTAS TEKNIK
LIMIT'S

ISSN 0216-1184

Alamat Redaksi Publikasi Ilmiah:

Fakultas Teknik – Universitas Satya Negara Indonesia
Jl. Arteri Pondok Indah No. 11 Jakarta Selatan 12240 Indonesia
Telp. (021) - 7398393, Fax. (021) - 77200352
http://www.usni.ac.id

ISSN 0216-1184

Jurnal Ilmiah Fakultas Teknik
LIMIT'S

Volume 19 September 2022 Nomor 2

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN MIKROTIK DENGAN METODE IP FILTERING DAN PORT KNOCKIING (STUDI KASUS BAROKAH.NET)

Muhammad Rifqi Maulana [1] , Abdul Kholiq[2]
Program Studi Teknik Informatika Fakultas Teknik
Mahasiswa Prodi Teknik Informatika[1], Dosen Prodi Sistem Informasi[2] Universitas Satya Negara Indonesia
Email: *muhammadrifqi419@gmail.com, abdulkholiq@usni.ac.id*

ABSTRAK

Keamanan jaringan pada server sangat penting, karena server adalah titik utama dalam penyaluran jaringan internet, jika keamanan jaringan lemah maka orang yang tidak berkepentingan dapat dengan mudah melakukan serangan terhadap server, baik untuk mendapatkan internet secara gratis atau merubah sistem pada server. Di Barokah.net sistem keamanan yang digunakan hanya pada login ke akses server dan menggunakan IP Static untuk identitas pada modem client, seiring berjalannya waktu di temukan ip address illegal yang muncul pada daftar IP ARP Mikrotik dan penyerangan menggunakan Brute Force yang terdeteksi pada Log sistem Mikrotik. Berfokus pada masalah tersebut penggunaan metode IP Filtering dan Port Knocking pada server utama merupakan cara yang tepat untuk meningkatkan sistem keamanan jaringan, dimana IP Filtering dan Port Knocking akan memberikan sebuah daftar dan autentikasi khusus agar perangkat yang ingin mendapatkan akses ke server dapat di perbolehkan oleh server. Sehingga metode IP Filtering dan Port Knocking dapat meningkatkan keamanan jaringan pada Barokah.net.

Kata Kunci : *Mikrotik, IP Filtering, Port Knocking, Server*

ABSTRACT

Network security on the server is very important, because the server is the main point in the distribution of the internet network, if network security is weak then unauthorized people can easily attack the server, either to get free internet or change the system on the server. At Barokah.net the security system is used only to login to access the server and use Static IP for identity on the client modem, over time illegal ip addresses are found that appear on the Mikrotik ARP IP list and attacks using Brute Force are detected in the Mikrotik system log . Focusing on this problem, the use of IP Filtering and Port Knocking methods on the main server is the right way to improve network security systems, where IP Filtering and Port Knocking will provide a list and special authentication so that devices that want to gain access to the server can be allowed by the server. So that IP Filtering and Port Knocking methods can improve network security on Barokah.net.

Ke*ywords *: *Mikrotik, IP Filtering, Port Knocking, Server*

PENDAHULUAN

Barokah.Net merupakan salah satu penyedia layanan internet berskala kecil yang berada di lingkup RT-RW pada daerah Caringin Kota Bekasi. Model distribusi layanan internet yang digunakan adalah jaringan Fiber To The Home (FTTH) yang menggunakan Mikrotik sebagai management bandwith dan server utama. Saat ini sistem keamanan yang di gunakan hanya pada login untuk akses ke server dan menggunakan IP static untuk identitas modem pada client. Namun seiring dengan berkembangnya jumlah pengguna layanan internet, juga mulai banyak orang orang yang mencoba masuk ke server atau sekedar menggunakan internet tanpa berlangganan. Hal ini penulis temukan dari observasi dan wawancara di lapangan, dimana ada upaya serangan menggunakan Brute Force serta IP Scanning, dan memang berdasarkan berdasarkan sistem keamanan yang ada saat ini hal tersebut sangat mungkin dilakukan, kemudian dengan terjadinya serangan-serangan tersebut mengakibatkan kinerja server dan layanan internet kerap mengalami gangguan.

Berdasarkan keadaan seperti ini diperlukan suatu solusi agar pihak yang merugikan tersebut tidak dapat akses apapun dari server. Dari hasil observasi yang peneliti lakukan terdapat beberapa solusi yang dapat di gunakan untuk mengatasi masalah tersebut yaitu Metode PPOE, IP Filtering dan port Knocking. Tetapi solusi dapat di implementasikan di Barokah.net adalah dengan menerapkan metode Ip Filtering dan Port Knocking, karena metode ini akan memfilter setiap ip address yang tidak terpakai dan bekerja dengan menonaktifkan port yang sering di gunakan dalam menyerang server seperti ssh.(22), telnet (23), dan www (80), yang kemudian akan dibuat sebuah autentikasi agar dapat masuk ke dalam port yang akan di gunakan untuk masuk ke dalam server. Metode keamanan jaringan ini sangat cocok dengan kondisi yang ada pada Barokah.net, di mana kurangnya SDM dan kondisi keuangan Barokah.net jika harus mengubah sistem menggunakan metode PPOE, karena jika menggunakan metode ini harus mengubah seluruh sistem yang ada pada server dan client.

TUJUAN DAN MANFAAT PENELITIAN

Adapun tujuan dan manffat penelitian yang hendak dicapai peneliti dalam penelitian ini adalah untuk menganalisis secara mendalam tentan masalah keamanan pada layanan jaringan internet yang terjadi pada Barokah.Net, serta mengimplementasikan Metode Keamananan IP Filtering dan Port Knocking pada layanan jaringan internet pada Barokah.Net agar layanan internet yang disediakan tersebut dapat berjalan lebih optimal dan aman dari *intruder*.

DASAR TEORI

Keamanan Jaringan

Menurut Joko Dwi Santoso dalam jurnal dengan judul keamanan jaringan nirkabel menggunakan wireless intrusion detection system (e-ISSN: 2655-142X, 2019) Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun network security biasanya bertentangan dengan network access, dimana bila network access semakin mudah, maka network security semakin rawan, begitu pula sebaliknya. Sebuah jaringan dikatakan aman apabila memenuhi 6 prinsip, yaitu :

1. Kerahasiaan (Secrecy)
2. Integritas (Integrity)
3. Ketersediaan (Availability)
4. Authentication
5. Akses Kontrol
6. Non-Repudiation

Mikrotik

Menurut Jurnal Um-Palembang Feby Ardianto dan Eliza Mikrotik merupakan sistem operasi router di-rilease dengan nama mikrotik routerOs yang mampu diinstall pada komputer biasa, tidak seperti sistem operasi router lainya yang hanya bisa diinstall pada hardware tertentu. Memiliki fungsi untuk membagi-bagi koneksi internet ke beberapa komputer pengguna user. Independen berbasis Linux khusus untuk komputer yang difungsikan sebagai router, didesain untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks. Mikrotik didesain untuk memberikan kemudahan bagi penggunanya, dapat diakses melalui windows atau application (WinBox). mencakup berbagai fitur seperti firewall dan nat, routing, hotspot, DNS server, DHCP server, management bandwitch, web proxy serta mampu menyaring akses di internet dan dapat memblokir website.

IP Address

Menurut Aidil Halim Lubis dan Abdul Halim Hasugian dalam penelitiannya menjelaskan IP address adalah metode pengalamatan pada jaringan komputer dengan cara memberikan beberapa angka tersusun berderet pada komputer (host), router atau peralatan jaringan lainnya. IP address sering disebut juga sebagai alamat logika yang diberikan pada peralatan jaringan yang menggunakan protokol TCP/IP. Protokol TCP/IP ini adalah yang paling banyak digunakan untuk meneruskan (routing) informasi pada jaringan WAN. Tiap-tiap komputer atau peralatan jaringan akan memiliki alamat IP yang unik dan masing-masing berbeda dengan yang lainnya. Hal tersebut untuk mencegah terjadinya kesalahan pada saat transfer data ketika berlangsung. Protokol TCP/IP ini berhubungan langsung dengan media fisik dari perangkat jaringan. Pada saat ini IP address yang digunakan memiliki 2 tipe yaitu IP v4 dan IP v6.

Port

Menurut Michael Orien dan Bayu Kanigoro di website socs.binus.ac.id/2019/11/06/port-jaringan-komputer/port port adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan Port Number dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam Port TCP dan Port UDP. Karena memiliki angka 16-bit, maka total maksimum jumlah port untuk setiap protokol transport yang digunakan adalah 65536 buah.

Port Knocking

Menurut Yudi Mulyanto, M. Julkarnain, dan Aldela Jabi Afahar dalam jurnal yang berjudul Implementasi *Port Knocking* Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar Port Knoking 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 user tertentu saja yang dapat mengakses sebuah port yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu.

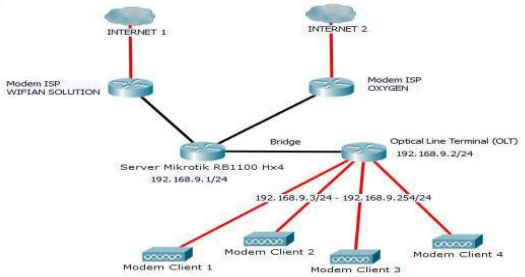
IP Filtering

Ip Filtering merupakan suatu sistem keamanan yang di buat dalam skala local di sebuah jaringan, di mana sistem ini akan berjalan pada firewall filter rule dan melakukan block pada ip address yang tidak terpakai. IP Filtering menyediakan perlindungan dasar untuk firewall dengan menentukan data yang diperbolehkan untuk melewati firewall berdasarkan rincian sesi IP Address.

METODOLOGI PENELITIAN

Analisis Hasil Dan Pembahasan

Dari hasil Analisa pada sistem jaringan barokah.net Topologi yang di gunakan ialah Topologi Star. Dimana router Mikrotik sebagai pusat untuk pengelolaan bandwith, dari menerima bandwith ISP yang kemudian akan di salurkan ke client. Untuk menyalurkan bandwith ke client Barokah.net menggunakan Fiber Optic sebagai media transmisinya, dimana Barokah.net menggunakan OLT HSGQ Epon yang kemudian akan di hubungkan menggunakan kabel Fiber Optic ke Modem Wireless Epon. Modem Wireless Epon ini yang akan di berikan IP Static dari router Mikrotik agar mendapatkan akses Internet, kemudian akan di buatkan segmen IP Address baru yang akan di pergunakan oleh client baik menggunakan wireless maupun kabel UTP.



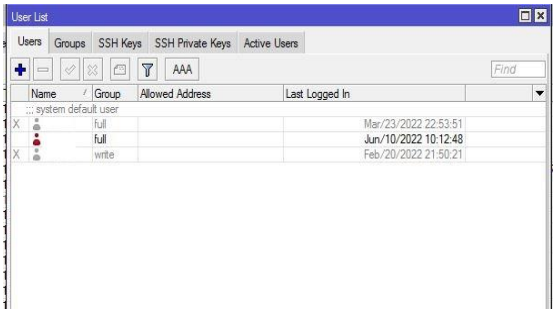
Gambar 1. Topologi Jaringan Yang Sedang Berjalan

Bandwith Internet Barokah.net saat ini sebesar 100 Mb/s dengan harga 5.280.000 dari ISP Wifian Solution dan 80 Mb/s dengan harga 2.200.000 dari ISP Oxygen, total kecepatan bandwith yang di miliki Barokah.net adalah 180 Mb/s. Dengan pembagian bandwith terdapat pada lampiran 2, maka modem pada setiap client akan mendapatkan Limit At 3 Mb/s saat pemakaian bandwith sedang padat dan mendapatkan kecepatan yang sesuai dengan Max limit paket saat pemakaian normal.

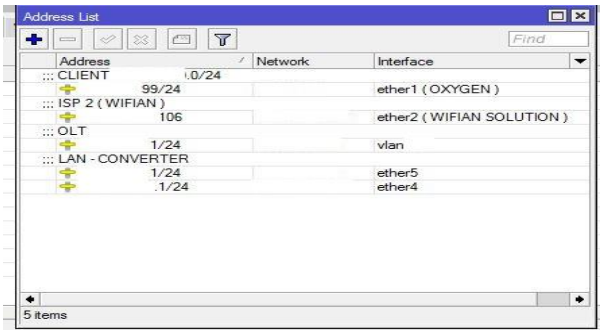
Analisa Sistem Keamanan Pada Jaringan

Dari hasil analisa terhadap sistem keamanan jaringan Barokah.net tingkat keamanan yang ada masih rendah, dimna untuk memanagement jaringan menggunakan User dan Password untuk Login ke Mikrotik, IP Static untuk jaringan local dan terdapat Port yang terbuka untuk masuk ke dalam server. IP static memiliki kekurangan karena tidak memiliki proses autentikasi apapun ke server, dimana orang lain bisa mendapatkan akses internet hanya dengan mengetahui range IP yang digunakan dan mencari ip yang tidak terpakai menggunakan IP Scanner. Port yang terbuka ini akan rentan sekali jika diserang menggunakan metode Brute force.

Gambar 2. Port Terbuka Pada Sistem Yang Berjalan



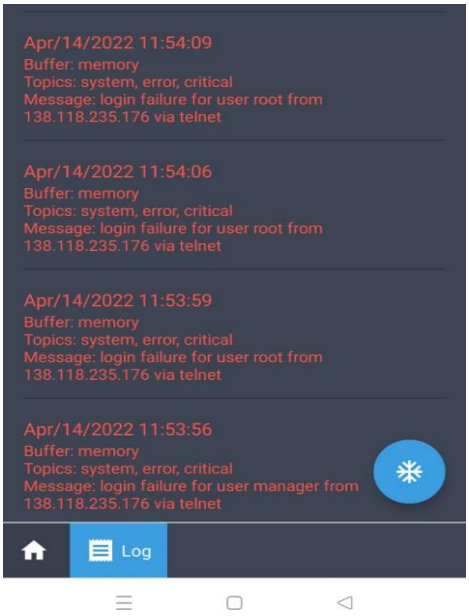
Gambar 3. User Dan Password Untuk Login Ke Mikrotik



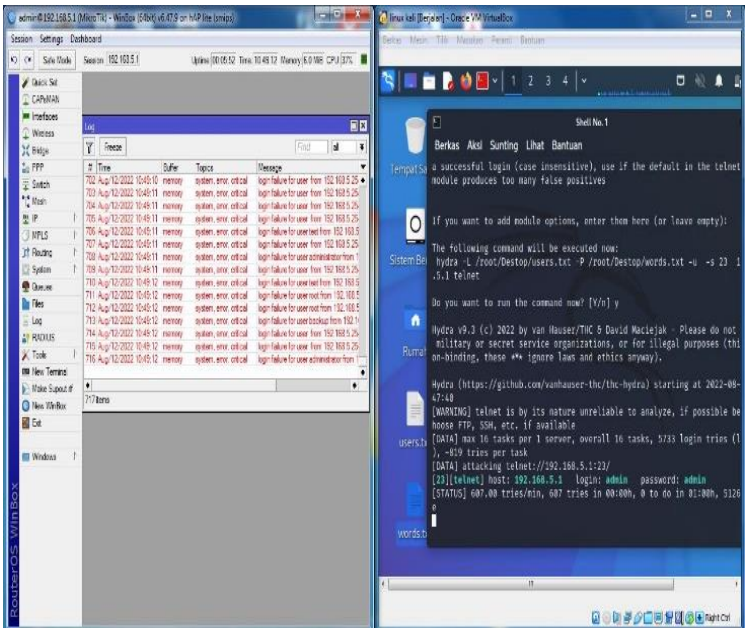
Gambar 4. IP Static Pada Server

Analisis Permasalahan

Barokah.net adalah salah satu penyedia layanan internet berskala kecil di wilayah Caringin Kota Bekasi. Koneksi jaringan client di sini menggunakan Fiber To The Home (FTTH) yang menggunakan sistem Ip Static untuk modem pelanggan. Sedangkan pada server utama menggunakan user dan password untuk dapat mengontrol server. Namun dalam proses berjalannya sistem terdapat isu percobaan untuk mendapatkan akses internet dan akses ke server utama tanpa izin dari pihak Barokah.net, dimana hal ini dapat merugikan Barokah.net secara finansial. Pembuktian salah satu permasalahan jaringan Barokah.net ialah serangan Brute Force dan IP Scanning yang berakibat pada berkurangnya kinerja server utama dan kerugian secara finansial. Saat ini sering terdapat keluhan seperti login failure dan client ilegal yang selanjutnya dapat berimbas pada penurunan performa jaringan internet yang terhubung pada jaringan tersebut.

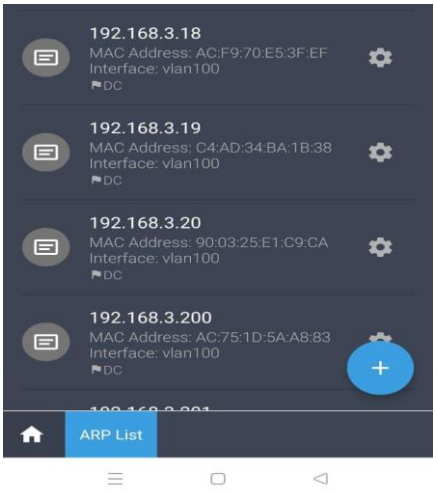


Gambar 5. Log System Server

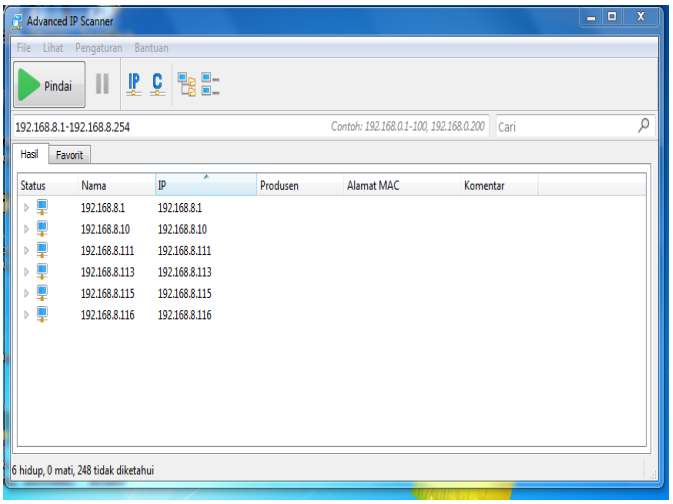


Gambar 6. Percobaan Brute Force

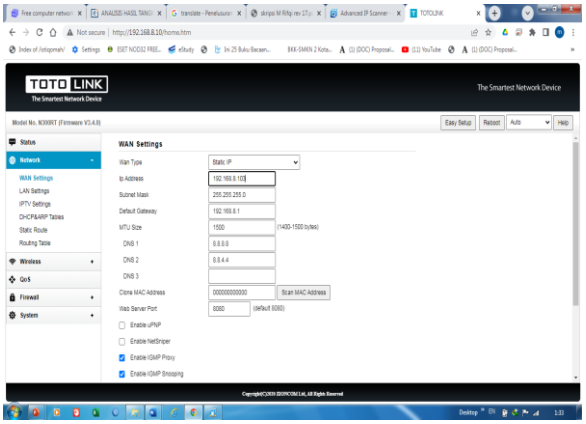
Pada Gambar 5 terdapat banyak percobaan login ke server utama secara terus menerus menggunakan ip public yang sama dan dalam waktu yang berdekatan, dimana ini hanya bisa di lakukan menggunakan Brute Force. Pada Gambar 6 peneliti melakukan percobaan penyerangan secara langsung menggunakan tool Hydra Pada Kali Linux, dimana hal ini berhasil dan terdapat pesan yang sama pada log system mikrotik. Dalam penyerangan ini menyebabkan cpu dan memori menjadi naik 37% hal ini akan dapat mengurangi kualitas server atau bahkan dapat terjadi deadlock pada server.



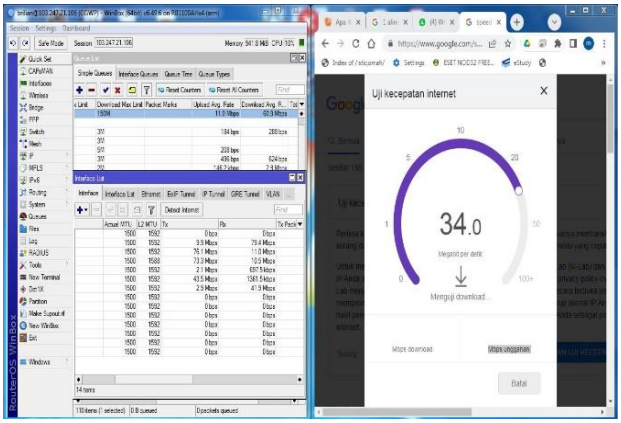
Gambar 7.Client Illegal dengan IP tidak terpakai



Gambar 8. Penggunaan IP Scanner



Gambar 9. Modem menggunakan ip ilegal



Gambar 10 IP Client Ilegal Mendapatkan Akses Internet

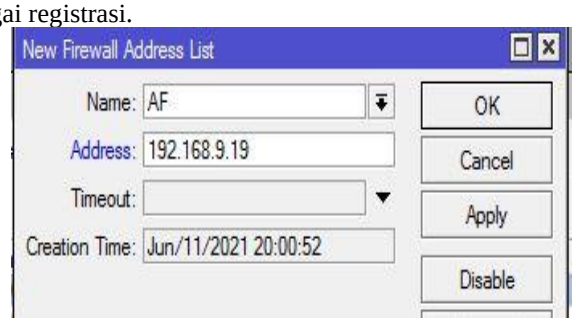
Pada Gambar 7 terdapat IP illegal yang digunakan oleh client, dimana hal ini di temukan pada IP ARP pada Mikrotik, IP Tersebut bisa didapatkan menggunakan IP Scanning seperti pada gambar 8. Pada gambar 9 peneliti melakukan percobaan menggunakan IP Address yang tidak terdaftar di barokah.net, dimana perangkat ini tetap mendapatkan akses internet dan tanpa adanya limitasi bandwith. Hal ini akan menyebabkan bandwith yang dimiliki oleh Barokah.net menjadi padat dan client tidak mendapatkan bandwith yang maksimal seperti yang terdapat pada gambar 10, hal ini akan sulit terdeteksi oleh pemilik karena di barokah.net belum ada karyawan yang dapat memantau server.

Berdasarkan literatur dan pengalaman yang pernah penulis dapatkan hal diatas dapat ditangani dengan merancang sistem keamanan jaringan yang ada di Barokah.Net dengan metode IP Filtering dan port Knocking untuk lebih memperkuat keamanan jaringan pada server Barokah.net.

HASIL DAN PEMBAHASAN

Pembuatan Address List

Address list akan dipergunakan untuk grouping ip address yang diperbolehkan untuk mendapat akses internet dari server dan sekaligus sebagai registrasi.

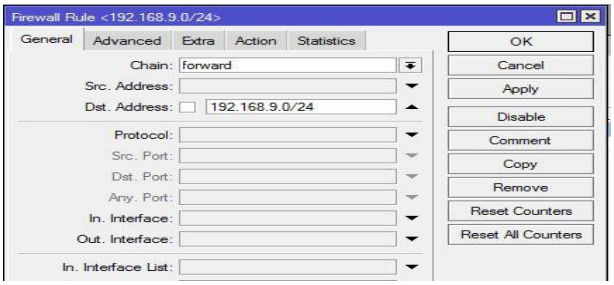


Gambar 11. Address List

Perintah ini akan pergunakan untuk mendaftarkan alamat ip yang akan di gunakan oleh client agar bisa mendapatkan akses internet.

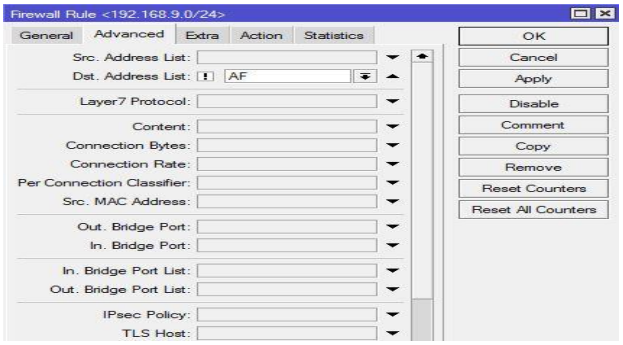
Pembuatan Filter Rule

Filter rule akan digunakan sebagai sistem yang melakukan bloking pada ip network yang sudah di tentukan sebagai client, dan akan melakukan pengecualian bloking terhadap ip address yang sudah terdaftar pada address list yang sebelumnya dibuat. Pengaturan di bawah untuk menambahkan daftar ip network local yang akan di blok dan melakukan pengecualian bloking pada ip yang sudah terdaftar pada address list yang sebelumnya di buat.



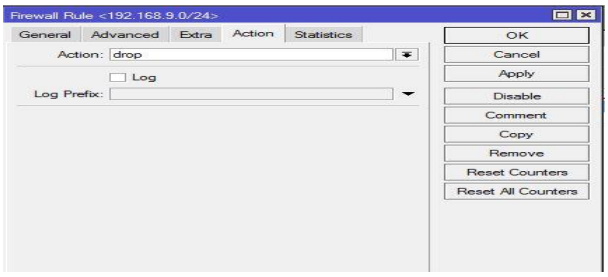
Gambar 12. IP Yang Di Bloking Dari DST

Perintah ini akan pergunakan untuk menambahkan IP Address yang akan diblok pada setiap data yang masuk dari ip yang didaftarkan.



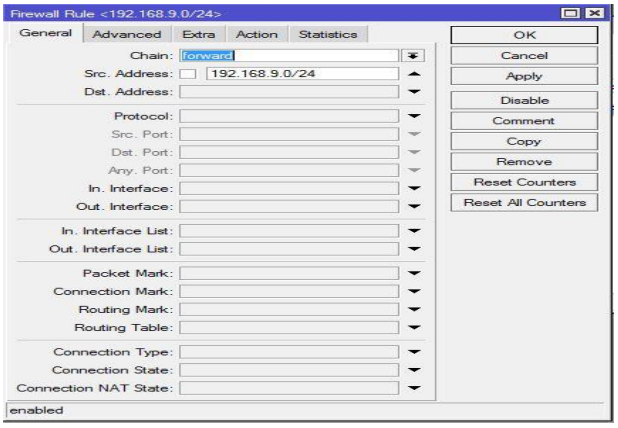
Gambar 13. Daftar Pengecualian Dari DST

Perintah ini akan dipergunakan untuk melakukan pengecualian bloking pada setiap data yang masuk dari ip yang terdapat di Address List.



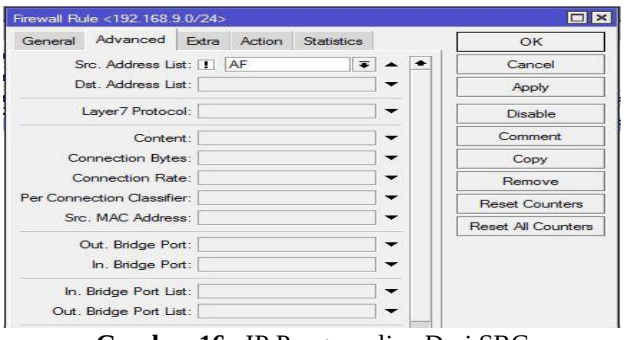
Gambar 14. Perintah Bloking Pada DST

Perintah ini akan dipergunakan untuk melakukan bloking pada setiap data yang masuk dari ip yang tidak terdapat di Address List.



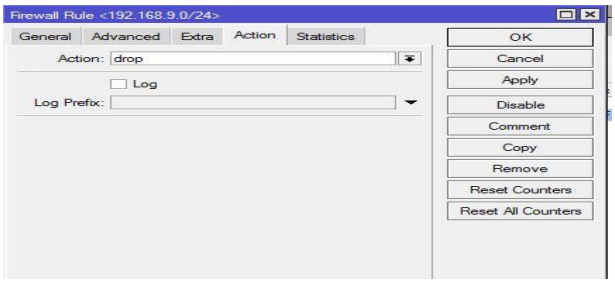
Gambar 15. IP Yang Di Bloking Dari SRC

Perintah ini akan pergunakan untuk menambahkan IP Address yang akan diblok pada setiap data yang keluar dari ip yang di daftarkan.



Gambar 16. IP Pengecualian Dari SRC

Perintah ini akan dipergunakan untuk melakukan pengecualian bloking pada setiap data yang keluar dari ip yang terdapat di Address List.

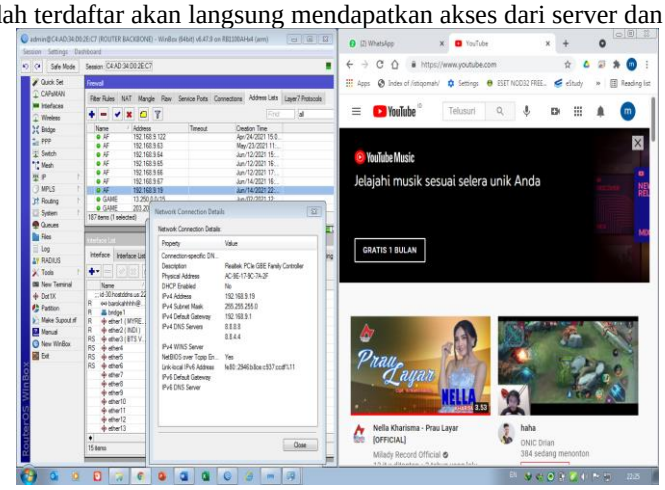


Gambar 17. *Perintah Bloking Pada SRC*

Perintah ini akan dipergunakan untuk melakukan bloking pada setiap data yang keluar dari ip yang tidak terdapat di Address List.

Hasil Perangkat Yang Sudah Terdaftar

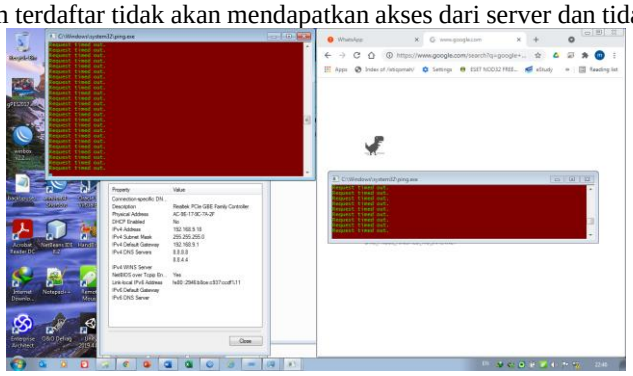
Perangkat yang sudah terdaftar akan langsung mendapatkan akses dari server dan dapat mengakses internet.



Gambar 18. Tampilan Perangkat Yang Mendapatkan Akses

Hasil Perangkat Yang Belum Terdaftar

Perangkat yang belum terdaftar tidak akan mendapatkan akses dari server dan tidak dapat mengakses internet.



Gambar 19. Tampilan Perangkat Yang Belum Terdaftar

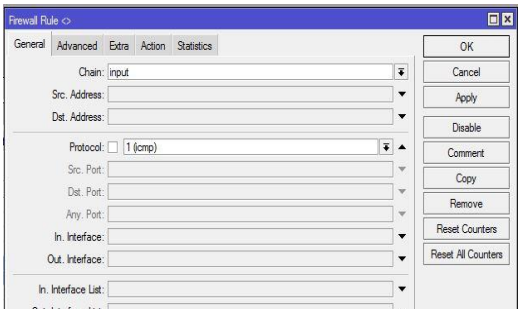
Penerapan Rancangan Port Knocking

Dalam mengimplementasikan Metode Port Knocking di perlukan penerapan pada Firewall Filter Rule dan Address List, dimana hal ini yang akan menjalankan metode Port Knocking pada sistem Server Mikrotik. Dalam penerapan rancangan Port Knocking adalah sebagai berikut :.

Filter Rule Input

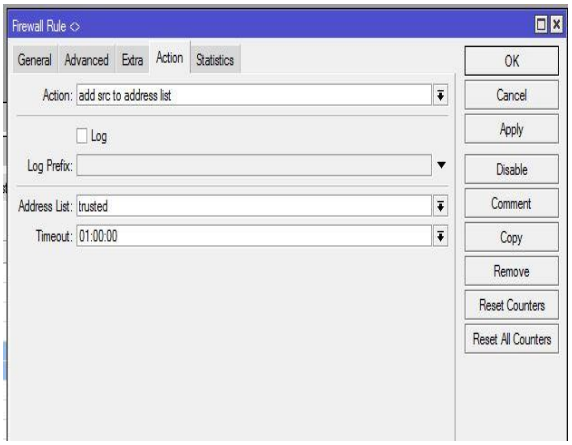
Filter rule input akan pergunakan sebagai sistem yang melakukan grouping IP Address secara otomatis ke dalam address list yang di perbolehkan untuk mengakses server utama.

Pengaturan dibawah di pergunakan untuk menerima packet ICMP yang harus di kirimkan oleh perangkat yang akan mengakses server utama.



Gambar 20. Pengaturan filter rule general

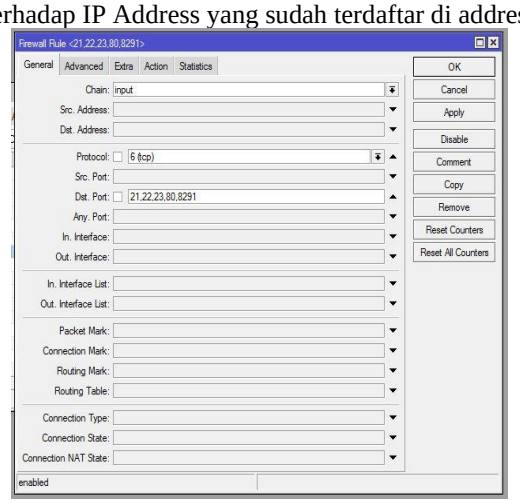
Pengaturan dibawah di pergunakan untuk menambahkan IP Address yang di miliki perangkat ke address list yang di perbolehkan untuk masuk ke dalam server utama.



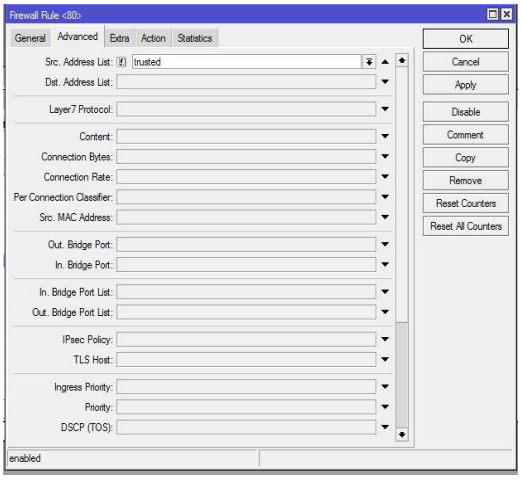
Gambar 21. Pengaturan filter rule action

Filter Rule Drop

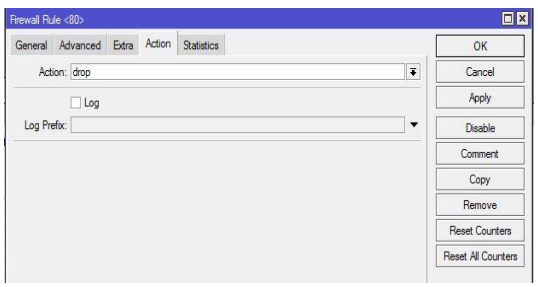
Filter rule drop akan pergunakan sebagai sistem yang melakukan blokir terhadap port yang akan di tutup dan melakukan pengecualian terhadap address list yang di buat sebelumnya. Pada pengaturan ini jika menerima packet TCP dari port 80 akan di lakukan blokir ke IP Address yang mengirim packet tersebut dan melakukan pengecualian terhadap IP Address yang sudah terdaftar di address list.



Gambar 22. Pengaturan filter rule general



Gambar 23. Pengaturan filter rule advanced

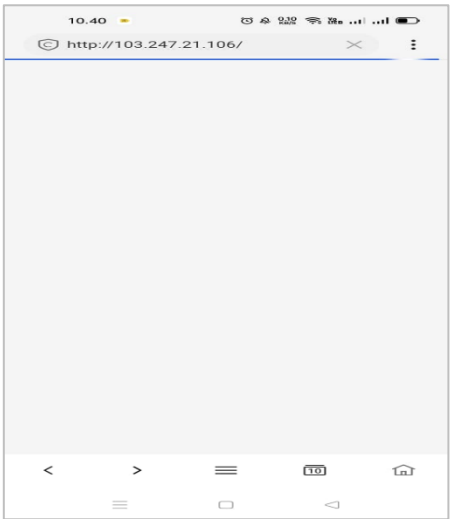


Gambar 24. Pengaturan filter rule action

Hasil Pengujian

Dalam melakukan pengujian peneliti menggunakan login langsung dengan memanggil IP server melalui browser, winbox, putty dan menggunakan metode Brute Force di Kali Linux dengan tool Hydra.

Perangkat yang sudah mengirimkan packet ICMP akan mendapatkan akses ke server utama yang kemudian akan melakukan login. Jika perangkat belum mengirimkan packet ICMP ke server maka halaman login server tidak akan muncul atau akan mendeteksi Network error.

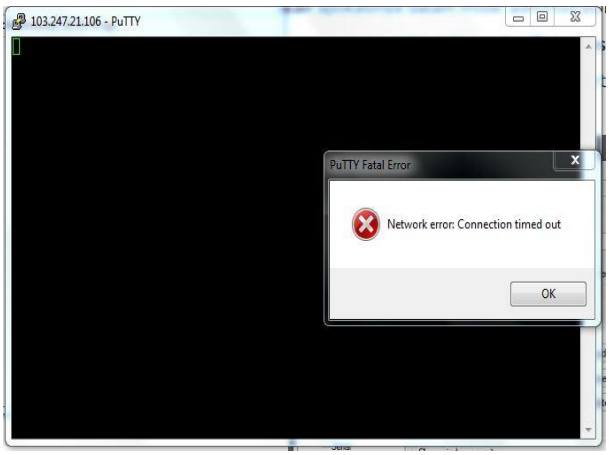


Gambar 25. Perangkat belum mengirimkan packet ICMP

Gambar 26. Perangkat sudah mengirimkan packet ICMP

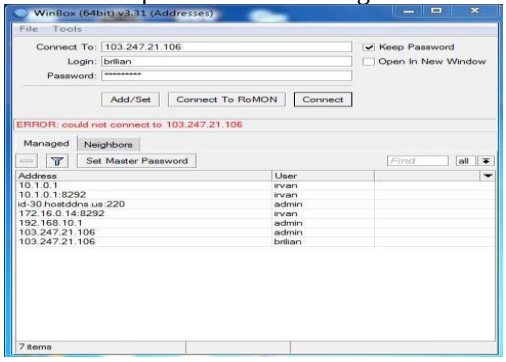
Pada percobaan menggunakan aplikasi Putty dengan memanggil IP Public server melalui port 22, dalam percobaan ini perangkat mendapatkan pesan Network Error karena aplikasi putty tidak dapat menemukan Port 22 yang sudah di tutup oleh Port Knocking.

Gambar 27. Percobaan login menggunakan Putty



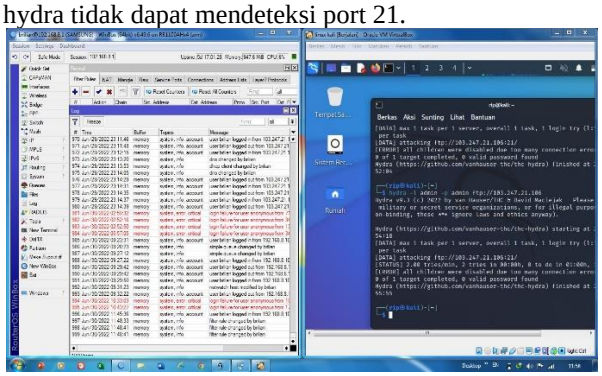
Gambar 28. Pesan error pada percobaan login menggunakan putty

Pada percobaan menggunakan aplikasi Winbox dengan memanggil IP Public server dan mengisi user dan password login, dalam percobaan ini perangkat mendapatkan pesan Network Error karena aplikasi Winbox tidak dapat menemukan Port 8291 yang sudah di tutup oleh Port Knocking.



Gambar 29. Pesan error pada percobaan login menggunakan Winbox

Pada penyerangan Brute force menggunakan tool Hydra pada kali linux tidak dapat melakukan penyerangan terhadap port 21 Mikrotik, hal ini di karenakan pada Kali linux belum melakukan pengiriman paket ICMP pada Router Mikrotik sehingga tool hydra tidak dapat mendeteksi port 21.



Gambar 30. Penyerangan menggunakan Brute Force

Evaluasi

Setelah di lakukan implementasi metode IP Filtering dan Port Knocking pada sistem yang berjalan terdapat kelebihan dan kekurangan yaitu :

Kelebihan

1. Metode IP Filtering dapat memblokir ip address yang tidak terdaftar dari semua permintaan akses ke server.
2. Metode Port Knocking dapat menutup semua port yang di gunakan dalam penyerangan Brute force, tetapi semua port yang ditutup tetap dapat di akses menggunakan autentikasi khusus yaitu dengan mengirimkan paket icmp berupa ping ker server.

Kekurangan

1. Metode IP Filtering dan Port Knocking tidak dapat mengidetifikasi perangkat yang melakukan penyerangan ke server, sehingga tidak dapat di lakukan tindakan khusus kepada perangkat yang melakukan penyerangan.
2. Autentikasi yang di buat pada IP Filtering masih terlalu mudah untuk di identifikasi.

Kesimpulan

Dari hasil rancangan sistem keamanan jaringan di Barokah.net maka dapat di simpulkan sebagai berikut :

1. Dalam menganalisa keamanan jaringan pada server barokah.net penulis menggunakan metode NDLC, dimana dalam masalah ini terdapat 2 metode penyerangan yaitu metode Brute Force dan IP Scanning
2. System IP Filtering dan Port Knocking meningkatkan keamanan jaringan local maupun public terutama dalam memfilter ip address ilegal yang mencoba mendapatkan akses dari server utama.

DAFTAR PUSTAKA

Kurniawan, Rudi. 2016. *Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode Ndlc (Network Development Life Cycle) Pada Bpu Bagas Raya Lubuklinggau.* Sumatra Selatan : Jurnal Ilmiah Betrik

Novaliano, Yoel. 2020. *Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode Ndlc (Network Development Life Cycle) Pada Bpu Bagas Raya Lubuklinggau. Bekasi* : Repository USNI.

Christian, Yefta. 2019. Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan Metode Port Knocking dan Action Tarpit pada Router Mikrotik. Batam : Telecomatics

Ari Muzakir dan Maria Ulfa. 2019. *Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan. Palembang* : Jurnal Simetris

Yudi Mulyanto, M. Julkarnain, Dan Aldela Jabi Afahar. 2021. Implementasi *Port Knocking* Untuk Keamanan Jaringan Smkn 1. Sumbawa Besar : Jinteks

Nanang Budiansyah, I Made Widiarta , dan Yunanri. 2020. Analisis Perbandingan Performa Free radius Dan User manager Pada Mikrotik. Sumbawa : Jinteks

Santoso, Joko Dwi. 2019. Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. Yogyakarta : Infosjurnal

Iwan Sofana dan Rifkie Primartha. 2019. Network Security dan Cyber Security. Bandung : Informatika Bandung

Towidjojo, Rendra. 2016. Mikrotik Kung Fu Kitab 1. ISBN 978-602-0823- 12-6 . Jakarta : Jasakom