Penerbit ADM RUMAH PENGETAHUAN
Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi

Hotspot Network Security System From Brute Force Attack Using Pfsense External Firewall (Case Study of Wifi-Ku.Net Hotspot)

Sistem Keamanan Jaringan Hotspot Dari Serangan Brute Force Menggunakan Firewall Eksternal Pfsense (Studi Kasus Hotspot Wifi-Ku.Net)

Angga Syaputera [1)]; Riska [2)]; Yessi Mardiana [3)]

[1)] ***Study Program of Computer Systems Engineering Faculty Of* Computer science Universitas Dehasen Bengkulu**
[2)] **Department of Computer Systems Engineering Faculty Of Computer science Uni*versitas Dehasen Bengkulu***
Email: [1)] Anggasyaputera@gmail.com

How to Cite :
Syaputera, A., Riska. R., Mardiana, Y., (2023).Sistem Keamanan Jaringan Hotspot Dari Serangan Brute Force. Jurnal Komputer, Informasi dan Teknologi, 3 (1). DOI: https://doi.org/10.53697/jkomitek.v3i1

ARTICLE HISTORY
Received [28 Mei 2023]
Revised [12 Juni 2023]
Accepted [13 Juni 2023]

KEYWORDS
Pfsense External Firewall, Brute Force, Mikrotik.

ABSTRAK

Banyak aktivitas yang sering dilakukan di jaringan internet yang tanpa disadari penggunanya mengancam privasi mereka. Dari beberapa serangan cybercrime salah satunya adalah metode brute force, dimana metode brute force adalah metode yang bertujuan untuk mendapatkan hak akses masuk ke suatu sistem secara paksa dengan mencoba semua kemungkinan username dan password yang sudah disiapkan attacker dalam sebuah wordlist.Tujuan dari penelitian ini adalah untuk mengetahui bagaimana cara mengimplemetasikan sistem keamanan jaringan hotspot dari serangan brute force menggunakan firewall eksternal PFSense pada hotspot wifi-ku.net.Metode penelitian yang digunakan adalah dengan menggunakan metode penelitian eksperimen yaitu menguji sebuah variabel terhadap variabel lain dengan objektif, sitematis dan terkontrol dengan memprediksi sebab dan akibat dari permasalahan yang penulis teliti terhadap sistem keamanan jaringan hotspot dari serangan brute force menggunakan firewall eksternal PFsense.Hasil dari penelitian yang telah dilakukan sebelum menerapkan firewall eksternal Pfsense didapatkan brute forece berhasil masuk kedalam router mikrotik, dan setelah menerapkan firewall eksternal Pfsense penyerangan dengan metode brute force sudah tidka bisa masuk lagi kedalam router mikrotik karena firewall eksternal Pfsense melakukan pemblokiran terhadap serangan dari brute force.

ABSTRACT

Many activities that are often carried out on the internet network that users without realizing threaten their privacy. From the several cybercrime attacks, one of them is the brute force method, where the brute force method is a method that aims to gain access rights to enter a system by force by trying all possible usernames and passwords that the attacker has prepared in a wordlist. The purpose of this study is to find out how to implement a hotspot network security system from brute force attacks using PFSense external firewall on a wifi-ku.net hotspot. The research method used is experimental research methods, namely testing a variable against other variables objectively, systematically and controlled by predicting the causes and consequences of the problems that the writer examine on the hotspot network security system from brute force attacks using PFsense external firewall. The results of the research that was carried out before applying Pfsense external firewall, it is found that the brute force

successfully entered Mikrotik router, and after applying Pfsense external firewall attack with Brute Force method is no longer able to enter Mikrotik router because Pfsense's external firewall blocked attacks from brute force.

PENDAHULUAN

Sejak wabah virus Covid-19 semua kegiatan sehari-hari masyarakat seperti sekolah, bekerja, dan bersosialisasi dilakukan dari rumah menggunakan jaringan internet sebagai sarana komunikasi menggantikan kegiatan tatap muka. Namun demikian semakin meningkatnya pengguna jaringan internet maka semakin besar pula peluang terjadinya ancaman serangan cybercrime atau kejahatan dunia maya yang merugikan pengguna internet lain bahkan pihak intansi pemerintah, rumah sakit, sekolah dan penyedia jasa jaringan internet itu sendiri tidak luput dari serangan cybercrime. Banyak aktivitas yang sering dilakukan di jaringan internet yang tanpa disadari penggunanya mengancam privasi mereka. Dari beberapa serangan cybercrime salah satunya adalah metode brute force, dimana metode brute force adalah metode yang bertujuan untuk mendapatkan hak akses masuk ke suatu sistem secara paksa dengan mencoba semua kemungkinan username dan password yang sudah disiapkan attacker dalam sebuah wordlist dengan bantuan software seperti THC Hydra, Medusa dan lain-lain. Wifi-ku.net merupakan jasa layanan internet rumah berskala kecil berbasis hotspot yang terletak di Desa Penum Kecamatan Taba Penanjung Kabupaten Bengkulu Tengah. wifi-ku.net sudah berjalan 3 tahun dengan rata-rata user voucher online 10 orang setiap harinya termasuk 5 pelanggan tetap bulanan. Meningkatnya kebutuhan akses internet pemilik usaha kecil hotspot wifi-ku.net mengkhawatirkan akan terjadinya penyerangan brute force yang berasal dari jaringan lokal yang berakibat terganggunya kualitas layanan koneksi internet.

Berdasarkan penelitian yang dilakukan oleh Alfarizi (2020) yang berdujul "implementasi keamanan jaringan pada router mikrotik terhadap serangan brute force pada server jurusan teknik komputer" dengan hasil. Didapatkan persentase CPU dan memori yang sangat besar pada Mikrotik Router OS yang berdampak pada kinerja dari Mikrotik Router OS tersebut seperti kesulitan untuk menjalankan tugasnya dan trafik menjadi lambat.Berdasarakan uaraian diatas, solusi yang dapat dilakukan adalah dengan menerapkan sistem keamanan firewall menggunakan sistem operasi Pfsense. Pencegahan dapat dilakukan dengan memberikan jeda waktu ketika beberapa kali penyerang salah memasukkan username dan password pada saat login kedalam router. Kemudian melakukan dropping connection terhadap IP penyerang kedalam sebuah address list. Serta menerapkan Pfsense sebagai firewall eksternal yang befungsi sebagai firewall koneksi yang datang dari jaringan lokal ke server wifi-ku.net.

LANDASAN TEORI

Sistem

Menurut Edhy dalam Hasbiyallah dan Jakaria (2018 : 62), Sistem secara umum, sistem dapat didefinisikan sebagai kumpulan hal atau kegiatan atau elemen atau subsistem yang saling bekerja sama atau yang dihubungkan dengan cara tertentu sehingga membentuk satu kesatuan untuk melaksanakan suatu fungsi guna mencapai tujuan.Sistem adalah "sekelompok dua atau lebih komponen-komponen yanga saling berkaitan (subsistem-subsistem yang bersatu untuk mencapai tujuan yang sama)" (Mulyadi dalam Asmara, 2016: 82).Pada intinya, sebuah sistem adalah sekumpulan entitas (hardware, brainware, software) yang saling berinteraksi, bekerjasama dan berkolaborasi untuk mencapai tujuan tertentu.

Keamanan Jaringan

Menurut Amarudin dan Ulum (2018: 72), Keamanan jaringan merupakan salah satu hal terpenting dalam implementasi jaringan komputer. Tidak sedikit jaringan komputer yang mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer. Dikarenakan kelalaian tersebut sehingga dapat membuka bagi para hacker untuk meretas dan merusak jaringan yang dibangun tersebut. Keamanan jaringan atau sistem

informasi adalah "proses dimana aset informasi dilindungi mencakup perlindungan atas kerahasiaan, integritas, dan ketersediaan aset informasi tersebut" (Alabady dalam Bustami dan Bahri, 2020: 61). Menurut Munawar dan Putri (2020 : 15), Keamanan jaringan komputer mengacu pada perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer agar tidak dihancurkan, diubah, atau lubang keamanan karena alasan kecelakaan atau berbahaya, sehingga sistem komputer terus beroperasi dengan handal, serta layanan komputer juga teratur.

Menurut Mutaqin (2016 : 3), Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah untuk mengakses setiap bagian dari sistem jaringan komputer. Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.Dapat disimpulkan bahwa keamanan jaringan adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan sehingga sistem komputer terus beroperasi dengan handal.

Hotspot

Menurut Iwan dalam Purwanto (2015 : 21), Hotspot adalah atau area hotspot adalah tempat khusus yang disediakan untuk mengakses internet mengunakan peralatan Wi-fi. Umumnya layanan hotspot bersifat gratis. Dengan berbekal laptop atau PDA maka koneksi internet dapat dilakukan secara cuma-cuma. Biasanya pengguna terlebih dulu harus melakukan registrasi kepenyedia layanan hotspot untuk mendapatkan login dan password. Kemudian pengguna dapat mencari area hotspot, seperti pusat perbelanjaan, kafe, hotel, kampus, sekolahan, bandara udara, dan tempat-tempat umum lainnya. Proses otentikasi dilakukan ketika browser diaktifkan.

Menurut Qirom dan Sungkar (2017 : 16), Hotspot adalah area dimana seorang client dapat terhubung dengan internet secara wireless (nirkabel atau tanpa kabel) dari PC, Laptop, notebook ataupun gadget seperti handphone dalam jangkauan radius kurang lebih beberapa ratus meteran tergantung dari kekuatan frekuensi atau signal nya.Hotspot adalah "suatu sistem yang memberikan fitur autentikasi pada user yang akan mengakses suatu jaringan. Bila user tersebut ingin terhubung ke jaringan tersebut maka user tersebut harus memasukkan username dan password terlebih dahulu" (Fitria dan Prihanto, 2018: 23).Dapat disimpulkan bahwa Hotspot adalah lokasi fisik tempat orang dapat mengakses Internet, biasanya menggunakan Wi-Fi, melalui jaringan area lokal nirkabel (WLAN) dengan router yang terhubung ke penyedia layanan Internet (ISP).

Brute Force

Menurut Santoso dkk (2016 : 2), Brute force adalah sebuah pendekatan yang langsung (straight forward) untuk memecahkan suatu masalah, biasanya didasarkan pada pernyataan masalah (problem statement) dan definisi konsep yang dilibatkan. Algoritma brute force memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas (obvious way). Menurut Sarno dalam Pratiwi dkk (2016 : 120), Algoritma brute force adalah algoritma yang digunakan untuk mencocokan pattern dengan semua teks antara 0 dan n-m untuk menemukan keberadaan Pattern teks. Algoritma brute force memecahkan masalah dengan sangat sederhana, langsung, dan jelas. Algortima brute-force merupakan suatu teknik yang biasa digunakan bila si penyusun algoritma lebih mempertimbangkan memperoleh solusi dari problem secara langsung apa adanya.Menurut Syaifuddin dkk (2018 : 348), Serangan brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas. Penyelesaian permasalahan password cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan password dengan masukan karakter dan panjang password tertentu tentunya dengan banyak sekali kombinasi password.

Mikrotik

Mikrotik RB750r2 juga merupakan router berukuran kecil dengan harga terjangkau yang dapat digunakan untuk koneksi jaringan internet di rumah, warnet, atau kantor. Kelebihan Mikrotik mudah di kehandalan fitur, harga relatif murah, lebih irit listrik, serta ukuran yang lebih kecil.

Menurut Hardana dalam Syaifudin dan Assegaff (2020 : 50), Mikrotik adalah sebuah perusahaan yang bergerak di bidang produksi perangkat keras (hardware) dan perangkat lunak (Software) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan router dan sistem ISP (Internet Service Provider) nirkabel. Mikrotik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer etwork yang handal, mencakup berbagai fitur yang dibuat untuk IP network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot. Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun. RouterBoard adalah router embedded produk dari Mikrotik. Routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash. Routerboard menggunakan OS RouterOS yang berfungsi sebagai router jaringan, bandwidth management, proxy server, DHCP, DNS server dan bisa juga berfungsi sebagai hotspot server. Selain itu, alat ini dapat juga digunakan untuk routing statik, routing dinamik, hotspot, VPN, DHCP server, DNS cahche,web proxy, dan lain sebagainya. Cara konfigurasi routerborad ini sangat gampang, bahkan lebih gampang dari pada router lain, semisal Cisco atau juniper.

Dapat disimpulkan bahwa Mikrotik merupakan sistem operasi Linux base yang digunakan untuk network router. Dengan fitur seperti IP Network jaringan wireless, provider warnet dan hotspot. Sistem administrasinya bisa diterapkan dengan menggunakan Windows Application (Winbox).

METODE PENELITIAN

Metode Analisis

Metode yang digunakan dalam penyusunan proposal skripsi ini adalah dengan menggunakan metode penelitian eksperimen yaitu menguji sebuah variabel terhadap variabel lain dengan objektif, sitematis dan terkontrol dengan memprediksi sebab dan akibat dari permasalahan yang penulis teliti terhadap sistem keamanan jaringan hotspot dari serangan brute force menggunakan firewall eksternal Pfsense. Serta dilakukan pembahasan perancangan dan pengimplementasian firewall Pfsense sebagai sistem keamanan dari serangan brute force.

Perancangan pengujian dilakukan setelah instalasi dan konfigurasi hardware dan software sistem keamanan jaringan hotspot wifi-ku.net. Adapun beberapa hal yang akan diuji pada sistem keamanan jaringan hotspot wifi-ku.net terhadap serangan brute force adalah sebagai berikut :

Tabel 1 Rencana pengujian

NO.	Jenis Pengujian	Kriteria	Hasil	Keterangan
1.	Serangan *brute force* menggunakan *software TCH Hydra*	Pengujian dilakukan kepada jaringan *wifi-ku.net* yang belum menggunakan *Firewall Pfsense*		
		Pengujian dilakukan kepada jaringan *wifi-ku.net* yang telah menggunakan *Firewall Pfsense*		
2.	Serangan *brute force* menggunakan *software Medusa*	Pengujian dilakukan kepada jaringan *wifi-ku.net* yang belum menggunakan *Firewall Pfsense*		
		Pengujian dilakukan kepada jaringan *wifi-ku.net* yang telah menggunakan *Firewall Pfsense*		

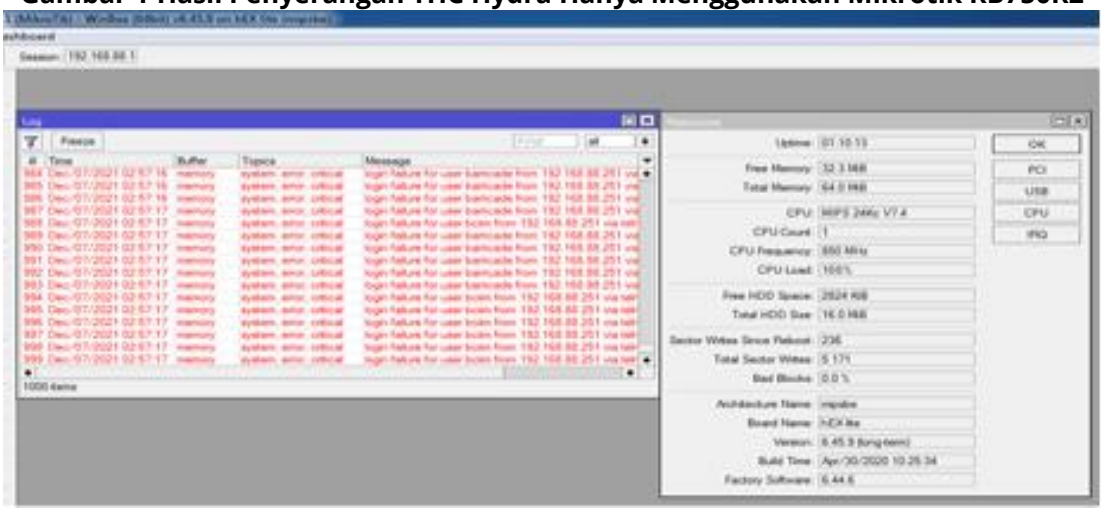
HASIL DAN PEMBAHASAN

Hasil

Hasil Pengujian sistem keamanan jaringan hotspot dari serangan brute force yang hanya menggunakan Mikrotik RB750R2 dan setelah diterapkan firewall eksternal Pfsense pada hotspot wifi-ku.net adalah sebagai berikut:

1. Penyerangan menggunakan THC Hydra pada hotspot wifi-ku.net yang hanya menggunakan Mikrotik RB750R2

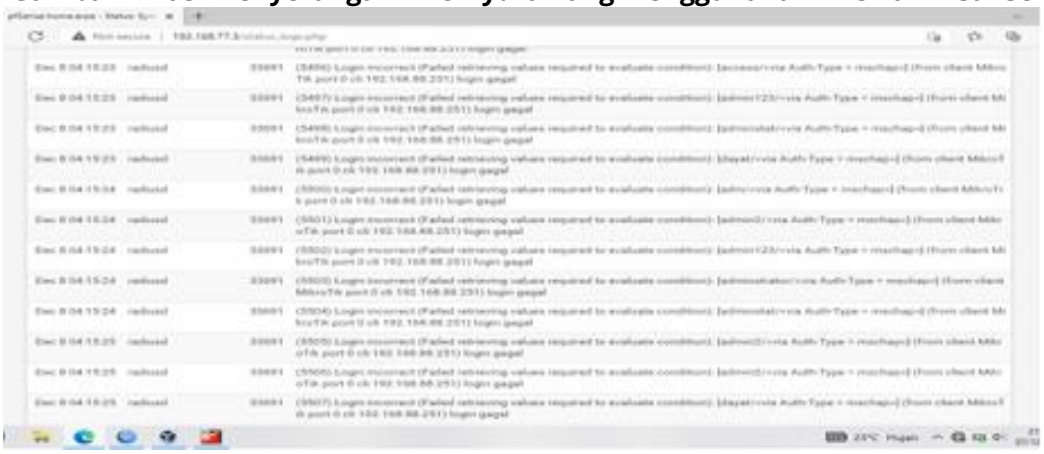
Gambar 1 Hasil Penyerangan THC Hydra Hanya Menggunakan Mikrotik RB750R2



Pada gambar 3 diatas bisa dilihat CPU pada mikrotik meningkat dan pada log mikrotik juga mencatat serangan yang telah dilakukan penulis menggunakan THC Hydra dan penyerangan menggunakan THC Hydra berhasil masuk pada sistem yang hanya menggunakan Mikrotik RB750R2.

2. Penyerangan menggunakan THC Hydra pada hotspot wifi-ku.net yang telah diterapkan firewall eksternal Pfsense

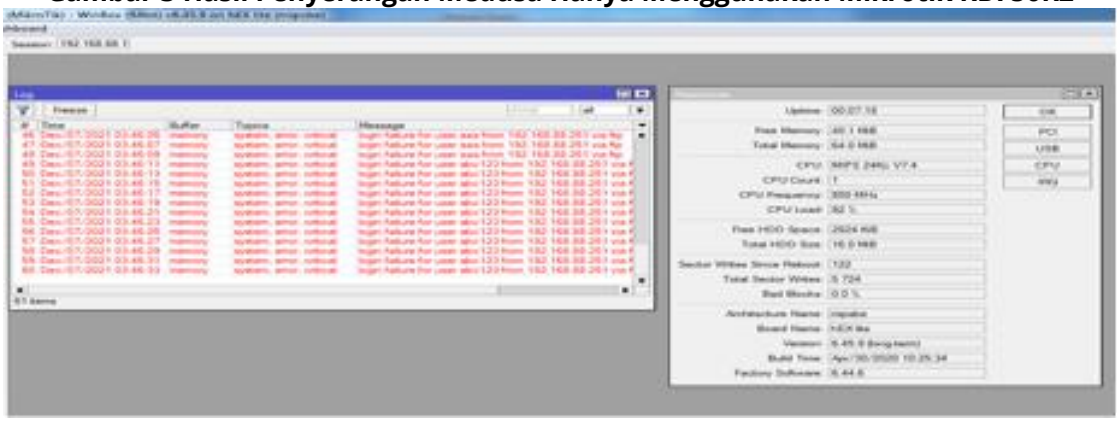
Gambar 2 Hasil Penyerangan THC Hydra Yang Menggunakan Firewall Pfsanse



Bisa dilihat pada gambar 4 semua serangan menggunakan THC Hydra semuanya ditampung oleh firewall Pfsanse dan CPU pada Mikrotik RB750R2 tidak mengalami peningkatan dan serangan menggunakan THC Hydra tidak bisa masuk pada sistem hotspot wifiiku.net.

3. Penyerangan menggunakan Medusa pada hotspot wifi-ku.net yang hanya menggunakan Mikrotik RB750R2

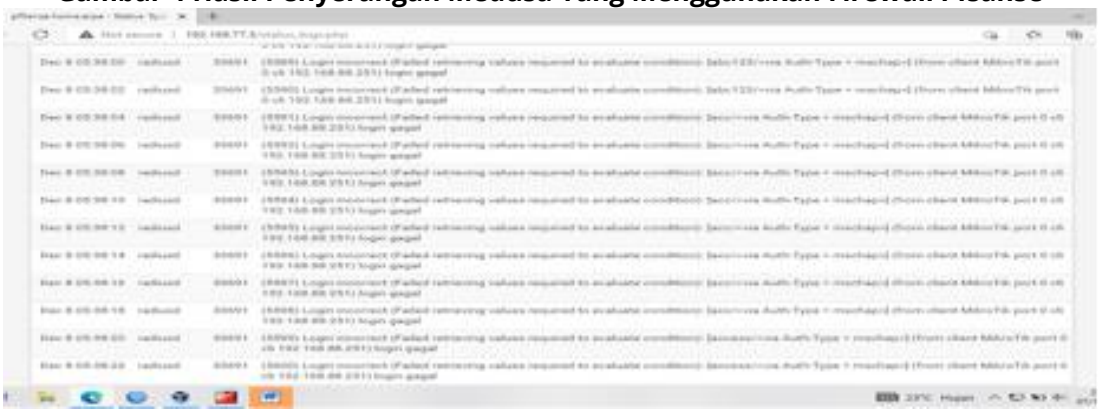
Gambar 3 Hasil Penyerangan Medusa Hanya Menggunakan Mikrotik RB750R2



Pada gambar 5 diatas bisa dilihat CPU pada mikrotik meningkat tetapi secara bertahap dan pada log mikrotik juga mencatat serangan yang telah dilakukan penulis menggunakan Medusa dan penyerangan menggunakan Medusa berhasil masuk pada sistem yang hanya menggunakan Mikrotik RB750R2.

4. Penyerangan menggunakan Medusa pada hotspot wifi-ku.net yang telah diterapkan firewall eksternal Pfsense

Gambar 4 Hasil Penyerangan Medusa Yang Menggunakan Firewall Pfsanse



Bisa dilihat pada gambar 6 semua serangan menggunakan Medusa semuanya ditampung oleh firewall Pfsanse dan CPU pada mikrotik RB750 R2 tidak mengalami peningkatan dan serangan menggunakan Medusa tidak bisa masuk pada sistem hotspot wifiiku.net.

Pembahasan

Pada bagian ini akan dibahas bagaimana cara mengimplementasikan sistem keamanan jaringan hotspot dari serangan brute force menggunakan Mikrotik RB750R2 dan eksternal firewall eksternal Pfsense.

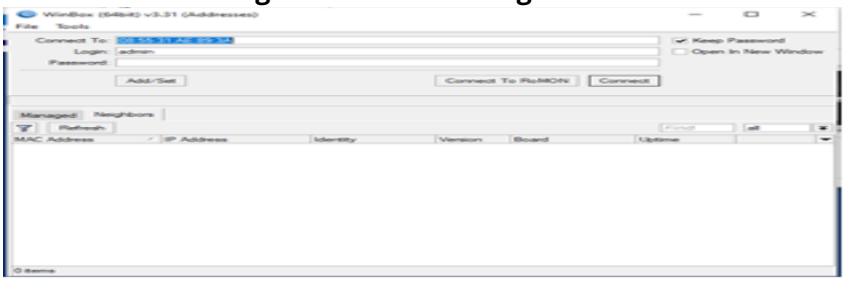
Instalasi dan Konfigurasi

Langkah-langkah instalasi dan Konfigurasi sistem keamanan hotspot dari serangan brute force menggunakan Mikrotik RB750R2 dan eksternal firewall eksternal Pfsense adalah sebagai berikut.

Konfigurasi Mikrotik RB750R2

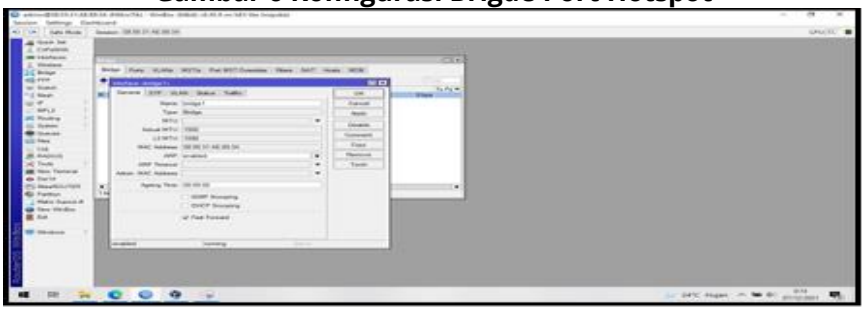
Adapun langkah awal dalam Konfigurasi Mikrotik RB750R2 adalah dengan menghubungkan port 2router mikotik ke laptop dengan kabel lan kemudian buka software Winboxpada form Connect Tomasukkan mac address yang terdapat di belakang router mikrotikRB75R2 Formlogin diisi admin dan password dikosongkan kemudian klik Connect.

Gambar 5 Konfigurasi Mikrotik dengan software Winbox



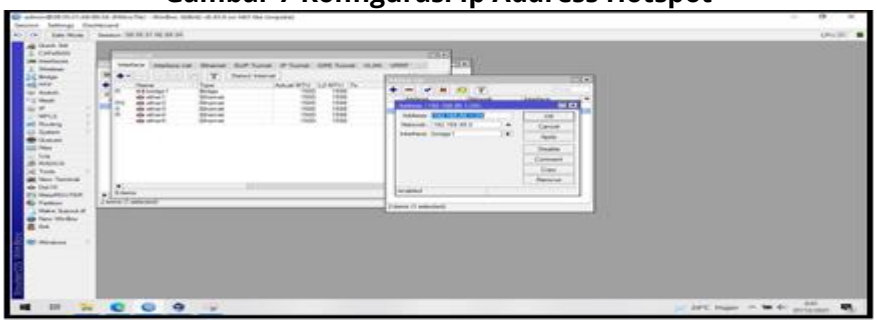
Selanjutnya lakukan setup Brigde pada port 2 dan 3 yang nantinya akan digunakan sebagai jalur hotspot klik brigde kemudian klik tanda tambah name default (bridge1) saja kemudian apply dan klik ok, settingan bridge digunakan untuk memaksimalkan penggunaan port pada mikrotik apabila di diperlukan layanan hotspot melalui kabel Lan dan access point.

Gambar 6 Konfigurasi Brigde Port Hotspot



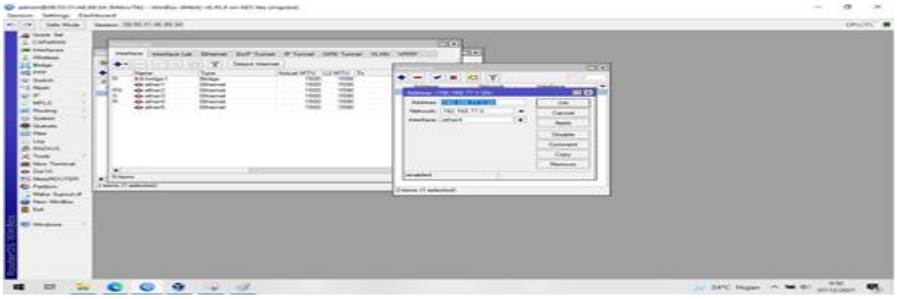
Langkah berikutnya adalah pada bagian tab ports menu brigde klik tanda tambah kemudian interface pilih ethernet2 dan Bridge pilih brigde1 klik apply dan ok. Kemudian klik tambah kembali interface diisikan dengan ethernet3 Brige diisikan dengan bridge1 klik apply dan ok. Sekarang port ethernet2 dan ethernet3 sudah bisa kita setting 1 segment ip address yang nanti nya digunakan untuk layanan hotspot.Berikutnya menambahkan Ip address pada port yang sudah kita gabungkan sebelumnya dengan klik tab IP kemudian Addresslist klik tambah kemudian isi pada kolom address 192.168.88.1/24 dan network di isi dengan 192.168.88.0 setelah itu interface pilih bridge1 klik apply dan ok.

Gambar 7 Konfigurasi Ip Address Hotspot



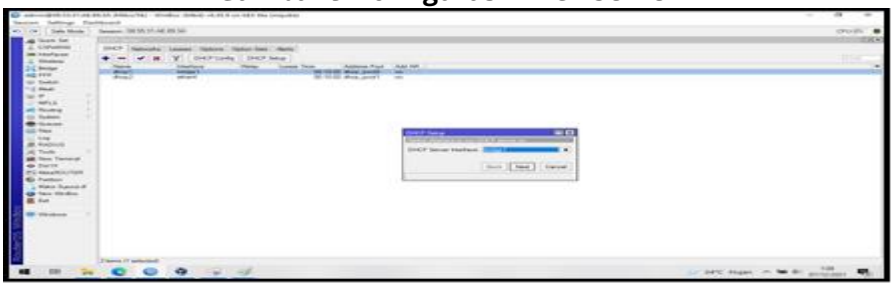
Selanjutnya menambahkan IP address pada port ethernet4 yang nanti akan digunakan jalur ekstenal firewall eksternal Pfsense klik tambah Address masukkan address 192.168.77.1/24network 192.168.77.0 interface ether4 klik apply dan ok.

Gambar 8 Konfigurasi IP Address Jalur Eksternal Firewall eksternal Pfsense



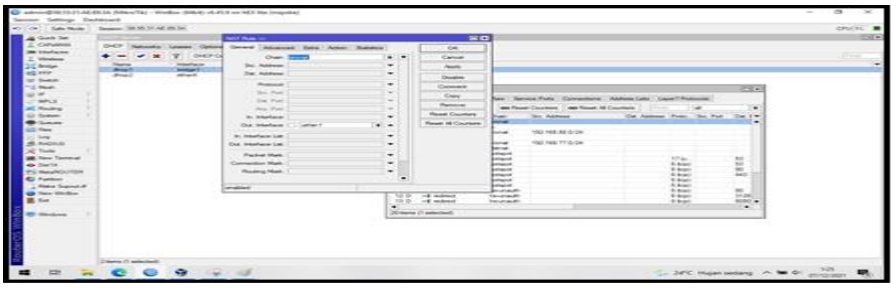
Berikutnya melakukan setup DHCP Server pada IP segmentyang telah kita buat sebelumnya klik IP pilih DHCP Server klik DHCP Setup pilih bridge1 pada DHCP Server Interface klik Next hingga selesai kemudian tambahkan kembali DHCP Server untuk IP segment jalur eksternal Pfsense pada bagian DHCP Server interface pilih ethernet4 klik next hingga selesai.

Gambar 9 Konfigurasi DHCP Server



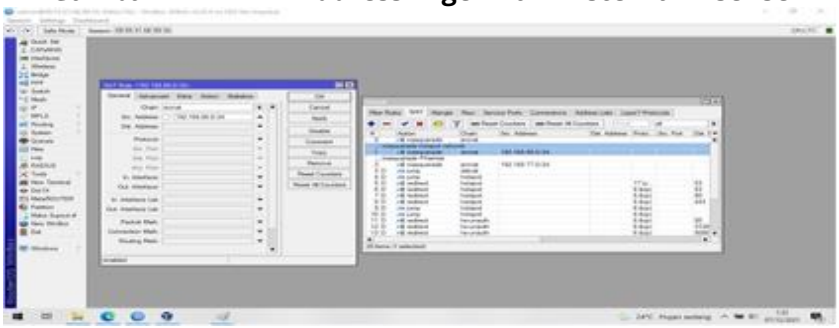
Sebelum melakukan setup hotspot agar mikrotik dapat mengakses internet maka diperlukan penambahan rulemasquerade pada firewall NAT klik tambah pada tab general pilih chain srcnat Out Interface pilih ether1 pada tab action pilih masqueradeapply dan ok.

Gambar 10 NAT interterface WAN



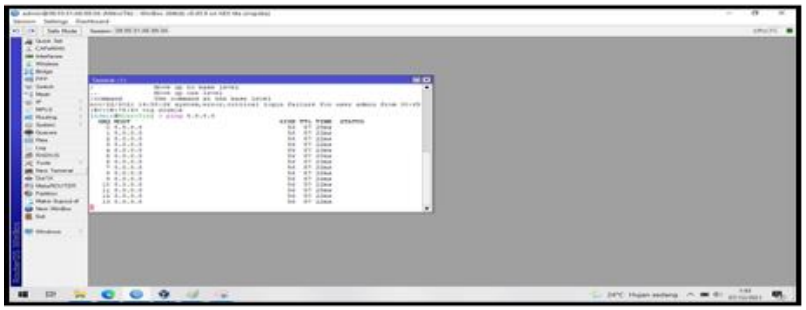
Kemudian tambahkan NAT untuk ip address brigde1 dan jalur eksternal firewall eksternal Pfsense agar dapat terhubung dengan internet pilih Chain srcnat form Src.Address diisi dengan ip range hotspot 192.168.88.0/24 kemudian pada tab action pilih masquerade apply dan ok. Kemudian tambahkan juga NAT ip range eksternal firewall eksternal Pfsense seperti langkah-langkah sebelumnya.

Gambar 11 NAT IP AddressBrige1 Dan Eksternal Pfsense



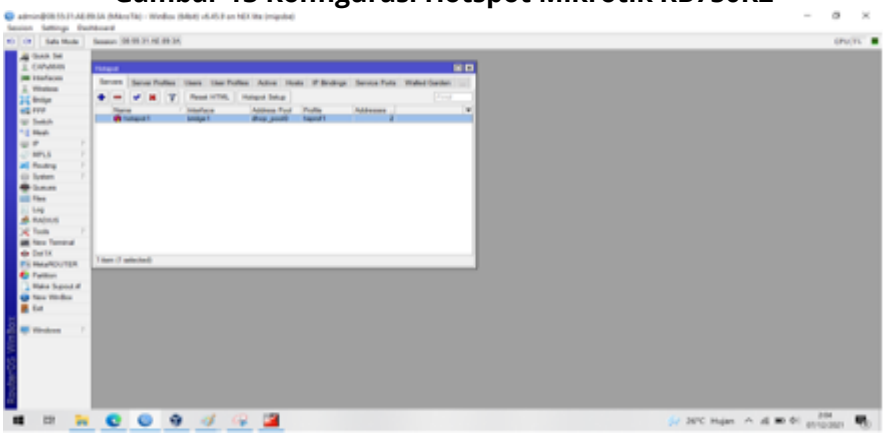
Mikrotik RB750R2 sudah mendapatkan akses internet dapat dilihat pada gambar 4.12 dibawah ini dengan melakukanping ke serverDNS google.

Gambar 12 Tes Koneksi Internet Mikrotik



Selanjutnya melakukan setuphotspot dengan klik IP pilih Hotspot kemudian klik setup hotspot pilih bridge1sebagaihotspot interface klik next hingga DNS name isi dengan wifi-ku.net next hingga selesai.

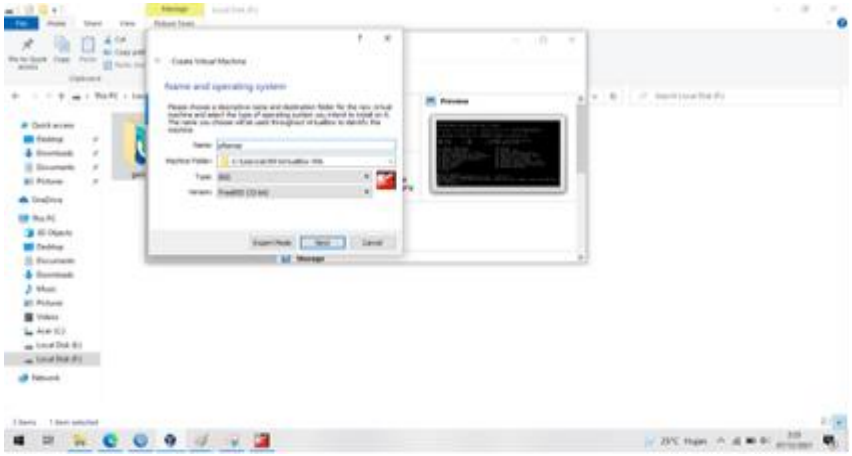
Gambar 13 Konfigurasi Hotspot Mikrotik RB750R2



2)Instalasi Pfsense Pada Virtualbox

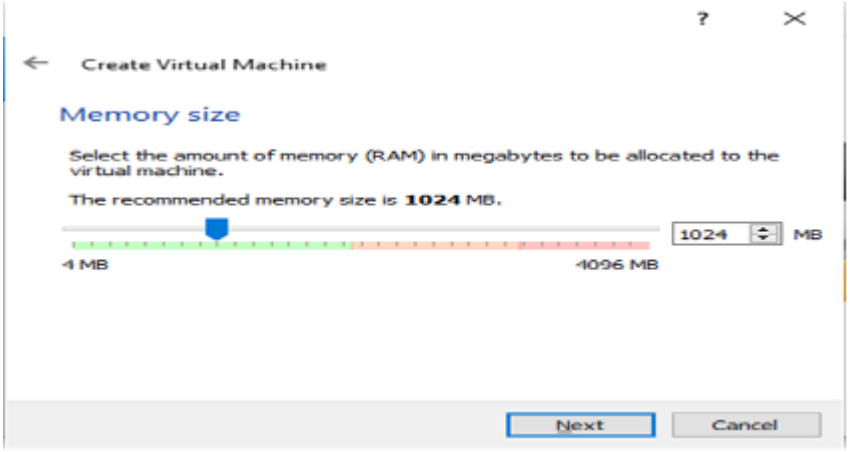
Buka aplikasi virtualbox Klik New kemudian name diisi dengan Pfsense type pilih BSD dan Version pilih FreeBSD kemudian klik next.

Gambar 14 Membuat Mesin Virtual Baru



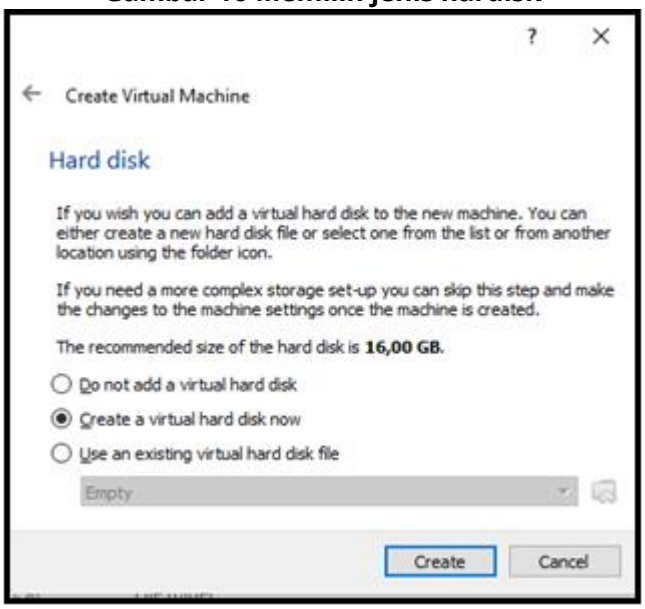
Selanjutnya memori size klik nextdisarankan menggunakan ukuran default agar tidak membebani komputer host.

Gambar 15 Memilih Alokasi Ram Untuk Mesin Virtual



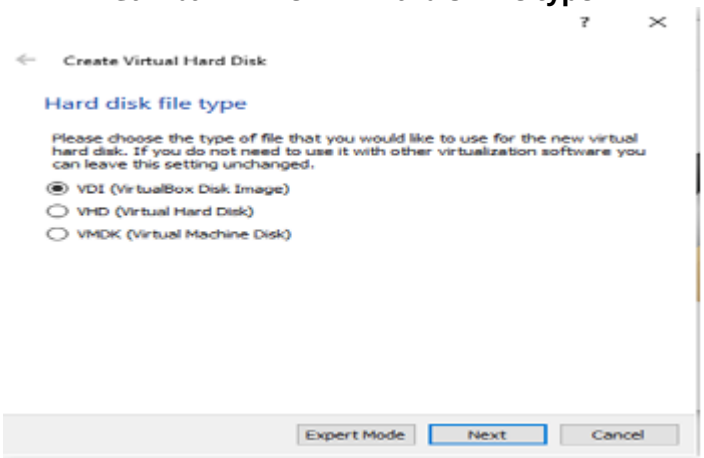
Berikutnya memilih jenis hardisk yang akan digunakan mesin virtualbox klik next

Gambar 16 Memilih jenis hardisk



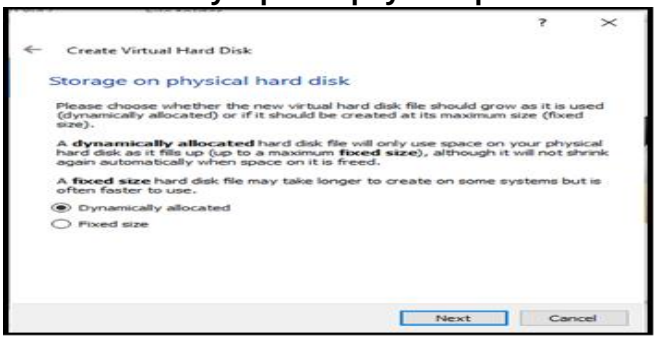
Berikutnya memilih hardisk file type ikuti default klik next.

Gambar 17 Memilih hardisk file type



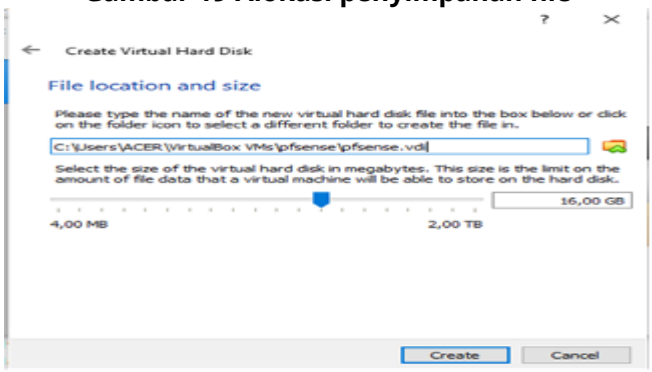
Penyimpanan physiical pada hardisk klik next

Gambar 18 Penyimpanan physiical pada hardisk



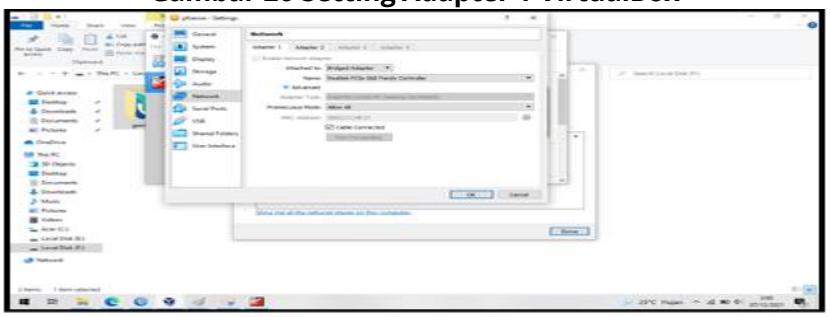
Kemudian alokasi penyimpanan file klik create.

Gambar 19 Alokasi penyimpanan file



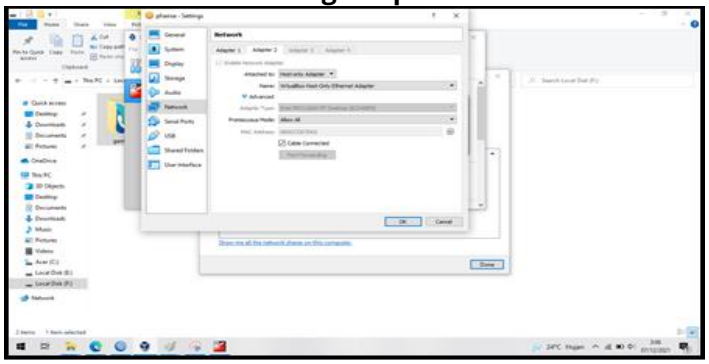
Kemudian masuk ke tab Setting pilih adapter 1 pada pilihan attached to plih bridge kemudianname pilih Realtek PCIe GbE Family Controller pada option advance Promicuous Mode PilihAllow All.

Gambar 20 Setting Adapter 1 VirtualBox



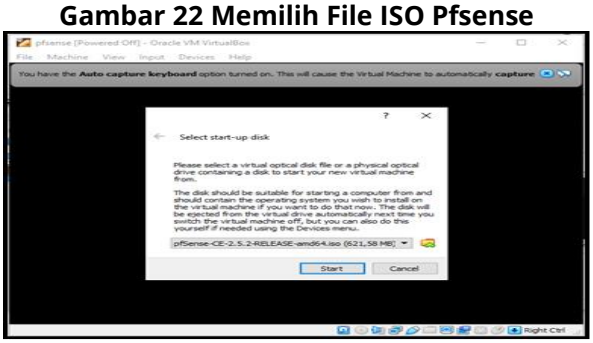
Berikutnya Setting Adapter 2 pada Attached pilih Host-only Adapter pada name pilih VirtualBox Host-only Adapter dan Promiscuous Mode pilih Allow All kemudian klik ok

Gambar 21 Setting adapter 2 VirtualBox



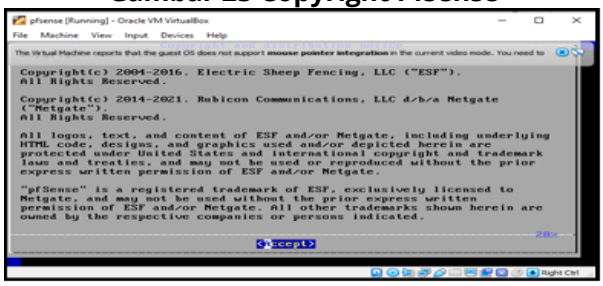
Jika selesai selanjutnya jalankan virtual mesin dengan mengklik gambar startsetelah booting pilih File Iso Pfsense dengan klik browse kemudian klik start Tunggu hingga proses booting selesai.

Gambar 22 Memilih File ISO Pfsense



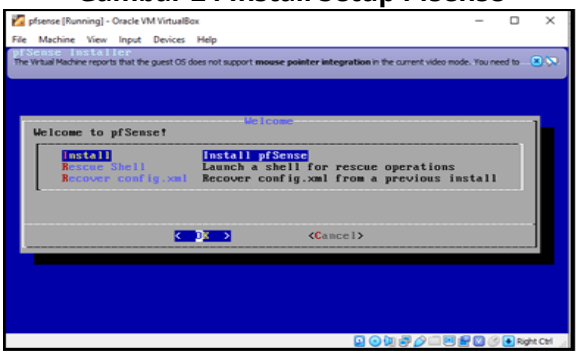
Jika sudah selesai booting maka akan masuk ke tampilan setup dari Pfsense klik Accept

Gambar 23 Copyright Pfsense



Klik install Pfsense kemudian ok

Gambar 24 Install Setup Pfsense



Kemudian klik next hingga menu ZFS configurations tekan spasi pada keyboard untuk menandai pilihan kemudian klik ok.

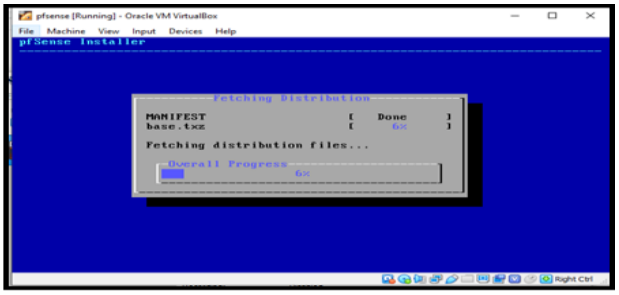
Gambar 25 ZFS configuration

Jika muncul peringan akan menghacurkan semua isi dalam hardisk ada0 pilih YES

Gambar 26 Pesan Peringatan Pfsense

Proses Instalasi Pfsense berlansung tunggu hingga selesai dan jika di minta untuk reboot klik yes.

Gambar 27 Proses Instalasi Pfsense



Setelah instalasi selesai maka Pfsense akan reboot dan booting ke menu utama CLI

KESIMPULAN DAN SARAN

Kesimpulan

Dari hasil pengujian yang telah dilakukan oleh penulis tentang pengimplementasian firewall eksternal Pfsense pada hotspot wifi-ku.net dapat disimpulkan, firewall eksternal Pfsense dapat mengatasi serangan brute force yang dilakukan menggunakan THC Hydra dan Medusa. Dan setelah diterapkan firewall eksternal Pfsense kinerja CPU tidak terganggu karena semua serangan ditampung oleh firewall eksternal Pfsense.

Saran

1. Untuk penelitian selanjutnya firewall eksternal Pfsense bisa dimanfaatkan untuk firewall pada jaringan public
2. Untuk penelitian selanjutnya bisa dicoba untuk melakukan penyerangan dengan menggunakan aplikasi penyerang lainnya dan bisa dilakukan penyerangan secara bersamaan supaya bisa tau seberapa tangguh firewall eksternal Pfsense

DAFTAR PUSTAKA

Alfarizi Mauludy Evrianta. 2020. Implementasi Keamanan Jaringan Pada Router Mikrotik Terhadap Serangan Brute Force Pada Server Jurusan Teknik Komputer. Palembang. Politeknik Negeri Sriwijaya, 48 Hal.

Amarudin and Ulum, F., 2018. Desain Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking Jurnal TEKNOINFO, 12(2) , 72-75.

Asmara, R. 2016. Sistem Informasi Pengolahan Data Penanggulangan Bencana Pada Kantor Badan Penanggulangan Bencana Daerah (Bpbd) Kabupaten Padang Pariaman Jurnal J-Click, 3(2) , 80-91.

Bustami, A. and Bahri, S., 2020. Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review Jurnal Pendidikan dan Aplikasi Industri (UNISTEK), 7(2) , 60-70.

Dirgantara, C.R.R., and Suartana, M.I., 2020. Implementasi Arp Watch Dengan Pfsense Untuk Mekanisme Pengamanan Access Point Jurnal Manajemen Informatika, 10(1) , 67-76.

Fitria, S.T. and Pirihanto, A., 2018. Implementasi Generate Voucher Hotspot Dengan Batasan Waktu (Time Based) Dan Kuota (Quota Based) Menggunakan User Manager Di Mikrotik Jurnal Manjemen Informatika, 8(2) , 18-24.

Hasbiyallah, M. and Jakaria, A.D., 2018. Aplikasi Penjualan Barang Perlengkapan Hand Phone Di Zildan Cell Singaparna Kabupaten Tasikmalaya JUMANTAKA, 1(1) , 61-70.

Hasrul, H. and Lawani, M.A., 2017. Pengembangan Jaringan Wireless Menggunakan Mikrotik Router Os Rb750 Pada Pt. Amanah Finance Palu Jurnal Elektronik Sistem Informasi dan Komputer, 3(1) , 11-19.

Khadafi, S., Nurmuslimah and Anggakusuma, K.F., 2019. Implementasi Firewall dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server Jurnal Ilmiah NERO, 4(3) , 181-188.

Munawar, Z. and Putri, I.N., 2020. Keamanan Jaringan Komputer Pada Era Big Data Jurnal Sistem Informasi, 2(1) , 14-20.

Muntahanah and Yulia, D., 2019. Aplikasi Pengarsipan Dokumen Menggunakan Metode String Matching (Studi Kasus Perpustakaan SMP Negeri 5 Seluma) Jurnal Informatika UPGRIS, 5(1) , 9-16.

Mutaqin, F.A., 2016. Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort Jurnal Sistem dan Teknologi Informasi (JUSTIN), 1(1) , 1-6.

Pratiwi,H., Arfyanti, I. And Kurniawan, D., 2016. Implementasi Algoritma Brute Force Dalam Aplikasi Kamus Istilah Kesehatan Jurnal Ilmiah Teknologi Informasi Terapan, 2(2) , 119-125.

Purwanto, E., 2015. Implementasi Jaringan Hotspot Dengan Menggunakan Router Mikrotik Sebagai Penunjang Pembelajaran (Studi Kasus : Smk Sultan Agung Tirtomoyo Wonogiri) Jurnal INFORMA Politeknik Indonusa Surakarta, 1(2) , 20-27.

Purwoko, M. and Hilal, H., 2019. Analisis Penerapan Firewall Nftables Sebagai Sistem Keamanan Server Pada Mesin Virtualisasi Jurnal Telekomunikasi dan Komputer, 9(1) , 1-21.

Santoso, W.B., Sundawa, F. and Azhari M., 2016. Implementasi Algoritma Brute Force Sebagai Mesin Pencari (Search Engine) Berbasis Web Pada Database JURNAL SISFOTEK GLOBAL, 6(1) , 1-8.

Suryana, N., and Saputra D.D., 2018. Perancangan Penggunaan Firewall Dan Proxy Server Untuk Membatasi Hak Akses Internet Jurnal Sutet, 8(1) , 44-53.

Syahputra, H. and Rendy., 2020. Perbandingan Manajemen Bandwidth Dengan Metode Hfsc, Priq Dan Cbq Pada Pfsense Jurnal Manajemen Informatika, 11(1) , 41-49.

Syaifudin, A. and Assegaff, S., 2020. Analisis Dan Pengembangan Manajemen Jaringan Dengan Menggunakan Mikrotik Rb750 Pada Ppm Al-Hidayah Jambi Jurnal Manajemen Sistem Informasi, 5(1) , 49-59.

Syaifuddin, Risqirwati, D. and Irwan, A.E., 2018. Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server Techno.com, 17(4) , 347-354.

Qirom and Sungkar, S.M., 2017. Rancang Bangun Jaringan Hotspot, Bandwidth Dan Blokir Website Berisi Konten Negatif Untuk Meningkatkan Layanan Pembelajaran Di Sd Negeri Bangun Galih 1 ¬Power Elektornik, 6(1) , 17-21.