MANAJEMEN ANCAMAN DAN KEAMANAN JARINGAN MELALUI PENGGUNAAN FIREWALL DENGAN MIKROTIK PADA PT DINAMIKA MEDIAKOM

Disusun oleh:

Nama : Viki Tegar Aditya
NIM : 19523177

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2023

HALAMAN PENGESAHAN DOSEN PEMBIMBING

MANAJEMEN ANCAMAN DAN KEAMANAN JARINGAN MELALUI PENGGUNAAN FIREWALL DENGAN MIKROTIK PADA PT DINAMIKA MEDIAKOM

TUGAS AKHIR

Disusun Oleh:

N a m a	: Viki Tegar Aditya
NIM	: 19523177

Yogyakarta, 26 Desember 2023

Pembimbing,

(Syarif Hidayat S.Kom., M.I.T)

HALAMAN PENGESAHAN DOSEN PENGUJI

MANAJEMEN ANCAMAN DAN KEAMANAN JARINGAN MELALUI PENGGUNAAN FIREWALL DENGAN MIKROTIK PADA PT DINAMIKA MEDIAKOM

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika - Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Tim Penguji

Ketua
Syarif Hidayat S.Kom., M.I.T

Anggota 1

Dr. Yudi Prayudi, S.Si., M.Kom

Anggota 2

Elyza Gustri Wahyuni, S.T., M.Cs.

Mengetahui,
Ketua Program Studi Informatika – Program Sarjana
Fakultas Teknologi Industri
Universitas Islam Indonesia

(Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Viki Tegar Aditya

NIM : 19523177

Tugas akhir dengan judul:

Manajemen Ancaman Dan Keamanan Jaringan Melalui Penggunaan Firewall Dengan Mikrotik Pada PT Dinamika Mediakom

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 19 Desember 2023

(VIKI TEGAR ADITYA)

iv

HALAMAN PERSEMBAHAN

Tugas akhir ini disajikan sebagai penghargaan kepada orang tua, saudara dan seluruh keluarga besar yang telah memberikan dukungan, kasih sayang dan senantiasa mendoakan penulis selama ini.

HALAMAN MOTO

“Sesungguhnya sesudah kesulitan ada kemudahan”
(QS Al-Insyirah 6)

“Orang yang meraih kesuksesan tidak selalu orang yang pintar. Orang yang selalu meraih kesuksesan adalah orang yang gigih dan pantang menyerah”
(Susi Pudjiastuti)

“Buat apa berkelimang harta jika tidak bisa menyanding orangtua”
(Viki Tegar Aditya)

KATA PENGANTAR

Assalamu'alaikum Warrahmatullahi Wabarakatuh.

Segala puji bagi Allah Subhanallahu wa Ta'ala atas rahmat serta petunjuk sehingga penulis berhasil menyelesaikan tugas akhir dengan baik. Dengan ridho Allah, penulis berhasil menyelesaikan tugas akhir sebagai persyaratan untuk meraih gelar sarjana Informatika dari Universitas Islam Indonesia.

1. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc. selaku Ketua Program Studi Teknik Informatika dan selaku dosen pembimbing akademik – Program Sarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
2. Bapak Syarif Hidayat S.Kom., M.I.T selaku dosen pembimbing dalam penyusunan tugas akhir.
3. Kedua orang tua dan keluarga besar yang telah memberikan dukungan serta senantiasi mendoakan penulis.
4. Semua pihak yang telah membantu penulisin menyusun tugas akhir yang tidak dapat disebutkan satu persatu.

Penulisan laporan tugas akhir ini masih memiliki kekurangan dan keterbatasan, karena keterbatasan pengetahuan dan pengalaman penulis dalam menyusunnya. Karena itu, penulis berharap agar diberikan kritik dan saran yang membangun agar dapat memperbaiki di masa yang akan datang. Semoga hasil tugas akhir ini dapat memberikan manfaat bagi orang lain.

Yogyakarta, 26 Desember 2023

(Viki Tegar Aditya)

SARI

Keamanan jaringan menjadi semakin penting dalam era teknologi informasi saat ini, di mana ancaman siber semakin canggih dan meluas. Serangan siber, malware, dan peretasan data adalah contoh ancaman keamanan jaringan yang dapat menyebabkan kerugian finansial, kerusakan reputasi, dan gangguan operasional. Oleh karena itu, untuk melindungi aset digital mereka, bisnis harus menerapkan strategi keamanan yang efisien. Firewall adalah alat umum untuk keamanan jaringan. Salah satu jenis tindakan keamanan komputer yang paling populer adalah firewall karena melindungi data dan melindungi dari kegagalan sistem. MikroTik Router merupakan salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang dapat diandalkan, dengan menyediakan berbagai fitur lengkap untuk jaringan dan nirkabel. Penelitian ini memfokuskan pada implementasi firewall MikroTik sebagai solusi untuk melindungi jaringan PT Dinamika Mediakom dari berbagai ancaman, termasuk serangan DDoS, serangan brute force, dan port scanning. Penelitian ini bertujuan untuk menginvestigasi dan menganalisis manajemen ancaman dan keamanan jaringan melalui penggunaan firewall dengan MikroTik dalam konteks PT Dinamika Mediakom.Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kualitatif dengan bersumber dari buku, jurnal maupun media cetak. Tahapan metodologi yang mencakup pengumpulan data, analisis kebutuhan, perancangan sistem, implementasi, dan rancangan pengujian. Dari penelitian ini didapatkan hasil berupa peningkatan CPU Load > 65% tanpa penggunaan firewall dimana CPU Load normal berada < 20% dan setelah di implementasikan konfigurasi firewall dapat menjaga CPU Load menjadi stabil dengan persentase < 20%. Pada serangan Brute Force Attack konfigurasi firewall dapat melindungi dari serangan hacker yang mencoba masuk dan memasukan IP Address penyerang kedalam daftar hitam. Pada serangan Port Scanning konfigurasi firewell dapat menutup port yang terbuka. PT Dinamika Mediakom dapat mengurangi risiko serangan dan melindungi jaringan. Terdapat peningkatan yang signifikan dalam manajemen keamanan jaringan, serta penurunan jumlah serangan dan upaya yang mencurigakan.

Kata kunci: manajemen ancaman, firewall, mikrotik, ddos, brute force attack, port scanning.

GLOSARIUM

Firewall :Firewall adalah sistem keamanan yang digunakan untuk mengontrol lalu lintas jaringan antara jaringan pribadi (internal) dan jaringan publik (eksternal). Tujuannya adalah untuk melindungi jaringan internal dari ancaman eksternal dengan memantau, memfilter, dan mengatur lalu lintas data.

Router :Router adalah perangkat jaringan yang mengarahkan lalu lintas data antar jaringan yang berbeda. Bertindak sebagai penghubung antara jaringan yang berbeda dan dapat membuat keputusan tentang jalur terbaik untuk mengirim data.

Mikrotik :MikroTik adalah produsen perangkat keras dan perangkat lunak jaringan yang populer. Mereka dikenal karena produk-produk mereka yang mencakup router, switch, dan firewall. MikroTik RouterOS adalah sistem operasi yang sering digunakan untuk mengelola jaringan.

DDoS :DDoS adalah serangan yang bertujuan untuk menghentikan atau mengganggu layanan online dengan mengalirkan lalu lintas data yang sangat besar ke target.

SSH :SSH adalah protokol keamanan yang digunakan untuk mengakses perangkat jaringan atau server dengan aman

Telnet :Telnet adalah protokol jaringan yang digunakan untuk mengakses perangkat jaringan atau server jarak jauh.

Brute Force Attack :Serangan yang mencoba untuk mencari kata sandi dengan menebak kombinasi yang mungkin.

Port Scanning :Serangan di mana penyerang mencoba mengidentifikasi port yang terbuka pada perangkat atau jaringan.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1. Latar Belakang

Bersamaan dengan meningkatnya permintaan untuk layanan yang cepat dan efektif, industri telekomunikasi saat ini berkembang dengan sangat cepat. Prinsip serupa berlaku untuk transmisi data, yang dimulai dengan bergabungnya dua komputer ke jaringan komputer. Jaringan komputer saat ini adalah layanan penting. Dibandingkan dengan komputer mandiri, jaringan komputer memiliki banyak manfaat. Data, perangkat lunak, dan berbagi peralatan semua dimungkinkan melalui jaringan komputer. Sehingga tim dapat berkomunikasi lebih efektif dan efisien. (Astari, 2018: 3).

Kumpulan komputer-komputer yang saling terhubung dan berdiri sendiri dikenal sebagai jaringan komputer (computer network). Jaringan komputer adalah pengelompokan beberapa komputer (dan perangkat lain seperti router, switch, dll) yang dapat dijelaskan secara awam.) yang saling berhubungan melalui media perantara. Media kabel atau nirkabel (wireless) dapat digunakan sebagai media perantara ini. Data akan ditransfer dari satu komputer ke komputer lain, memungkinkan setiap komputer yang terhubung untuk berbagi perangkat keras atau bertukar informasi. (Iwan, 2008)

Dengan seiring berkembangnya secara pesat terdapat ancaman mengenai keamanan data elektronik. Bagi bisnis yang menawarkan layanan teknologi informasi (TI) serta sektor lain seperti perbankan, transportasi, berita, lembaga pendidikan, dan perusahaan ekspor-impor yang mengandalkan fasilitas TI sebagai infrastruktur penting (penting), keamanan data elektronik sangatlah penting. Aset bagi bisnis adalah informasi atau data. Dengan meminimalkan risiko, memaksimalkan laba atas investasi, dan mengejar peluang bisnis, keamanan data secara tidak langsung dapat menjamin kelangsungan bisnis. Risiko kerusakan, kehilangan, atau paparan data kepada pihak luar yang tidak diinginkan meningkat seiring dengan banyaknya informasi perusahaan yang disimpan, dikelola, dan dibagikan. Keamanan informasi melindungi data dari berbagai risiko untuk menjamin kelangsungan bisnis, mengurangi kerugian perusahaan, dan meningkatkan laba atas investasi dan peluang bisnis. Untuk menjamin data terkirim dan diterima oleh pengguna yang dituju, diperlukan suatu sistem pengelolaan sistem informasi yang memungkinkan data dapat didistribusikan secara elektronik. (Syafrizal, 2017)

Keamanan jaringan sangat penting bagi bisnis di era digital yang sangat maju saat ini. Keamanan sistem informasi adalah istilah umum untuk semua mekanisme yang diperlukan yang harus dimasukkan ke dalam suatu sistem untuk melindunginya dari semua ancaman yang membahayakan keamanan data informasi dan keamanan aktor sistem. Ancaman mencakup berbagai perilaku karyawan, termasuk ketidakpedulian, kelalaian, mencuri kata sandi karyawan lain, dan membagikan kata sandi kepada karyawan lain. untuk ancaman eksternal, seperti serangan peretas, infeksi spyware dan virus, serta intrusi. (Putro, 2014: 115).

Ancaman keamanan jaringan seperti serangan siber, malware, dan peretasan data dapat mengakibatkan kerugian finansial, reputasi yang rusak, dan gangguan operasional. Oleh karena itu, perusahaan perlu mengadopsi strategi keamanan yang efektif untuk melindungi aset digital mereka. Salah satu alat yang umum digunakan untuk mengamankan jaringan adalah firewall. Teknologi Firewall, Firewall adalah salah satu jenis tindakan keamanan komputer yang paling banyak digunakan karena melindungi keamanan komputer dan mencegah kegagalan komputer.. Firewall dapat berupa perangkat keras, perangkat lunak, atau antara dua komputer atau lebih. Firewall dapat memainkan peran yang lebih besar dalam perlindungan komputer karena semua aliran data harus disaring melalui firewall. Secara umum firewall mempunyai fungsi sebagai berikut: fungsi pertama, firewall dapat mencegah orang lain yang tidak berhubungan memasuki komputer pribadi pengguna; fungsi kedua, bahkan jika orang luar memasuki sistem, firewall dapat mencegahnya mengakses tempat pertahanan; ketiga, firewall dapat mencegah kunjungan ke situs web karena kemampuannya memfilter alamat yang tidak diinginkan; dan terakhir, firewall dapat memblokir akses ke situs web tertentu. Pada dasarnya, komputer akan menyediakan fungsi pemantauan keamanan. (Zen Munawar dan Novianti Indah Putri, 2020: 19)

Segala bentuk ancaman yang datang baik langsung maupun tidak langsung akan mengganggu kegiatan yang sedang berlangsung dalam jaringan. Dalam rangka melindungi kemungkinan serangan-serangan tersebut perlu di terapkan konsep firewall. Dimana firewall dirancang untuk mencegah akses yang tidak diinginkan yang datang baik dari internal maupun external jaringan. Penerapan konsep firewall terlihat cukup sederhana yaitu bila ada traffic yang datang dan menuju suatu jaringan, firewall kemudian akan melakukan pemeriksaan serta control terhadap traffic tersebut kemudian dikirimkan ke tujuannya.MikroTik Router merupakan salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang dapat diandalkan, dengan menyediakan berbagai fitur lengkap untuk jaringan dan nirkabel. Di

samping itu, MikroTik juga dapat berperan sebagai pelindung bagi komputer lain dan memberikan prioritas kepada komputer lain untuk mengakses data Internet dan data lokal. MikroTik memiliki tujuan untuk mengendalikan kecepatan transfer data dan mengelola jaringan komputer. Pengaturan router MikroTik diletakkan pada komputer yang berperan sebagai gerbang untuk sebuah jaringan. Gateway komputer bertugas membagi data yang keluar masuk dari dan ke komputer lainnya agar semua komputer dapat mengakses data bersama. (Mancill, 2002).

PT. Dinamika Mediakom adalah singkatan dari Dinamika Media Komunikasi sebuah perusahaan yang bergerak di bidang ICT (Information Communications Technology). PT. Dinamika Mediakom mempunyai beberapa cabang di jawa tengah, seperti : Klaten, Batang, Banjarnegara, Magelang dan Temanggung. Sedangkan untuk kantor pusat terletak di Yogyakarta, tepatnya di Jalan Raya Kledokan no.38, Kledokan, Caturtunggal, kecamatan Depok, Sleman, Daerah Istimewa Yogyakarta.

Penelitian dilakukan di PT Dinamika Mediakom yang terdapat masalah pada rentannya keamanan jaringan. Keamanan jaringan sangatlah penting bagi perusahaan agar tidak terjadinya pencurian data oleh seorang hacker. Dengan permasalahan tersebut maka penelitian ini berjudul “Manajemen Ancaman dan Keamanan Jaringan melalui penggunaan Firewall dengan Mikrotik di PT. Dinamika Mediakom”. Penelitian akan dilakukan dengan metode blackbox yang menguji berbagai serangan, antara lain : Serangan DDoS, Brute Force attack, dan Port Scanning. Penyerangan akan dilakukan dengan perbandingan memakai firewall mikrotik dan tidak memakai firewall maka dapat di simpulkan untuk hasil dari penelitian.

Keamanan jaringan telah menjadi isu yang semakin mendesak dalam era digital yang gejolak ini. Dengan berkembangnya teknologi informasi dan konektivitas yang semakin meluas, ancaman terhadap integritas, kerahasiaan, dan ketersediaan data serta infrastruktur jaringan juga semakin meningkat. Keberadaan ancaman siber, baik yang datang dari luar maupun dari dalam organisasi, menuntut adanya pendekatan yang komprehensif dalam

manajemen keamanan jaringan. Manajemen Ancaman dan Keamanan Jaringan merupakan konsep yang luas yang berfokus pada strategi dan taktik yang digunakan untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta infrastruktur jaringan dari berbagai macam ancaman siber. Dalam era di mana ketergantungan terhadap teknologi informasi semakin mendalam, risiko terhadap keamanan jaringan menjadi semakin signifikan. Ancaman siber dapat berkisar dari serangan malware yang merusak, peretasan yang merusak data sensitif, hingga serangan DDoS yang menyebabkan kelumpuhan layanan. Oleh karena itu, manajemen ancaman dan keamanan jaringan melibatkan serangkaian tindakan proaktif untuk mengidentifikasi, mengurangi, dan merespons ancaman-ancaman ini.

Dalam praktiknya, manajemen ancaman dan keamanan jaringan melibatkan penerapan kebijakan keamanan yang tepat, penggunaan teknologi keamanan seperti firewall dan sistem deteksi intrusi, serta pelatihan untuk pengguna agar dapat mengenali dan menghindari potensi ancaman. Manajemen Ancaman dan Keamanan Jaringan merupakan upaya berkelanjutan yang harus diadopsi oleh organisasi dan individu untuk menjaga keberlanjutan operasional dan melindungi aset informasi yang berharga dari ancaman siber yang terus berkembang.

Dalam konteks ini, penelitian ini bertujuan untuk menyelidiki dan menganalisis upaya-upaya dalam manajemen ancaman dan keamanan jaringan melalui penggunaan firewall dengan menggunakan teknologi MikroTik dengan studi kasus dalam perusahaan PT. Dinamika Mediakom. Perangkat firewall telah lama menjadi penopang utama dalam pertahanan jaringan, memungkinkan pengaturan akses, pemantauan lalu lintas, dan perlindungan terhadap serangan siber yang beragam

1.2. Rumusan Masalah

1. Rentanya keamanan jaringan di PT. Dinamika Mediakom.

1.3. Batasan Masalah

Batasan masalah dari penelitian ini sebagai berikut:

1. Penelitian dilakukan di PT. Dinamika Mediakom
2. Implementasi penelitian dilakukan dengan simulasi.
3. Fokus dari penelitian ini adalah pada Manajemen Ancaman Dan Keamanan Jaringan Melalui Penggunaan Firewall Dengan Mikrotik.

1.4. Tujuan Penelitian

Tujuan penelitian antara lain:

1. Menyelediki dan menganalisa berbagai ancaman dan keamanan jaringan menggunakan firawall dengan perangkat Mikrotik.
2. Membantu perusahaan melindungi jaringan dari ancaman siber.
3. Dapat memanajemen ancaman yang lebih efektif.

1.5. Manfaat Penelitian

Manfaat penelitian antara lain:

1. Penelitian ini akan memberikan bahan referensi dan literatur bagi para akademisi dan mahasiswa yang mempelajari keamanan jaringan, sehingga dapat meningkatkan pemahaman mereka tentang topik ini.

2. Penelitian ini diharapkan dapat memberikan wawasan lebih mendalam tentang bagaimana peran firewall dalam manajemen ancaman dan keamanan jaringan perusahaan. Hasil penelitian ini dapat membantu perusahaan dalam merancang strategi keamanan yang lebih baik, memilih teknologi firewall yang sesuai, serta meningkatkan kesadaran akan pentingnya perlindungan jaringan dari ancaman siber.

3. Penelitian ini dapat membantu perusahaan untuk mengatasi masalah keamanan jaringan dengan menggunakan Firewall dengan MikroTik yang dapat mengidentifikasi dan memblokir akses yang mencurigakan serta memberikan perlindungan terhadap serangan malware dan virus.

1.6. Metodologi Penelitian

Penelitian ini akan menggunakan pendekatan kualitatif dengan studi kasus sebagai metodologi utama. Data akan dikumpulkan melalui wawancara dengan para profesional keamanan jaringan di perusahaan yang telah mengimplementasikan firewall, serta analisis dokumentasi terkait konfigurasi firewall, kebijakan akses, dan laporan keamanan. Data yang terkumpul akan dianalisis untuk mengidentifikasi pola, tren, serta dampak implementasi firewall terhadap manajemen ancaman dan keamanan jaringan.

1.7. Sistematika Penulisan

BAB I PENDAHULUAN

1.1 Latar Belakang

Pada sub bab ini, membahas mengenai berbagai komponen penting yang menjadi dasar penelitian akan dijelaskan secara rinci, Keamanan jaringan menjadi semakin penting dalam era digital saat ini, seiring dengan meningkatnya ancaman siber yang dapat mengganggu integritas dan ketersediaan data serta infrastruktur jaringan. Ancaman tersebut tidak hanya datang dari luar, tetapi juga dari dalam organisasi. Oleh karena itu, perlindungan terhadap jaringan melalui penggunaan solusi keamanan, seperti firewall, menjadi krusial dalam menjaga kelangsungan operasional dan kerahasiaan informasi.

1.2 Rumusan Masalah

Dalam konteks ini, penelitian ini bertujuan untuk menjawab pertanyaan-pertanyaan penting penelitian

1.3 Batasan Masalah

Penelitian ini memiliki batasan dengan fokus pada penggunaan firewall MikroTik sebagai solusi keamanan jaringan. Meskipun ancaman siber memiliki beragam bentuk, penelitian ini akan memfokuskan pada beberapa jenis ancaman yang relevan dan mungkin muncul dalam berbagai lingkungan jaringan.

1.4 Tujuan Penelitian

Tujuan utama dari penelitian ini adalah untuk mengidentifikasi potensi ancaman yang ada dalam jaringan, mengevaluasi efektivitas penggunaan firewall MikroTik dalam mengatasi ancaman tersebut, dan menghasilkan panduan praktis untuk manajemen keamanan jaringan yang lebih efektif

1.5 Manfaat Penelitian

Penelitian ini memiliki manfaat yang luas, baik bagi praktisi IT, organisasi, maupun lingkungan akademis. Praktisi IT akan mendapatkan wawasan yang lebih baik tentang strategi keamanan jaringan yang efektif, sementara organisasi dapat mengaplikasikan rekomendasi dari penelitian ini untuk meningkatkan perlindungan data dan sistem. Di sisi

akademis, penelitian ini akan memberikan sumbangan pengetahuan terkait manajemen ancaman dan keamanan jaringan.

1.6 Metodologi Penelitian

Penelitian ini akan menggunakan pendekatan kualitatif dengan studi kasus sebagai metodologi utama dan ditambahkan data pendukung dengan wawancara dari pihak perusahaan.

BAB II LANDASAN TEORI

Pada Bab 2, yang merupakan Landasan Teori, penelitian ini akan merinci konsep-konsep dan prinsip-prinsip dasar yang mendukung pengembangan manajemen ancaman dan keamanan jaringan dengan menggunakan firewall MikroTik.

BAB III METODOLOGI PENELITIAN

Pada Bab 3, yang merupakan Metodologi Penelitian, akan diuraikan tentang bagaimana penelitian ini dilakukan, dari pendekatan penelitian hingga teknik pengumpulan dan analisis data yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Pada Bab 4, yang merupakan Pembahasan, penelitian ini akan merinci hasil dan analisis data yang diperoleh dari penelitian.

BAB V SIMPULAN DAN SARAN

5.1 Kesimpulan

Bagian ini membahas rangkuman temuan-temuan dan analisis dari hasil dan pembahasan yang telah dipaparkan dalam BAB IV.

5.2 Saran

Sub-bab bagian terakhir ini akan memberikan saran kepada peneliti-peneliti masa depan mengenai bagaimana topik ini dapat diperluas atau ditingkatkan dalam penelitian berikutnya.

BAB II
TINJAUAN PUSTAKA

Tabel 2.1 Literatur Review

No.	Penulis	Judul	Topik/Tujuan	Metode	Hasil
1	Fachri, F.	Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing	Penggunaan berbagai metode dan alat, seperti fail2 ban, Metasploit, Medusa untuk mengidentifikasi kerentanan dan melindungi sistem dari serangan.	Metode yang digunakan adalah pengujian penetrasi, Metodologi ini terdiri dari lima bagian utama yang saling berhubungan, termasuk Pengumpulan Intelijen, Analisis Kerentanan, Eksploitasi, Pasca Eksploitasi, dan Pelaporan.	Penetration Testing efektif dalam mengidentifikasi kerentanan dan melindungi sistem dari serangan. Penelitian menemukan kerentanan pada server dan berhasil mencegah serangan brute force.
2	Abraham Yano Suharmanto, Arie S.M Lumenta, Xaverius B.N. Najoan	Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi	Penelitian berfokus pada evaluasi kerentanan keamanan jaringan dan situs web di Universitas Sam Ratulangi (Unsrat). Tujuannya adalah untuk menganalisis dan mengidentifikasi potensi ancaman keamanan, seperti packet sniffing, serangan DDoS, dan kerentanan server web, serta mengusulkan	Penelitian menggunakan beberapa metode untuk pengumpulan data, termasuk observasi, pengujian, dan studi literatur. Penelitian juga menggunakan penelitian tindakan, yang melibatkan diagnosa dan penerapan tindakan nyata untuk mendeteksi dan memecahkan masalah. Metodologi ini juga	Keamanan jaringan belum sepenuhnya dapat dikatakan aman, walaupun dikatakan belum aman tetapi tingkat ancaman yang ditunjukkan hanya berada di level 2 dan tidak mendapatkan tingkat keamanan pada level high pada web alert akan tetapi jaringan

			rekomendasi untuk meningkatkan keamanan jaringan dan situs web. Penelitian ini bertujuan untuk melindungi data penting dari serangan peretas dan untuk menilai tingkat keamanan jaringan dan situs web secara keseluruhan di Unsrat.	melibatkan pengujian penetrasi, seperti yang terlihat pada penelitian terkait lainnya.	unsrat masih bisa terkena Flooding dan metode penyerangan DDOS masih bisa dilakukan. Sedangkan pada level Medium yang mengandung informasi sensitif, dan sehingga keamanan website Unsrat berhasil dan dapat penetrasi dan server terganggu.
3	Alfred, Joko Christian Chandra	Pemanfaatan Firewall Pada Jaringan Komputer SMK FADILAH	Membahas pemanfaatan firewall pada jaringan komputer di SMK Fadilah untuk mengatasi masalah akses internet yang tidak terbatas dan penyalahgunaan akses internet oleh siswa. Tujuannya adalah untuk mengimplementasikan firewall menggunakan router Mikrotik untuk membatasi akses ke situs web tertentu dan untuk mengamankan akses internet.	Penelitian menggunakan beberapa metode, termasuk observasi langsung, wawancara, studi literatur, analisis, implementasi, dan penyusunan laporan akhir. Metode-metode ini dipilih untuk memastikan bahwa tujuan penelitian dapat dicapai secara efektif.	Implementasi firewall router Mikrotik di SMK Fadilah secara efektif mengatasi akses internet yang tidak terbatas dan penyalahgunaan akses internet oleh siswa. Konfigurasi firewall berhasil membatasi akses ke situs web tertentu, mencegah siswa mengakses situs jejaring sosial dan situs streaming selama sesi lab.

4	Amarudin, Faruk Ulum	Desain Keamanan Jaringan pada Mikrotik Router OS Menggunakan Metode Port Knocking	Merancang keamanan jaringan pada Mikrotik Router OS dengan menggunakan metode Port Knocking untuk meningkatkan keamanan jaringan. Penelitian ini bertujuan untuk mencapai hal tersebut dengan menggunakan simulator GNS3 untuk mendesain dan mensimulasikan topologi keamanan jaringan.	Penelitian ini menggunakan metode Port Knocking untuk keamanan jaringan pada Mikrotik Router OS. Penelitian ini juga melibatkan penggunaan simulator GNS3 untuk mendesain dan mensimulasikan topologi keamanan jaringan. Penelitian juga menggabungkan penggunaan sertifikat digital untuk otentikasi dan implementasi Port Knocking berdasarkan sertifikat x509.	Metode Port Knocking cocok untuk menjaga keamanan jaringan, dan mengakses router admin harus melewati dua gerbang keamanan. Artikel ini menyarankan bahwa penelitian lebih lanjut diperlukan untuk mengembangkan peran perutean yang lebih kompleks
5	Efrahim Sinyo Rio Ola Balen Langobelen, Rr. Yuliana Rachmawat, Catur Iswahyudi	Analisis dan Optimasi dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus di TAMAN PINTAR YOGYAKARTA	Analisis dan optimalisasi keamanan jaringan menggunakan firewall Mikrotik di Taman Pintar Yogyakarta. Tujuannya adalah untuk Meningkatkan keamanan jaringan melalui berbagai konfigurasi, termasuk pengaturan firewall, manajemen port layanan, dan konfigurasi filter jembatan,	Penelitian menggunakan konsep Prepare Plan Design Implement Operate and Optimize (PPDIOO) sebagai metodologi penelitian. Metodologi ini merupakan pendekatan siklus hidup yang terus menerus dilakukan dalam proses pengembangan dan implementasi jaringan. Penelitian juga	Penelitian berhasil meningkatkan sistem keamanan jaringan di Taman Pintar Yogyakarta melalui konfigurasi firewall, manajemen port layanan, dan konfigurasi filter jembatan. Selain itu, penelitian ini juga menyarankan pengembangan sistem untuk

			serta untuk mengembangkan sistem untuk mendeteksi dan mengatasi serangan jaringan secara langsung dan meningkatkan keamanan secara keseluruhan terhadap serangan yang berpotensi merusak.	menggabungkan konfigurasi untuk sistem keamanan jaringan komputer Taman Pintar Yogyakarta	mendeteksi dan mengatasi serangan jaringan secara langsung, serta meningkatkan keamanan secara keseluruhan terhadap serangan yang berpotensi merusak.

2.1. Konsep Keamanan Jaringan

Ide keamanan jaringan mengacu pada kumpulan prosedur, metode, dan alat yang digunakan untuk menjaga keandalan, keakuratan, dan ketersediaan data serta infrastruktur jaringan dalam suatu perusahaan atau lingkungan lainnya. Di dunia digital yang terus berkembang di mana jaringan komputer menjadi pondasi hampir semua aspek kehidupan kita, mulai dari bisnis hingga pemerintahan, keamanan jaringan adalah hal yang paling penting.

Integritas data mengacu pada persyaratan bahwa data akurat dan tidak berubah. Kerahasiaan adalah tindakan mencegah akses tidak sah terhadap informasi pribadi dan sensitif. Aksesibilitas data mengacu pada kemampuan pihak yang berwenang untuk mengakses dan memanfaatkan data kapan pun diperlukan. Oleh karena itu, gagasan keamanan jaringan bertujuan untuk mencapai keseimbangan ideal antara ketiga faktor tersebut.

Keamanan jaringan mengacu pada tindakan yang dilakukan untuk melindungi jaringan komputer dari akses tidak sah, serangan dunia maya, dan ancaman keamanan lainnya. Tujuan keamanan jaringan adalah untuk memastikan kerahasiaan, integritas, dan ketersediaan sumber daya jaringan seperti data, aplikasi, dan perangkat. Keamanan jaringan mencakup berbagai praktik dan teknologi seperti firewall, sistem deteksi intrusi, jaringan pribadi virtual (VPN), dan enkripsi. Alat-alat ini membantu melindungi jaringan dari ancaman seperti port scanning, brute force attack, dan serangan DDoS. Selain solusi teknis, keamanan jaringan juga memerlukan kebijakan dan prosedur organisasi untuk memastikan bahwa staf dilatih mengenai praktik terbaik keamanan siber dan proses keamanan diikuti secara konsisten. Keamanan jaringan merupakan aspek penting dalam kelangsungan bisnis dan perencanaan pemulihan bencana, karena kegagalan dalam keamanan jaringan dapat mengakibatkan kerugian finansial dan reputasi yang signifikan, dan menyebabkan kerugian yang tidak dapat diperbaiki pada operasi organisasi.

2.2. Ancaman Siber dan Jenisnya

Ancaman siber adalah ancaman yang muncul dalam dunia digital dan melibatkan serangan terhadap sistem komputer, jaringan, dan data yang tersimpan di dalamnya. Ancaman siber mencakup berbagai jenis serangan yang dapat mengakibatkan dampak yang merugikan, baik pada tingkat individu, organisasi, maupun negara. Ancaman siber adalah upaya pencurian, pengambilan, dan perusakan data secara ilegal. Ancaman siber bisa datang dari berbagai pihak,

seperti hacker, spionase perusahaan, kelompok teroris, organisasi kriminal, hingga individu. Jenis-jenis ancaman siber yang umum saat ini antara lain:

1. Serangan Distributed Denial of Service (DDoS)
2. Port Scanning
3. Brute Force Attack

Setiap jenis ancaman siber memiliki cara kerja dan dampak yang berbeda-beda. Oleh karena itu, penting bagi pengguna internet aktif dan penyedia layanan internet seperti aplikasi dan situs web untuk memahami jenis-jenis ancaman siber dan cara mengatasinya. Beberapa cara yang dapat dilakukan untuk mengatasi ancaman siber antara lain dengan memberikan proteksi dengan kode otentik, proteksi terhadap jaringan, proteksi terhadap aplikasi yang digunakan, dan berbagai macam proteksi lainnya.

Selain itu, peretas jaringan atau "hacker" juga merupakan ancaman siber yang serius. Mereka dapat mencoba meretas sistem, mencuri data penting, atau menyusup ke dalam jaringan dengan tujuan mencapai keuntungan pribadi atau politik. Ancaman ini dapat datang dalam berbagai bentuk dan dapat menargetkan berbagai jenis infrastruktur jaringan, termasuk komputer, server, router, switch, dan perangkat jaringan lainnya.

Serangan Distributed Denial of Service (DDoS), yang dimaksudkan untuk mematikan jaringan dengan membanjirinya dengan lalu lintas, dan serangan Man-in-the-Middle (MitM), yang mencegat dan mengalihkan lalu lintas jaringan untuk mencuri informasi.

Ancaman jaringan dapat datang dari sumber internal dan eksternal. Ancaman internal mencakup karyawan yang mungkin secara sadar atau tidak sadar mengungkap informasi sensitif, sedangkan ancaman eksternal dapat mencakup peretas atau pelaku jahat yang menargetkan jaringan dengan maksud untuk menimbulkan kerugian.

Untuk melindungi dari ancaman jaringan, diperlukan pendekatan berlapis terhadap keamanan siber. Hal ini termasuk penerapan firewall dan sistem deteksi intrusi, pembaruan perangkat lunak dan patch keamanan secara berkala, penggunaan kata sandi yang kuat dan autentikasi multi-faktor, serta memberikan pelatihan keamanan siber secara berkala kepada semua pengguna jaringan. Dengan mengambil langkah-langkah ini, bisnis dapat mengurangi risiko ancaman jaringan dan menjaga keamanan jaringan.

2.3. Pengenalan Firewall dan Fungsinya

Firewall adalah komponen penting dari keamanan siber dan mengacu pada sistem keamanan jaringan yang memantau dan mengontrol lalu lintas jaringan masuk dan keluar berdasarkan aturan yang telah ditentukan. Firewall bertindak sebagai penghalang antara jaringan internal tepercaya dan jaringan eksternal yang tidak tepercaya, seperti internet, untuk mencegah akses tidak sah dan serangan berbahaya. Firewall dapat berupa peralatan perangkat keras, program perangkat lunak, atau kombinasi keduanya dan beroperasi dengan memeriksa paket data yang melewati jaringan dan memblokir akses ke lalu lintas yang tidak sah. Firewall sangat berguna untuk mencegah port scanning, brute force attack dan jenis serangan siber lainnya yang dapat mengeksploitasi kerentanan dalam jaringan dan menyebabkan kerusakan parah.

Fungsi utama dari firewall adalah untuk melakukan monitoring dan mengontrol semua akses masuk atau keluar koneksi jaringan berdasarkan aturan keamanan yang telah ditetapkan sebelumnya. Firewall juga mampu mencegah kebocoran informasi yang berharga dan mencegah pengguna mengirim file rahasia atau nilai rahasia ke pihak lain tanpa menyadarinya Oleh karena itu, firewall sangat penting untuk mencegah terjadinya hal yang tidak diinginkan dan membantu menjamin keamanan pengguna internet.

Salah satu fungsi utama firewall adalah mencegah akses yang tidak sah ke jaringan. Ini dilakukan dengan menerapkan aturan atau kebijakan yang mengizinkan atau memblokir lalu lintas berdasarkan berbagai faktor, seperti alamat IP, port, atau protokol tertentu. Dengan cara ini, firewall dapat menghalangi potensi penyerang dari luar untuk mencapai sumber daya yang ada di dalam jaringan.

Selain itu, firewall juga berperan dalam mendeteksi dan mencegah serangan siber. Ini mencakup serangan seperti serangan DDoS (Distributed Denial of Service), serangan port scanning, serangan brute force attack, dan banyak lainnya. Firewall dapat menggunakan metode seperti inspeksi berbasis tanda tangan, inspeksi berbasis perilaku, atau peringatan intrusi untuk mengidentifikasi ancaman ini dan mengambil tindakan yang sesuai, seperti memblokir alamat IP yang mencurigakan atau mengirim peringatan kepada administrator jaringan.

Firewall juga memiliki fungsi untuk mengatur akses pengguna ke sumber daya jaringan internal. Ini berarti bahwa administrator dapat menentukan siapa yang memiliki izin untuk

mengakses aplikasi, data, atau layanan tertentu dalam jaringan. Melalui autentikasi dan otorisasi, firewall memastikan bahwa hak akses sesuai dengan peran dan kebutuhan pengguna.

2.4. Pengenalan Firewall dengan Mikrotik

Sistem operasi khusus yang disebut Mikrotik didasarkan pada Linux. perangkat elektronik yang berfungsi sebagai router. Mikrotik dibuat sederhana Untuk keperluan administrasi jaringan, ini banyak digunakan. penggunaan komputer untuk tugas-tugas seperti desain dan konstruksi sistem jaringan. dari komputer sederhana hingga komputer kompleks. Awalnya ditujukan ketika Mikrotik didirikan pada tahun 1995. Penyedia layanan internet (juga dikenal sebagai ISP), klien yang memanfaatkan teknologi nirkabel. Saat ini, MikroTik menawarkan layanan ke berbagai ISP nirkabel untuk berbagai penyedia akses Internet. Indonesia adalah salah satu negara terpopuler di dunia. (Riadi, 2011)

Penggunaan firewall dengan MikroTik adalah salah satu solusi yang populer dalam mengelola keamanan jaringan MikroTik, sebagai produsen perangkat jaringan yang terkenal menyediakan berbagai perangkat keras dan perangkat lunak yang dirancang untuk menghadapi berbagai ancaman siber dengan efektif.

Firewall pada MikroTik memiliki beberapa fungsi, antara lain:

a. Melindungi jaringan dari berbagai macam serangan komputer luar, baik yang berasal dari WAN (Internet) maupun dari LAN (Local).
b. Membatasi komputer dari jaringan internet dengan cara mengatur dan melakukan penyaringan pada akses yang masuk dengan kriteria tertentu.
c. Mengontrol aliran data, mengatur dan membatasi konten, serta memprioritaskan bandwidth untuk konten-konten lebih penting untuk bisnis.
d. Menandai paket data dan koneksi tertentu yang dapat diterapkan pada fitur MikroTik lainnya, seperti pada routes, pemisahan bandwidth pada queues, NAT, dan filter rules.
e. Mencegah kebocoran informasi yang berharga dan mencegah pengguna mengirim file rahasia atau nilai rahasia ke pihak lain tanpa menyadarinya.

Salah satu keunggulan penggunaan firewall MikroTik adalah dengan menggunakan firewall pada MikroTik, pengguna internet dapat merasa lebih aman dan terlindungi dari berbagai macam serangan komputer luar. Selain itu, firewall juga dapat membantu meningkatkan efisiensi dan produktivitas bisnis dengan mengatur aliran data dan membatasi akses ke situs-situs yang tidak relevan atau tidak produktif, fleksibilitasnya dalam mengatur

aturan keamanan yang sangat detail. Ini memungkinkan administrator jaringan untuk mengontrol lalu lintas jaringan dengan presisi tinggi, memutuskan lalu lintas yang diizinkan dan yang harus diblokir berdasarkan berbagai kriteria seperti alamat IP, port, protokol, dan bahkan jenis aplikasi.

MikroTik dapat digunakan sebagai firewall untuk melindungi jaringan dari berbagai macam serangan komputer luar. Firewall pada MikroTik memiliki beberapa fitur yang dapat digunakan untuk mengawasi dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan. Beberapa fitur pada firewall MikroTik antara lain Filter Rules, NAT, Mangle, Service Ports, Connections, Address List, dan Layer 7 Protocols. Filter Rules digunakan untuk menentukan suatu paket data dapat masuk atau tidaknya kedalam sistem router MikroTik. NAT digunakan untuk melakukan port forwarding (dstnat) dan mengkoneksikan user ke jaringan internet (srcnat). Mangle digunakan untuk menandai sebuah koneksi. Service Ports digunakan untuk mengatur port-port yang digunakan oleh layanan-layanan tertentu. Connections digunakan untuk melihat koneksi-koneksi yang sedang aktif. Address List digunakan untuk membuat daftar alamat IP yang akan diizinkan atau diblokir. Layer 7 Protocols digunakan untuk mengatur lalu lintas data berdasarkan jenis protokol yang digunakan. Dengan menggunakan fitur-fitur tersebut, MikroTik dapat membantu melindungi jaringan dari ancaman siber dan menjaga keamanan pengguna internet

Dengan semua fitur dan fleksibilitas yang ditawarkannya, penggunaan firewall dengan MikroTik telah menjadi pilihan yang sangat populer dalam manajemen keamanan jaringan. Ini memberikan administrator jaringan alat yang kuat untuk melindungi infrastruktur mereka dari ancaman siber yang terus berkembang dan menjaga kelancaran operasi jaringan yang kritis.

Keuntungan lain menggunakan router MikroTik sebagai firewall adalah mendukung pemfilteran HTTPS, yang memungkinkan router mencegat dan memfilter lalu lintas web terenkripsi. Hal ini sangat berguna dalam memblokir akses ke situs web berbahaya dan mencegah serangan phishing.

BAB III
METODOLOGI PENELITIAN

3.1. Metode Pengembangan

Tipe penelitian yang akan dilakukan menggunakan Research and Development (RnD). *Research and Development* adalah aktivitas riset dasar untuk mendapatkan informasi terhadap produk yang akan dikembangkan, setelah itu produk akan dikembangkan dan diuji. *Research and Development* adalah metode dan langkah-langkah untuk menghasilkan produk baru atau mengembangkan dan menyempurnakan produk yang sudah ada untuk menguji efektivitas produk sehingga produk tersebut dapat ditinjau ulang. (Okpatrioka, 2023: 89) Adapun tahapan-tahapan penelitian yang akan dilakukan, dapat dilihat pada Gambar 3.1

Gambar 3. 1 Tahap RnD

Berdasarkan Gambar 3.1, Tahap RnD mempunyai beberapa tahapan sebagai berikut:

1. Pengumpulan Data

   Pada tahap ini dalam fokus utama adalah mengumpulkan data yang relevan dan diperlukan untuk analisis. Informasi yang dikumpulkan berkaitan dengan pengaturan jaringan saat ini atau strategi manajemen ancaman yang digunakan oleh perusahaan, seperti penerapan firewall. Pengumpulan data ini merupakan langkah awal yang penting karena akan menjadi landasan bagi langkah selanjutnya. Pengumpulan data dilakukan melalui pemeriksaan bahan studi kepustakaan yang diambil dari buku, jurnal, terbitan berkala atau media cetak lain yang terpercaya. Selain itu, dilakukan wawancara bersama pihak perusahaan.

2. Analisis Kebutuhan

   Tahap pengumpulan data akan dilanjutkan dengan tahap analisis kebutuhan. Untuk memahami masalah dan kesulitan keamanan jaringan yang perlu diselesaikan, peneliti kini akan mempelajari data yang telah dikumpulkan. Hal ini termasuk menentukan ancaman saat ini, kelemahannya, dan kemungkinan dampak serangan untuk memahami masalah dan tantangan keamanan jaringan yang perlu diatasi. Ini mencakup identifikasi ancaman yang ada, kerentanannya, dan potensi dampak jika terjadi serangan. Analisis ini juga akan membantu dalam menentukan kebutuhan spesifik yang harus dipenuhi oleh solusi keamanan, termasuk fitur dan fungsionalitas yang diperlukan dari firewall MikroTik.

3. Perancangan

   Setelah kebutuhan keamanan jaringan teridentifikasi, tahap perancangan akan dimulai. Ini mencakup perencanaan konfigurasi firewall MikroTik yang akan diimplementasikan. Pada tahap ini, peneliti akan merancang aturan-aturan keamanan yang sesuai dengan kebutuhan, seperti mengatur akses, mengelola aliran lalu lintas, dan menentukan cara mengatasi ancaman tertentu. Desain ini harus mempertimbangkan arsitektur jaringan yang ada dan memastikan bahwa firewall akan berintegrasi dengan lancar.

4. Implementasi

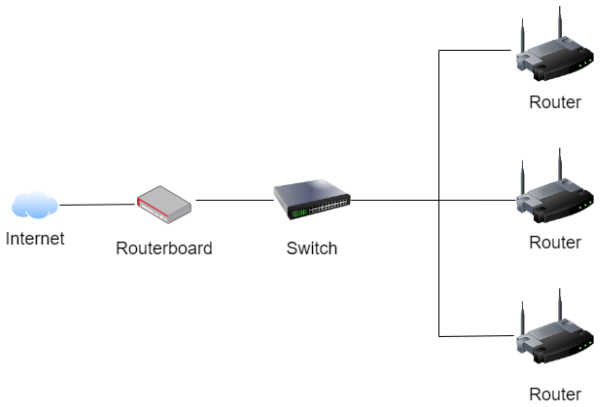
Setelah perancangan selesai, tahap implementasi akan dimulai. Ini adalah saat di mana konfigurasi firewall MikroTik yang telah dirancang akan diterapkan pada lingkungan jaringan yang sesungguhnya. Administrator jaringan akan memasang perangkat keras MikroTik jika diperlukan, mengatur aturan-aturan keamanan, dan menguji pengaturan. Implementasi yang cermat dan tepat adalah kunci untuk memastikan firewall berfungsi sesuai rencana dan melindungi jaringan dengan efektif.

5. Rancangan Pengujian

Setelah firewall MikroTik diimplementasikan, langkah selanjutnya adalah rancangan pengujian. Ini merupakan tahap penting untuk memastikan keamanan jaringan yang diterapkan dapat berkinerja dengan baik. Pengujian akan mencakup simulasi serangan, pengujian keandalan, dan penilaian apakah aturan-aturan keamanan berfungsi seperti yang diharapkan. Hasil dari pengujian ini akan digunakan untuk menilai apakah firewall MikroTik efektif dalam mengatasi ancaman dan apakah perlu dilakukan penyesuaian atau perbaikan.

3.2. Analisis Kebutuhan

Analisis kebutuhan adalah proses untuk mendapatkan kebutuhan dari sistem yang akan diteliti. Kebutuhan sistem didapatkan dari hasil wawancara dan studi penelitian terdahulu yang memiliki kaitan dengan penelitian ini, sehingga sistem yang dibuat dapat memenuhi kebutuhan.



Gambar 3. 2 Topologi Non Firewall

Gambar diatas menggunakan mikrotik tetapi tidak memanfaatkan fitur firewallnya.

Tabel 3. 1 Kelemahan dan Kebutuhan Sistem

No	Kelemahan	Kebutuhan
1	Tidak ada firewall yang digunakan	Dibutuhkan perangkat mikrotik yang dapat memfilter data yang ingin keluar masuk.

Software dan hardware yang dibutuhkan dalam proses pelaksanaan penelitian adalah sebagai berikut

a. Software :
b. Winbox
c. Advanced Port Scanner
d. Script DDoS
e. Command Promt
f. Putty

Hardware:

a. Routerboard Mikrotik RB951Ui 2HnD
b. Kabel lan
c. Laptop
d. Akses internet

3.3. Analisis Pengguna Sistem

Analisis pengguna sistem merupakan tahapan penting dalam proses pengembangan teknologi informasi, yang tujuan utamanya adalah memahami kebutuhan, preferensi dan harapan masyarakat yang akan menggunakan sistem. Melalui analisis ini, pengembang perangkat lunak dapat mengumpulkan informasi berharga tentang bagaimana pengguna berinteraksi dengan sistem, apa yang diharapkan dari sistem, dan apa yang akan membuat pengalaman pengguna menjadi efektif dan lebih memuaskan.

Proses analisis pengguna sistem mencakup identifikasi berbagai pengguna potensial, memahami peran dan tugas mereka dalam menggunakan sistem, dan menentukan kebutuhan fungsional dan non-fungsional yang perlu dipenuhi. Analisis ini juga membantu

mengidentifikasi tantangan atau hambatan yang mungkin dihadapi pengguna saat berinteraksi dengan sistem.

Analisis pengguna sistem dalam konteks ini mencakup mengidentifikasi peran pengguna yang berbeda di PT Dinamika Mediakom, seperti administrator jaringan, staf TI, dan mungkin pemilik bisnis. Setiap kelompok pengguna memiliki kebutuhan unik terkait pengelolaan dan pemantauan keamanan siber. Pemahaman menyeluruh tentang peran dan tanggung jawab setiap pengguna sangat penting untuk merancang kebijakan keamanan yang tepat.

Selain itu analisisnya mencakup pemahaman terhadap lingkungan jaringan saat ini di PT Dinamika Mediakom, termasuk infrastruktur, perangkat keras, dan perangkat lunak yang digunakan. Hal ini membantu memahami bagaimana solusi firewall dengan MikroTik dapat diintegrasikan secara mulus ke dalam lingkungan yang ada. Analisis kebutuhan pengguna juga mencakup pengenalan ancaman siber yang pernah atau mungkin dihadapi PT Dinamika Mediakom. Informasi ini membantu merancang aturan firewall yang efektif untuk menghadapi kemungkinan serangan.

Selain itu, pemahaman tingkat kompetensi teknis pengguna PT Dinamika Mediakom akan mempengaruhi desain antarmuka pengguna agar mudah digunakan dan dipahami oleh semua pihak yang terlibat dalam manajemen keamanan siber. Secara keseluruhan, analisis pengguna sistem memberikan dasar yang diperlukan untuk merancang, menerapkan, dan mengelola solusi keamanan jaringan yang disesuaikan dengan kebutuhan dan lingkungan unik PT Dinamika Mediakom. Hal ini akan membantu melindungi infrastruktur jaringan dari berbagai ancaman siber dan menjaganya tetap berjalan lancar.

3.4. Pengumpulan Data

Pada penelitian ini pengumpulan data dilakukan dengan observasi, studi pustaka, dan wawancara.

a. Observasi

Observasi merupakan kegiatan mencari informasi yang berkaitan dengan penelitian. Dalam penelitian ini akan melakukan observasi mengenai serangan yang

sering dilakukan kepada routerboard sehingga dapat menanggulangi dan meminimalisir kebocoran data yang akan terjadi.

b. Studi pustaka

Studi pustaka adalah kegiatan mempelajari penelitian-penelitian terdahulu seperti jurnal dan buku-buku yang memuat informasi atau dokumen yang berkaitan dengan penelitian ini sehingga dapat membantu dalam perancangan dan persiapan penelitian ini. Studi pustaka yang dimaksud untuk meneliti berbagai dokumen, jurnal, buku ataupun media cetak mengenai manajemen keamanan jaringan yang serupa dengan yang akan dikembangkan. Kajian pustaka yang digunakan adalah jurnal, buku dan website kredibel.

c. Wawancara

Wawancara adalah kegiatan mengumpulkan informasi melalui tanya jawab dengan narasumber yang relevan atau berkaitan dengan penelitian ini sehingga mendapatkan informasi yang berguna untuk penelitian ini. Saat pengumpulan informasi dilakukan dengan wawancara kepada Ahli IT pada perusahaam.

3.5. Kebutuhan Sistem

Kebutuhan sistem perangkat lunak atau sistem teknologi informasi adalah serangkaian pernyataan atau spesifikasi yang menguraikan apa yang diharapkan darinya. Ini adalah kriteria tepat yang diikuti oleh para insinyur perangkat lunak saat merancang, membuat, dan menguji sistem untuk memastikan sistem tersebut dapat memenuhi permintaan dan tujuan pengguna. Kebutuhan sistem mencakup berbagai topik, termasuk fungsi utama sistem, antarmuka pengguna, kinerja, keamanan, dan integrasi sistem. Mereka juga dapat menentukan bagaimana sistem harus menangani data, bagaimana aturan bisnis harus dipatuhi, dan pemantauan dan pelaporan apa yang harus dilakukan.

Analisis kebutuhan sistem yang efektif merupakan langkah awal yang penting dalam pembuatan perangkat lunak atau teknologi informasi. Hal ini memudahkan untuk memahami apa yang diinginkan pengguna dan pemangku kepentingan lainnya tanpa kebingungan atau kesalahpahaman, sehingga menghasilkan sistem yang efektif, dapat diandalkan, dan sesuai tujuan. Landasan keberhasilan mengarahkan seluruh proses pengembangan sistem adalah terciptanya persyaratan sistem yang jelas dan menyeluruh.

Analisis kebutuhan sistem dapat dibagi menjadi empat aspek utama berdasarkan jenis kebutuhan yang diketahui: kebutuhan input, proses, antarmuka, dan kebutuhan output. Inilah cara pandang yang lebih terperinci:

1. Kebutuhan input

   Kebutuhan input untuk penelitian ini mencakup data yang diperlukan untuk analisis ancaman dan keamanan siber. Hal ini mencakup data historis serangan cyber sebelumnya yang terjadi terhadap PT Dinamika Mediakom, data konfigurasi jaringan yang ada, dan informasi mengenai kebijakan keamanan yang diterapkan. Selain itu masukannya berupa wawancara dengan staf IT atau manajer jaringan untuk memahami kebutuhan dan harapan mereka terhadap sistem keamanan yang akan diterapkan.

2. Kebutuhan proses

   Kebutuhan proses mencakup langkah-langkah yang diperlukan untuk menganalisis ancaman, merancang aturan keamanan, dan menerapkan firewall dengan MikroTik. Hal ini mencakup proses mengidentifikasi potensi ancaman, menentukan aturan firewall yang sesuai, dan mengintegrasikan solusi keamanan ke dalam infrastruktur jaringan yang ada pada PT Dinamika Mediakom.

3. Kebutuhan antarmuka

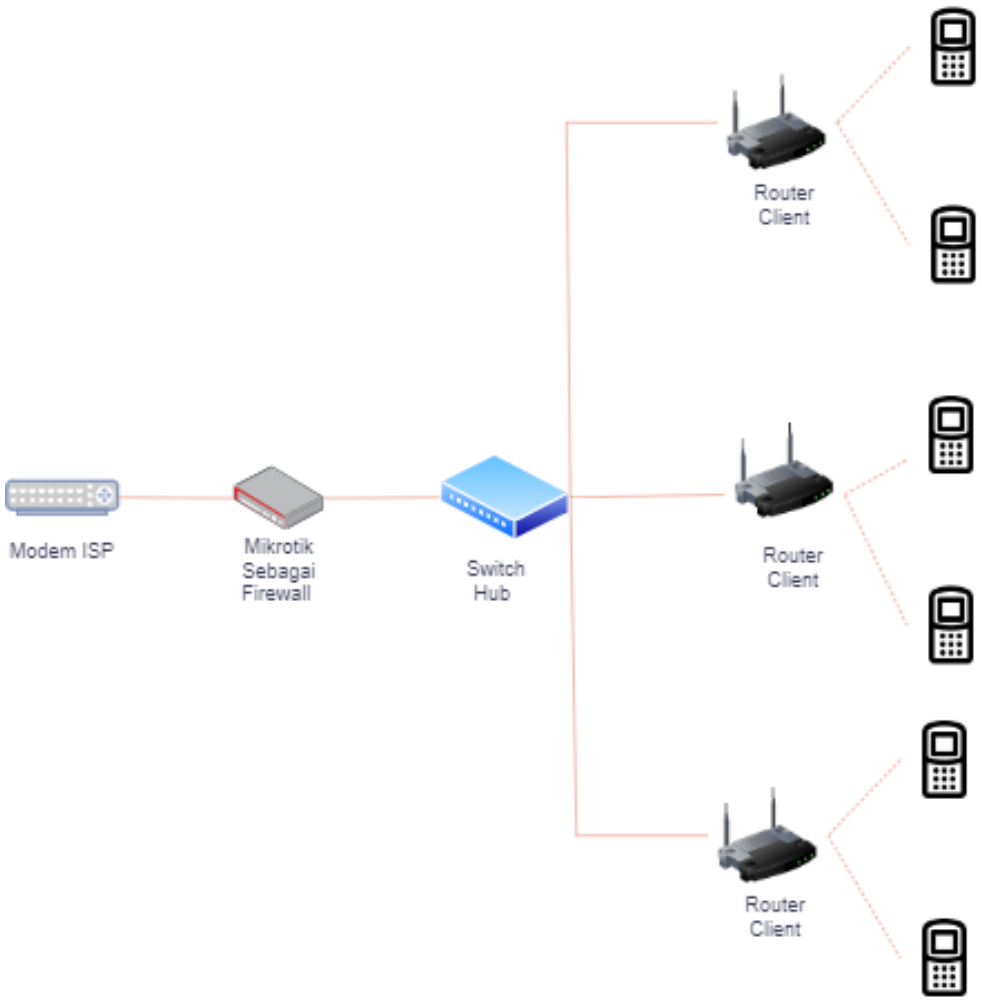
   Dalam konteks penelitian ini, kebutuhan antarmuka mencakup desain dan pengaturan antarmuka firewall MikroTik. Ini termasuk konfigurasi antarmuka berbasis teks atau GUI (Graphical User Interface) yang akan digunakan untuk mengelola dan memantau firewall. Kebutuhan antarmuka juga dapat mencakup pelaporan keamanan yang mudah dimengerti oleh pengguna atau personel IT PT Dinamika Mediakom.

4. Kebutuhan output

   Kebutuhan output mencakup hasil analisis ancaman, laporan keamanan, dan pemberitahuan potensi serangan. Dalam pencarian ini, hasil mungkin juga mencakup dokumen konfigurasi MikroTik Firewall yang perlu dibuat untuk referensi dan pemeliharaan di masa mendatang. Hasil ini akan membantu membuat keputusan yang tepat terkait keamanan siber.

3.6. Perencangan

Pada tahap rancangan menggunakan metode firewall filtering untuk membuka dan menutup aksess yang akan di izinkan atau tidaknya. Dengan metode firewall filtering adalah metode yang efektif untuk melakukan management ancaman keamanan jaringan karena dapat melakukan buka tutup akses sesuai dengan apa yang dibutuhkan.



Gambar 3. 3 Topologi dengan Firewall

Pada tahap rancangan ini menggunakan metode firewall filtering untuk membuka dan menutup akses yang akan di izinkan atau tidaknya. Dengan metode firewall filtering adalah metode yang efektif untuk melakukan management ancaman keamanan jaringan karena dapat melakukan buka tutup akses sesuai dengan apa yang dibutuhkan.

3.7. Implementasi

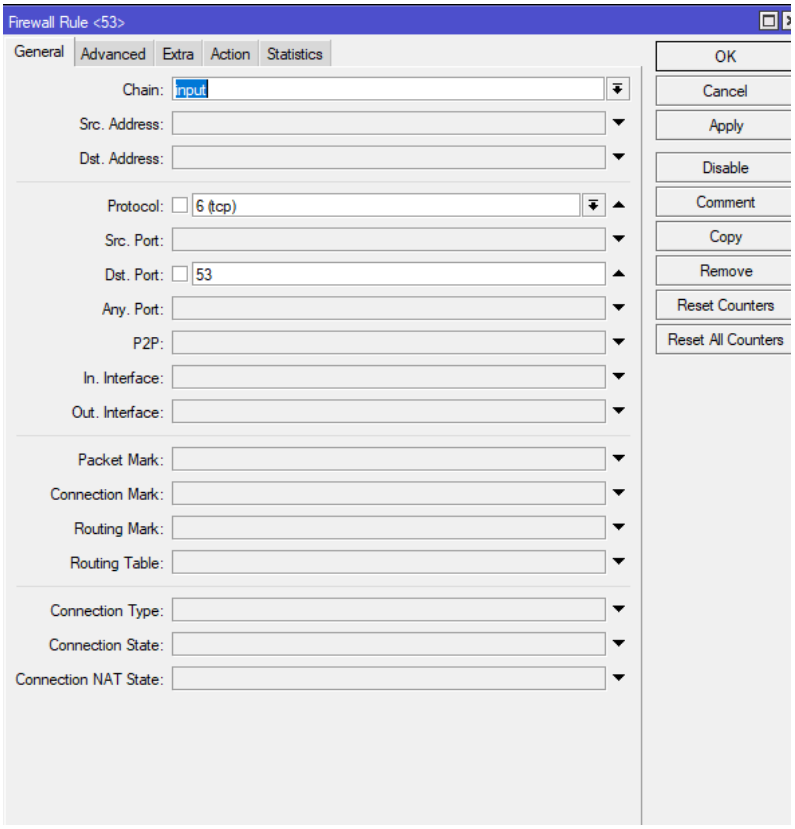
Implementasi merupakan tahap yang melakukan konfigurasi rule firewall, yang berfungsi menutup port komunikasi yang tidak digunakan dan pembatasan akses penggunaan jaringan internet.

Berikut konfigurasi serangan yang akan dilakukan :

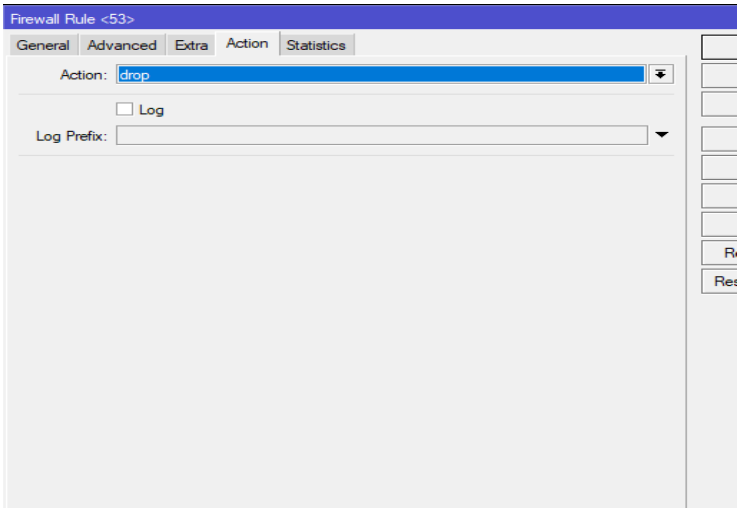
1. Serangan DDoS

   Dapat dilakukan konfigurasi dengan masuk ke tahap IP > Firewall > Filter Rule

   Konfigurasi dibawah ini untuk memfilter setiap paket data yang masuk pada protol tcp dan dengan port 53 yaitu port ftp dan setiap paket data yang masuk akan ditutup atau diblokir.



Gambar 3. 4 *Konfigurasi general Firewall untuk DDoS*

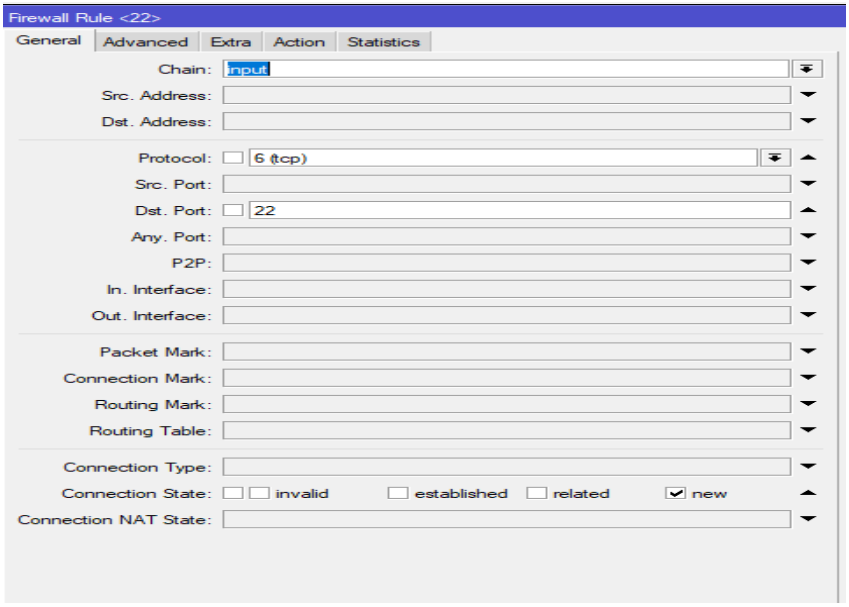


Gambar 3. 5 *Konfigurasi action Firewall untuk DDoS*

2. Serangan Brute Force Attack

Brute Force Attack dilakukan dengan berbagai cara dengan mencoba melakukan dengan menggunakan SSH dan Telnet.

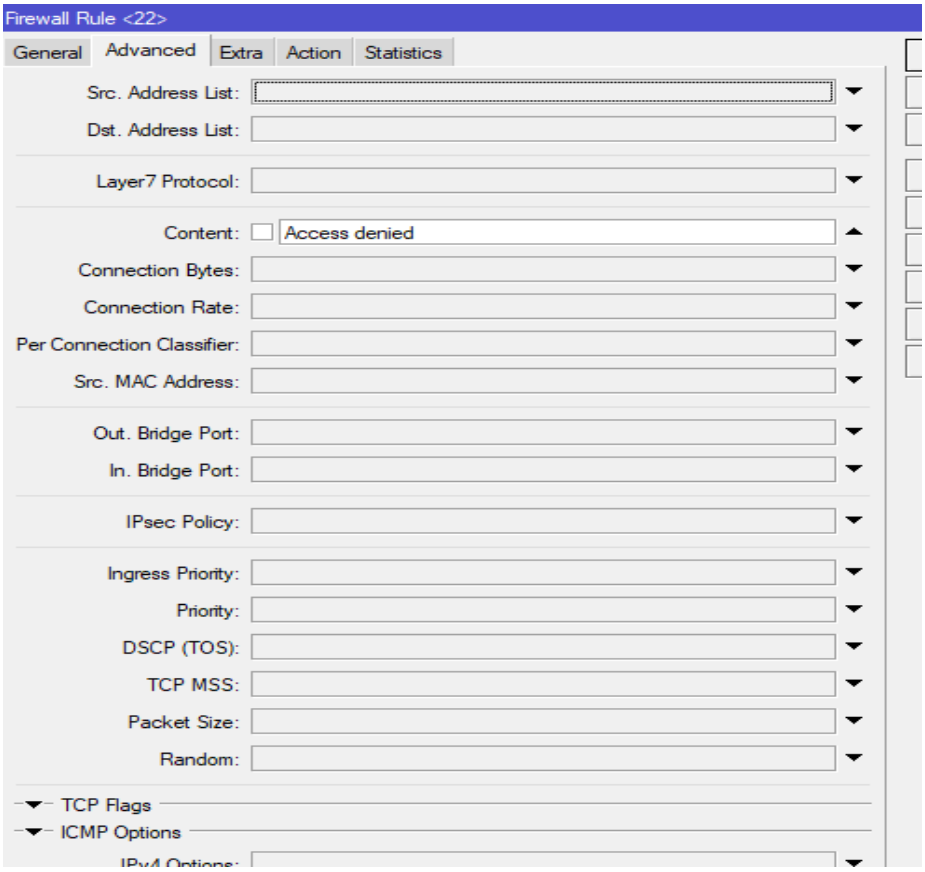
Pada konfigurasi ini untuk memfilter paket masuk dengan protokol tcp pada port ssh yaitu 22 jika ada yang mencoba login dan memasukan sandi yang salah akan muncul “access denied” kemudian jika ada seseorang yang mencoba login berkali kali IP akan di masukkan ke dalam daftar blacklist dan akan di blok selama 10 hari.



Gambar 3. 6 *Konfigurasi general Firewall untuk Brute Force Attack dengan SSH*

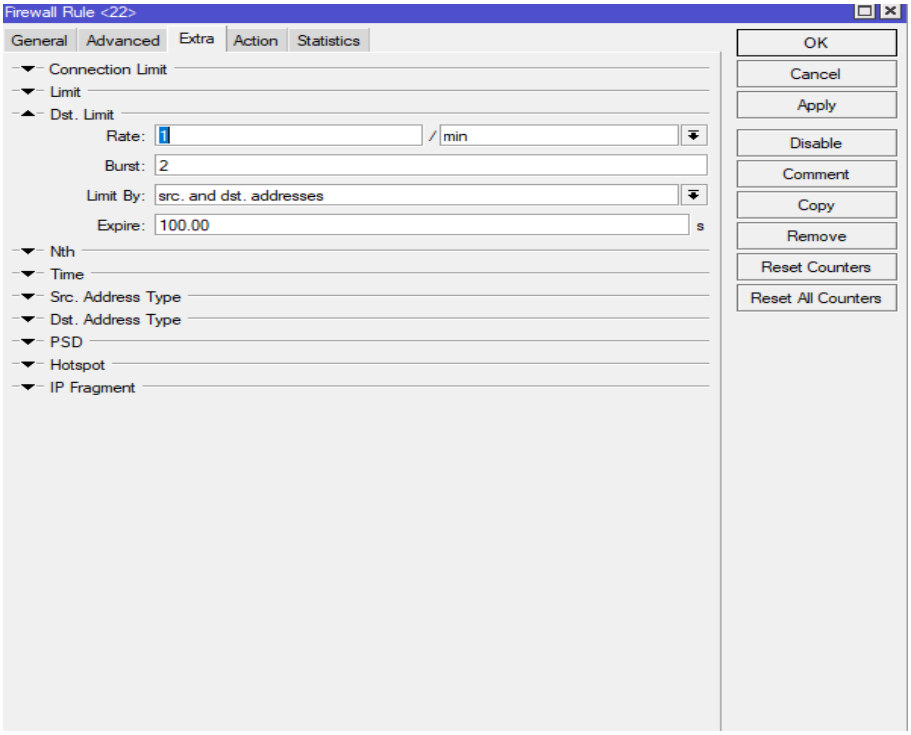
Content : Access denied

Pada konfigurasi ini akan menampilkan pesan “Access denied” setiap percobaan login yang gagal.



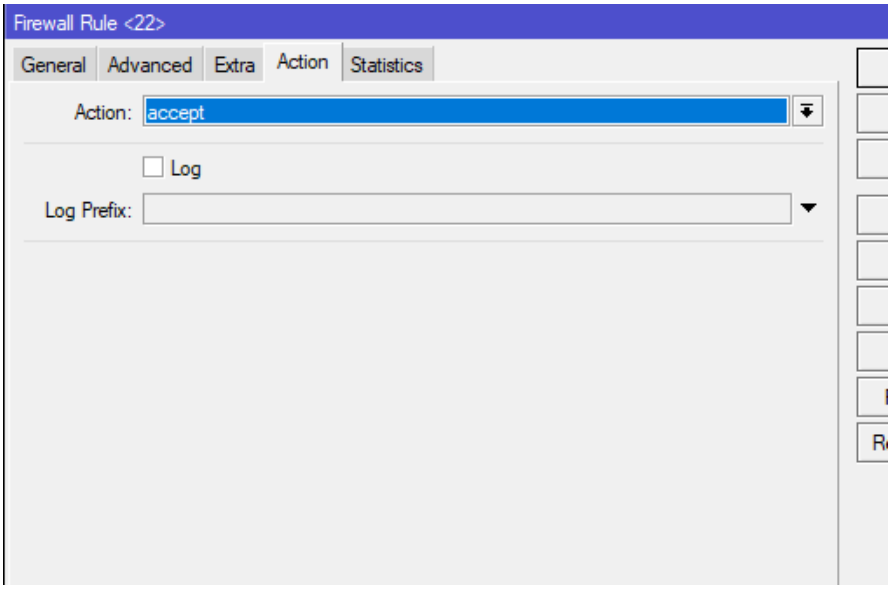
Gambar 3. 7 *Konfigurasi text yang ditampilkan*

Konfigurasi dibawah ini untuk membuat limit percobaan login dan kemudian IP Address yang melakukan percobaan login akan dimasukan kedalam list.



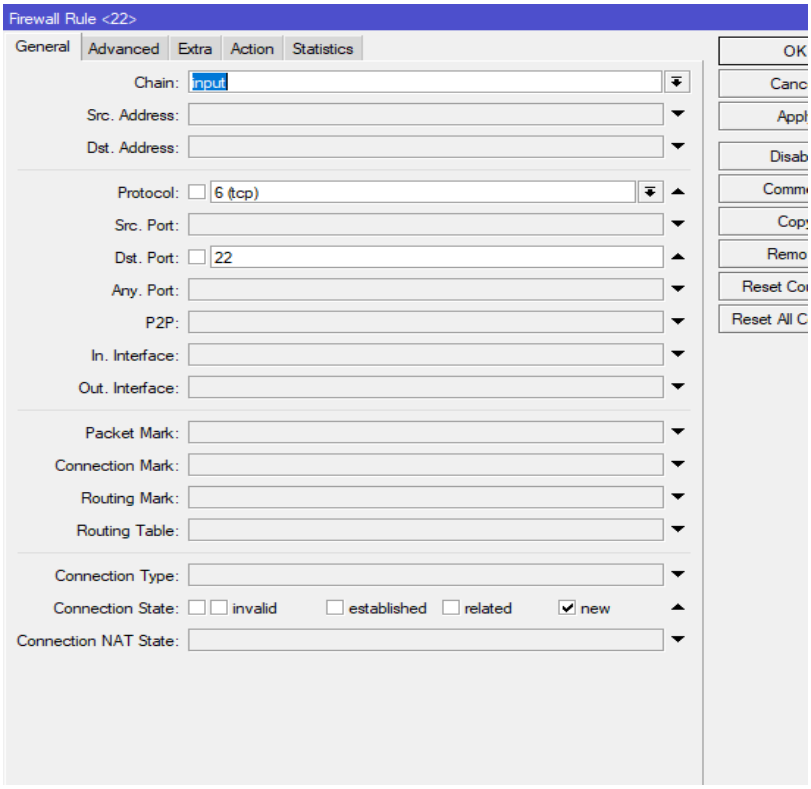
Gambar 3. 8 Konfigurasi limit Firewall untuk Brute Force Attack dengan SSH

Konfigurasi ini mengizinkan untuk IP Address yang sudah masuk ke dalam list.



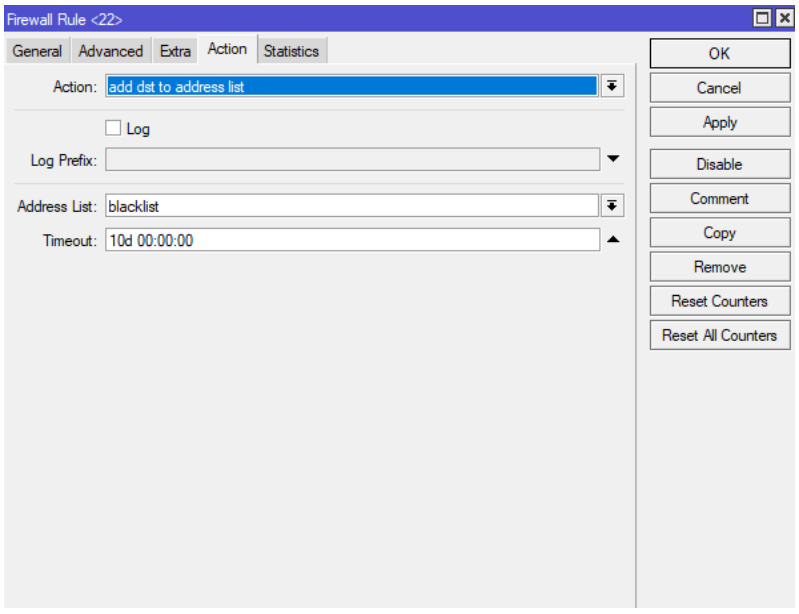
Gambar 3. 9 Konfigurasi action Firewall untuk Brute Force Attack dengan SSH

Pada konfigurasi ini untuk memfilter paket masuk dengan protokol tcp pada port ssh.



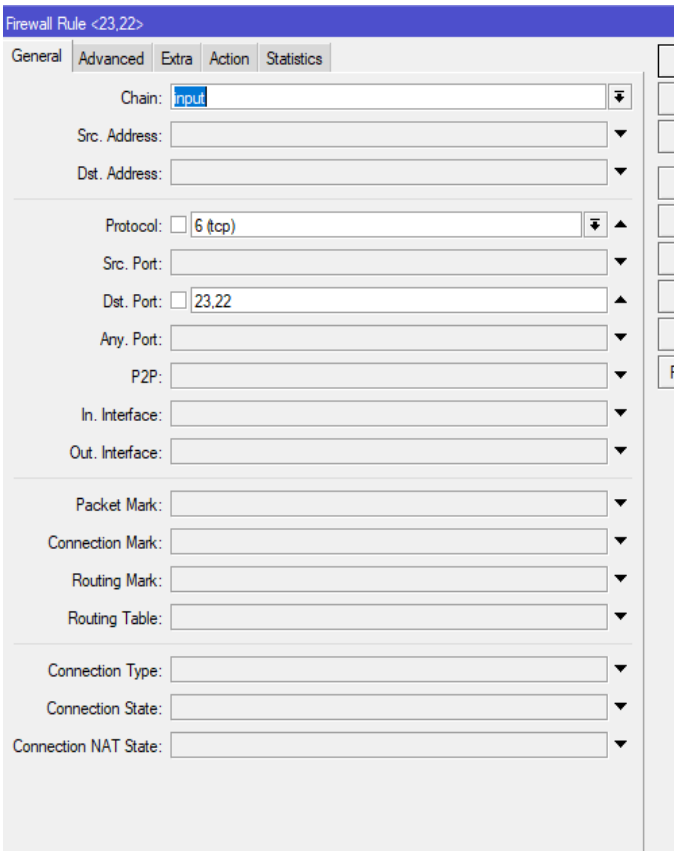
Gambar 3. 10 Filter Rules baru untuk daftar blacklist

Konfigurasi ini untuk meneruskan IP Address yang sudah dilist kedalam daftar hitam dan akan di blokir selama 10 hari.



Gambar 3. 11 *Konfigurasi Firewall tambah ip yang di blacklist di Brute Force Attack*

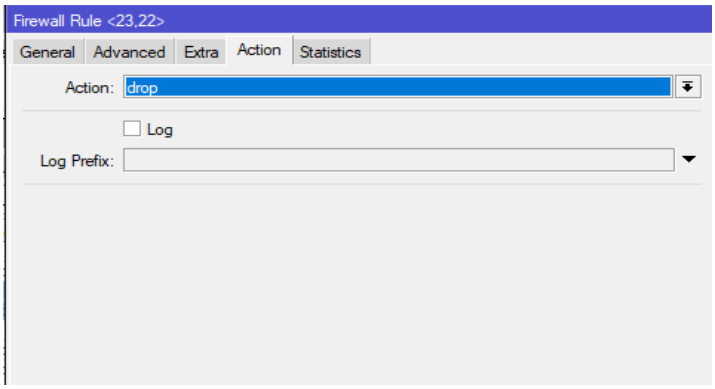
Pada konfigurasi ini untuk memfilter paket masuk dengan protokol tcp pada port ssh dan telnet.



Gambar 3. 12 *Filter Rules untuk SSH dan Telnet*

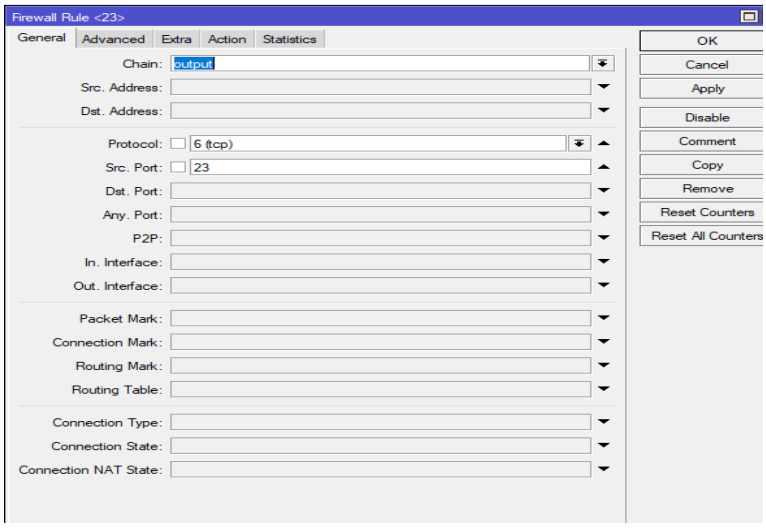
Action : drop

Untuk memblokir dan membatasi IP Address yang masuk kedalam daftar hitam.



Gambar 3. 13 *Action drop oleh port SSH dan Telnet*

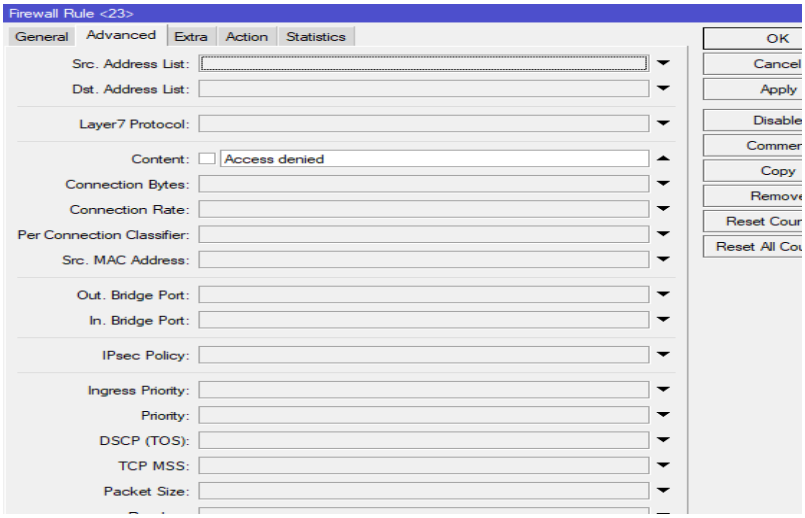
Konfigurasi ini untuk memfilter paket keluar dengan protokol tcp pada port telnet.



Gambar 3. 14 Konfigurasi general Telnet

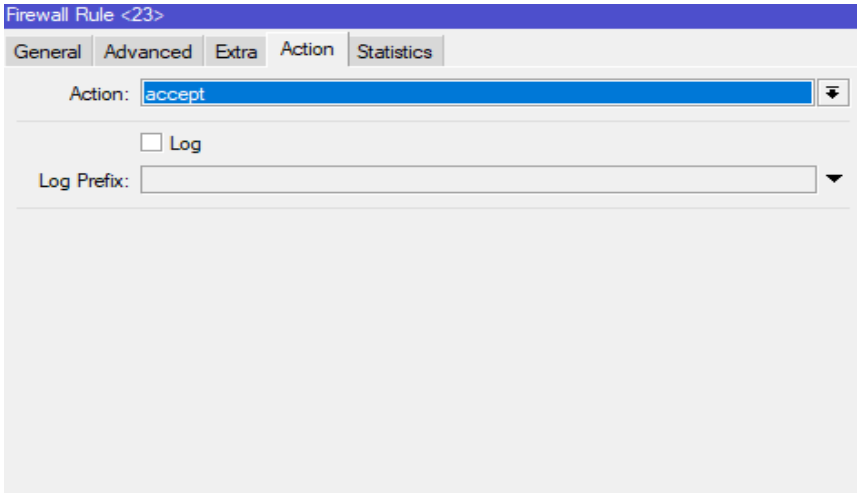
Content : Access denied

Pada konfigurasi ini akan menampilkan pesan “Access denied” setiap percobaan login yang gagal.



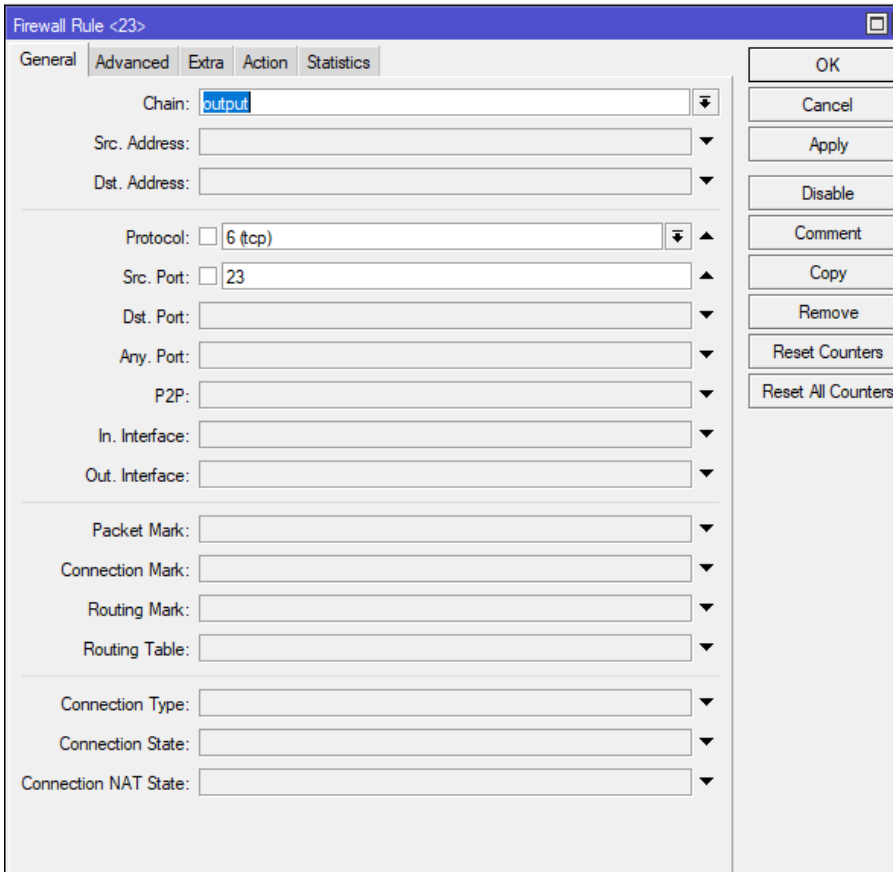
Gambar 3. 15 *Konfigurasi text Telnet*

Konfigurasi untuk mengizinkan paket tersebut.



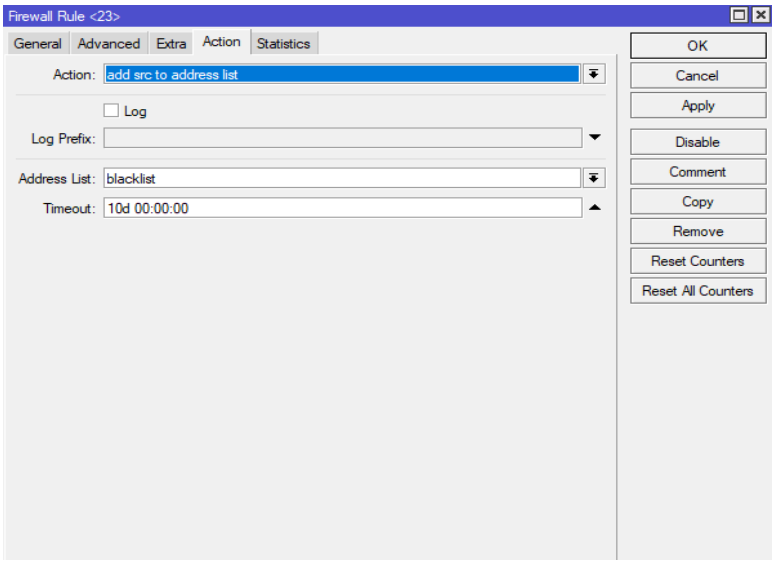
Gambar 3. 16 *Konfigurasi action Telnet*

Konfigurasi ini untuk memfilter paket keluar dengan protokol tcp pada port telnet.



Gambar 3. 17 *Filter Rules baru Telnet untuk blacklist*

Konfigurasi ini untuk meneruskan IP Address yang sudah dilist kedalam daftar hitam dan akan di blokir selama 10 hari.

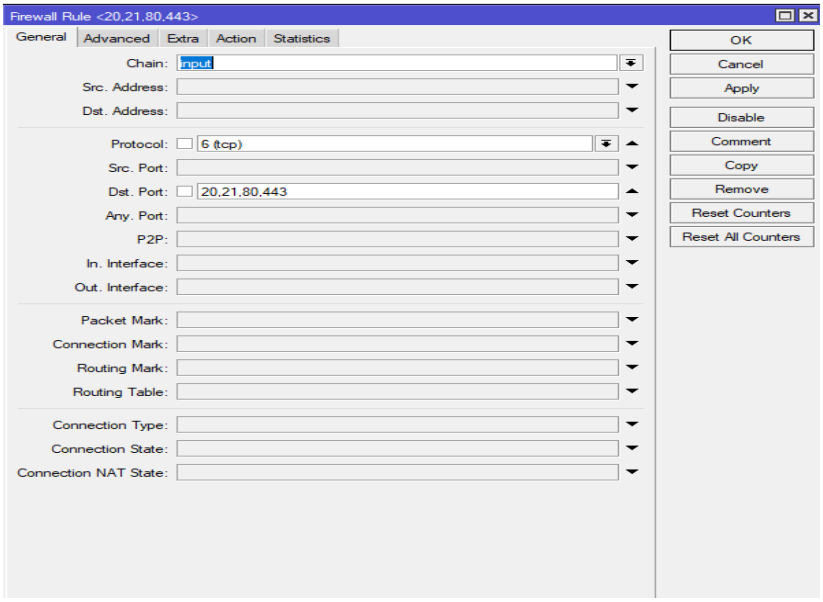


Gambar 3. 18 *Action Firewall Telnet*

3. Serangan Port Scanning

Dapat dilakukan konfigurasi dengan masuk ke tahap IP > Firewall > Filter Rule

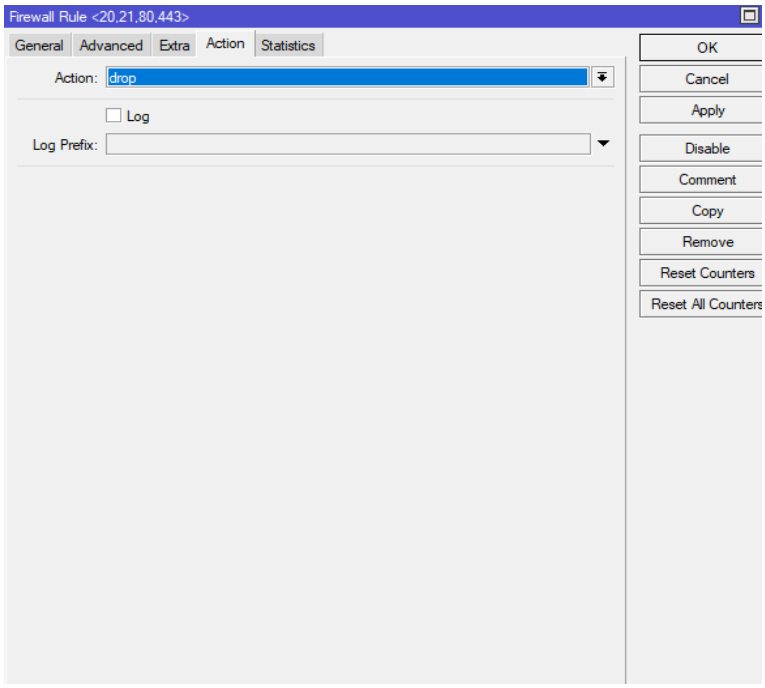
Pada konfigurasi ini untuk memfiter paket yang masuk dengan port 20,21,80 dan 443 yaitu port untuk FTP, HTTP dan HTTPS



Gambar 3. 19 *Konfigurasi firewall menutup port*

Action : drop

Untuk menutup port yang telah ditentukan



Gambar 3. 20 *Action drop Port Scanning*

3.8. Rencana Pengujian

Dalam rangka mengevaluasi efektivitas implementasi metode firewall filtering pada jaringan lokal, tahap pengujian menjadi langkah kunci. Pengujian ini bertujuan untuk menguji sejauh mana sistem keamanan yang telah diterapkan dapat melindungi jaringan dari berbagai ancaman siber yang mungkin terjadi.

Pengujian dilakukan dengan metode blackbox melalui berbagai serangan siber yang direplikasi dalam lingkungan yang terkendali. Pertama, jaringan diserang dengan serangan DDoS (Distributed Denial of Service), yang membanjiri jaringan dengan lalu lintas palsu untuk melihat apakah firewall mampu mengidentifikasi dan memblokir serangan tersebut. Kemudian, pengujian dilanjutkan dengan simulasi brute force attack menggunakan protokol SSH dan Telnet, yang mencoba untuk mencari celah dalam keamanan dengan mencoba kombinasi kata sandi yang berbeda. Selanjutnya, pengujian melibatkan serangan port scanning yang bertujuan untuk mengeksplorasi lubang keamanan potensial dalam jaringan dengan memeriksa port yang terbuka

BAB IV
HASIL DAN PEMBAHASAN

4.1. Implementasi Sistem Pengujian

Penyebaran sistem pengujian serangan menggunakan MikroTik merupakan langkah penting dalam menjaga keamanan jaringan. Sistem ini dirancang untuk mengidentifikasi dan menguji seberapa baik sistem keamanan yang diterapkan di lingkungan jaringan dapat melindungi terhadap tiga jenis serangan cyber utama, yaitu serangan DDoS (Denial of Service) terdistribusi), serangan brute force, dan pemindaian port.

Serangan DDoS adalah jenis serangan yang bertujuan untuk menyelimuti jaringan dengan lalu lintas yang sangat tinggi, sehingga sumber daya jaringan tidak dapat diakses oleh pengguna yang sah. Penerapan pengujian DDoS pada sistem ini dimaksudkan untuk mereproduksi serangan tersebut guna mengukur kemampuan firewall MikroTik dalam menangani lonjakan lalu lintas yang tidak biasa. Hasil pengujian DDoS akan membantu menentukan apakah jaringan memiliki perlindungan yang memadai terhadap serangan tersebut. Selain itu, pengujian tersebut mencakup serangan brute force, upaya menebak kata sandi dengan menguji berbagai kombinasi. Biasanya, protokol SSH dan Telnet menjadi sasaran serangan ini. Sistem ini akan mencoba mengevaluasi apakah firewall MikroTik dapat mendeteksi dan memblokir serangan brute force atau apakah serangan tersebut berhasil menembus sistem. Jika serangan ini berhasil, kebijakan keamanan dan pengaturan firewall perlu dievaluasi dan diperkuat.

Pemindaian port, sebuah serangan yang mencari kerentanan keamanan dengan memeriksa port yang terbuka, juga sedang diuji. Sistem akan mencoba mereproduksi jenis serangan ini untuk menentukan apakah firewall MikroTik dapat mendeteksi aktivitas mencurigakan dan memblokir upaya pemindaian port. Dengan mengidentifikasi dan mengatasi jenis serangan ini, jaringan akan lebih tangguh dalam upaya menemukan pelanggaran keamanan.

Hasil pengujian ini akan memberikan informasi berharga mengenai efektivitas sistem keamanan yang ada. Jika firewall MikroTik dapat mengatasi ketiga jenis serangan tersebut, maka akan menjadi bukti positif bahwa langkah keamanan yang dilakukan cukup kuat. Namun, jika kelemahan teridentifikasi, hal ini akan memungkinkan tim keamanan untuk

melakukan perbaikan dan peningkatan yang diperlukan untuk memperkuat pertahanan jaringan. Oleh karena itu, penerapan sistem pengujian serangan ini merupakan langkah penting dalam menjaga keamanan jaringan dan melindungi aset informasi.

4.2. Hasil Pengujian Sistem

4.2.1. Penyerangan DDOS

DDos adalah metode serangan yang melibatkan pengiriman banyak paket melalui jaringan, mencegah perangkat jaringan bekerja sebagaimana mestinya. Serangan DDoS merupakan serangan yang sangat umum dan dapat dilakukan oleh hacker dari mana saja. Serangan ini dapat menyebabkan server crash dan menyebabkan kesalahan sistem. (Mukmin, 2022: 282-283).

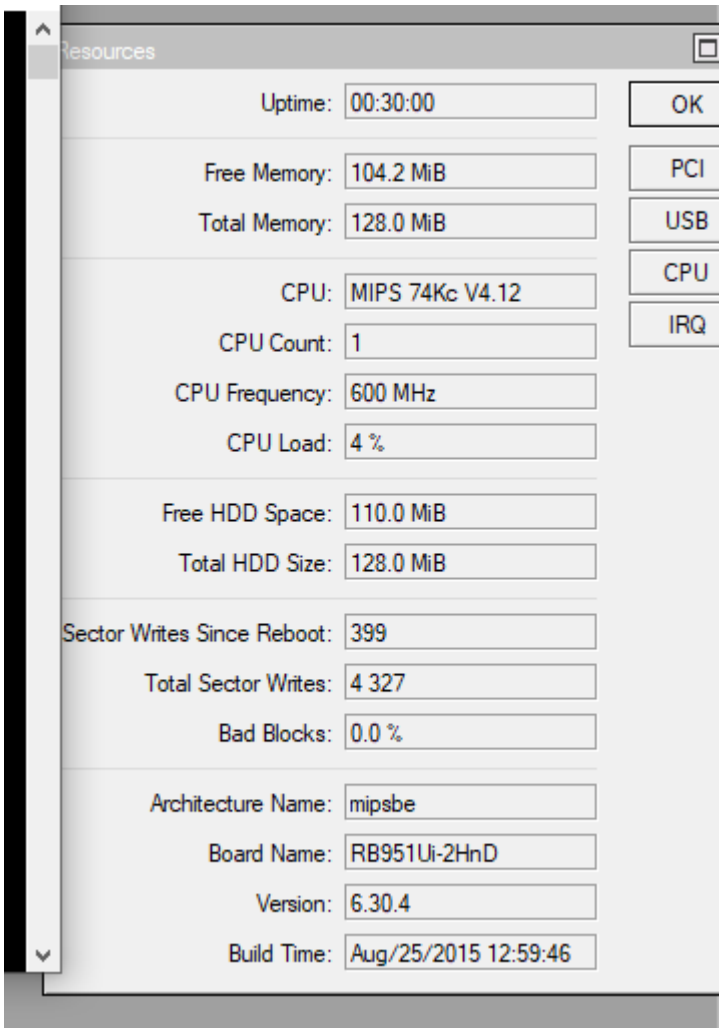
Pengujian DDoS (Distributed Denial of Service) dengan MikroTik merupakan bagian penting dalam menjaga dan meningkatkan keamanan jaringan. Serangan DDoS telah menjadi ancaman serius bagi berbagai jenis organisasi dan jaringan, yang bertujuan melumpuhkan layanan karena kelebihan lalu lintas. Oleh karena itu, pengujian sistem ini menjadi langkah penting untuk memastikan bahwa jaringan dapat bertahan dan berfungsi dengan baik dalam menghadapi serangan tersebut.

Selama pengujian sistem DDoS, skenario serangan direplikasi dalam lingkungan yang terkendali. Skenario ini melibatkan sejumlah besar komputer atau perangkat yang bersatu untuk mengirimkan lalu lintas ke target, sehingga menciptakan lonjakan lalu lintas. Tujuannya adalah untuk menguji apakah firewall MikroTik dapat mengidentifikasi serangan ini dan mengambil tindakan untuk memblokir alamat IP atau pola lalu lintas yang mencurigakan. Tes ini juga akan mengevaluasi apakah sumber daya jaringan, seperti bandwidth, CPU, dan memori, mampu menangani lalu lintas yang sangat padat.

Selain itu, pengujian DDoS juga membantu organisasi mempersiapkan rencana darurat dan taktik respons yang efektif ketika menghadapi serangan di dunia nyata. Dengan memahami kemampuan sistem dalam mengatasi serangan DDoS, organisasi dapat mengambil langkah proaktif untuk meningkatkan ketahanan dan meminimalkan dampak serangan tersebut terhadap operasi mereka.

Pengujian sistem DDoS dengan MikroTik menjadi elemen penting dalam upaya menjaga keandalan dan kinerja jaringan, sekaligus melindungi aset dan layanan dari ancaman DDoS yang semakin sering terjadi. Hal ini merupakan investasi penting untuk menjaga kelangsungan operasional dan integritas data di dunia yang semakin terhubung dan rentan terhadap serangan siber.

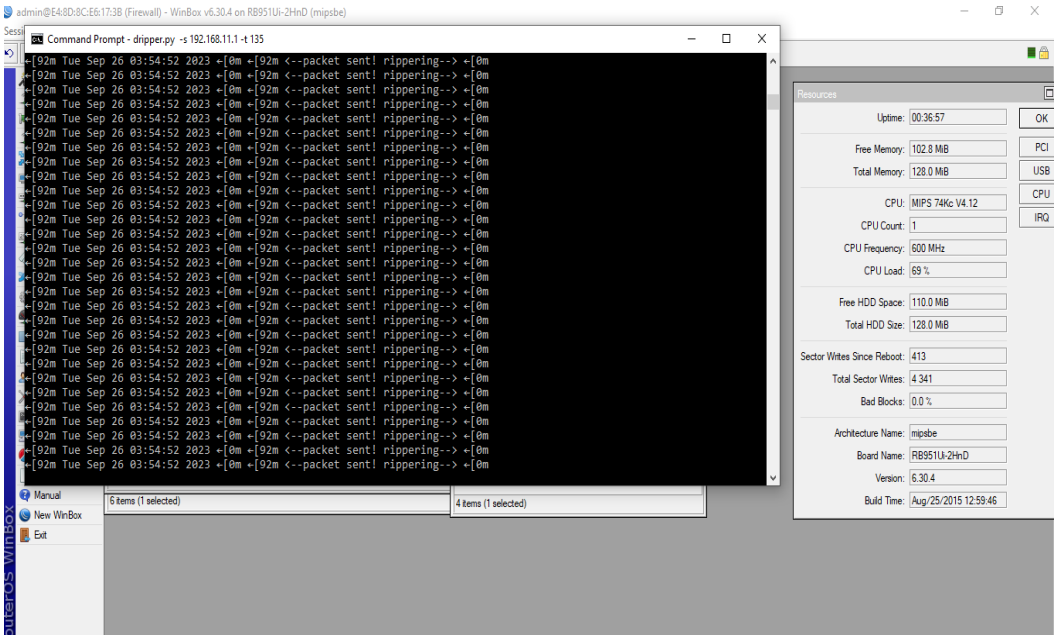
Pada kasus dalam penelitian ini, serangan DDoS di uji dengan sebagai berikut:



Gambar 4. 1 Kondisi Sistem sebelum diserang oleh DDoS

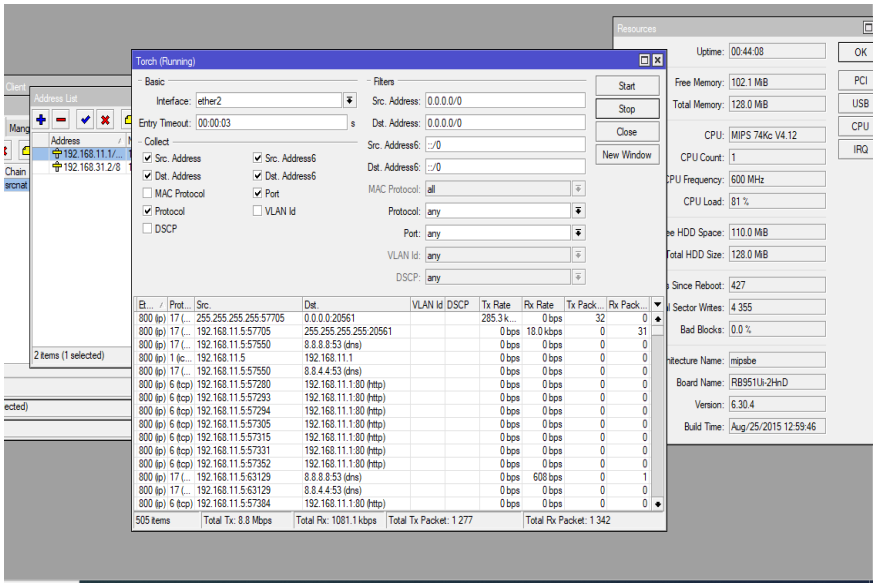
Kondisi sebelum diserang, cpu load rendah. Kondisi sebelum diserang, CPU load rendah adalah gambaran tentang situasi yang seringkali terjadi pada sistem jaringan yang belum terkena serangan DDoS. Pada saat itu, CPU load atau beban pemrosesan pada perangkat MikroTik yang menjadi bagian dari infrastruktur jaringan beroperasi dalam

kisaran yang rendah, menunjukkan bahwa sistem sedang berfungsi dengan baik dan tidak terlalu diberatkan oleh tugas pemrosesan yang berlebihan.



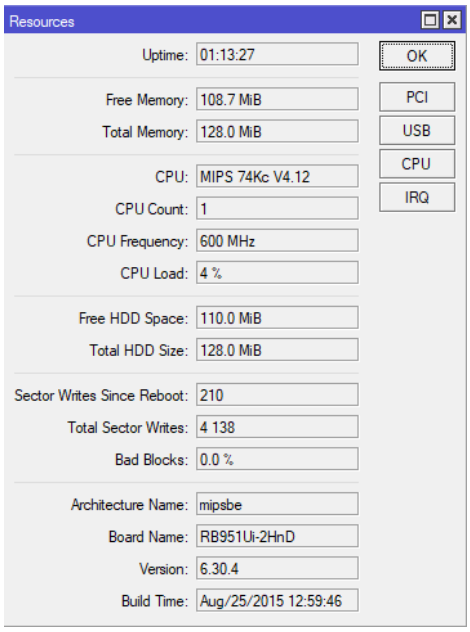
Gambar 4. 2 Serangan DDoS

Setelah di serang cpu load naik dan log juga terdeteksi banyak spam trafik. Ketika serangan DDoS terjadi, perubahan signifikan terlihat pada sistem. Beban CPU, awalnya rendah, tiba-tiba melonjak. Ini adalah hasil dari upaya sistem untuk memproses dan memproses lalu lintas yang padat akibat serangan DDoS. Perangkat MikroTik dan infrastruktur jaringan lainnya semakin tertekan ketika mereka mencoba memblokir, mengidentifikasi, dan merespons serangan berulang-ulang. Selain lonjakan beban CPU, log sistem juga mendeteksi peningkatan nyata dalam lalu lintas spam masuk. Serangan DDoS sering kali disertai dengan upaya membanjiri jaringan dengan lalu lintas yang tidak terkait dan merusak. Log ini dapat mencatat berbagai upaya serangan yang bertujuan membebani sistem secara berlebihan dan mengganggu kinerja jaringan secara keseluruhan.



Gambar 4. 3 Hasil Sebelum Menggunakan Firewall

Hasil setelah menggunakan firewall untuk bertahan dari serangan sistem DDoS dengan MikroTik mencerminkan efektivitas langkah-langkah keamanan yang diterapkan untuk melindungi jaringan. Firewall bertindak sebagai garis pertahanan pertama yang berupaya mendeteksi, mencegah, dan memitigasi serangan DDoS sebelum mencapai targetnya. Hasil penerapan firewall ini merupakan indikator kunci untuk mengevaluasi tingkat perlindungan yang telah berhasil diberikan pada jaringan.



Gambar 4. 4 Hasil CPU Load setelah terdapat Firewall

No.	Pengujian Penyerangan Distributed Denial of Services (DDoS)	Hasil	
		Sebelum ada firewall	Setalah ada firewall
1	Uji coba serangan ke-1	88%	5%
2	Uji coba serangan ke-2	91%	9%
3	Uji coba serangan ke-3	69%	11%
4	Uji coba serangan ke-4	76%	7%
5	Uji coba serangan ke-5	86%	4%
6	Uji coba serangan ke-6	98%	10%
7	Uji coba serangan ke-7	95%	5%
8	Uji coba serangan ke-8	78%	4%
9	Uji coba serangan ke-9	80%	4%
10	Uji coba serangan ke-10	93%	8%

Tabel 4.2.1 Hasil Pengujian Blackbox DDoS

Pengamatan terhadap beban CPU setelah penerapan firewall di jaringan menggunakan MikroTik cukup menggembirakan. Terlihat bahwa setelah penerapan firewall, beban CPU sistem kembali ke tingkat yang sangat rendah. Hal ini menunjukkan bahwa firewall berhasil memenuhi peran defensifnya, mengidentifikasi serangan, dan mengelola beban pemrosesan secara efektif.

Kembalinya beban CPU yang rendah merupakan pertanda positif bahwa sistem keamanan yang diterapkan, termasuk konfigurasi firewall MikroTik, berhasil melindungi jaringan dari serangan DDoS. Ini juga berarti bahwa firewall dapat secara efektif memblokir lalu lintas yang mencurigakan atau berlebihan dari serangan DDoS, sehingga mencegah tekanan berlebihan pada sumber daya sistem. Hasil ini menegaskan bahwa firewall merupakan lapisan pertahanan yang kuat dalam jaringan untuk melindungi terhadap serangan DDoS dan mampu menjaga stabilitas operasional dan

kinerja jaringan. Dengan kembali ke beban CPU yang rendah, jaringan dapat beroperasi secara optimal dan pengguna dapat mengakses layanan tanpa gangguan dari serangan siber. Dengan demikian, hasil tersebut menunjukkan bahwa firewall dengan MikroTik merupakan langkah efektif untuk menjaga keamanan dan stabilitas jaringan terhadap ancaman serangan DDoS.

4.2.2. Penyerangan Brute Force Attack

Serangan Brute Force adalah algoritma yang menyelesaikan masalah dengan cara yang sangat sederhana, mudah dimengerti dan jelas. Mengatasi masalah password cracking menggunakan algoritma brute force yang akan mengatur dan mencari semua kemungkinan password dengan memasukkan karakter dan panjang password tertentu, tentunya banyak kombinasi password yang dapat diatasi melalui. Mungkin inilah sebabnya mengapa keamanan TI atau keamanan informasi diperlukan bagi suatu organisasi. Menurut Charles P. Pfleeger, keamanan komputer adalah mencegah serangan terhadap pengguna komputer atau hacker yang mengakses jaringan. (Syaifuddin, 2018: 348).

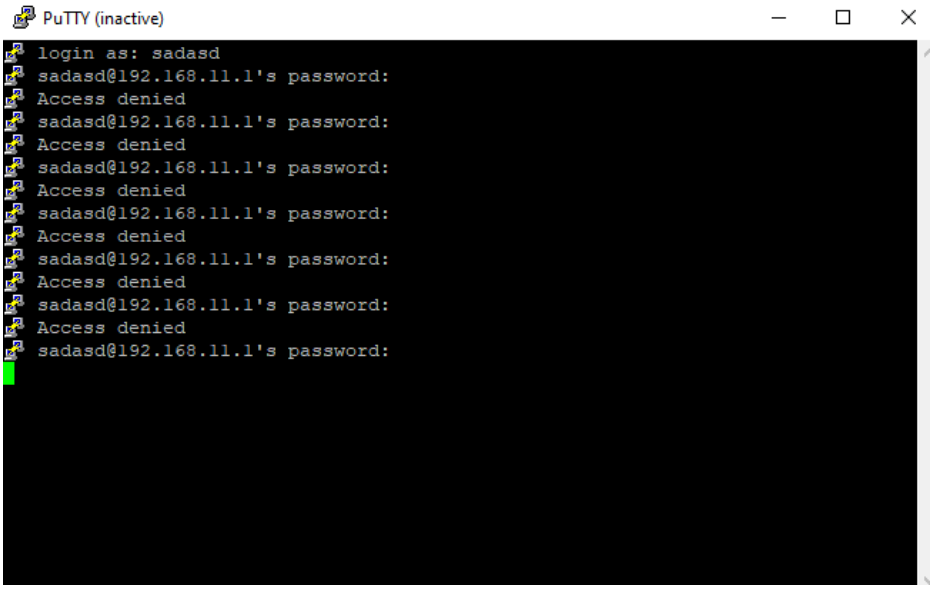
Serangan brute force attack dengan menggunakan MikroTik adalah tindakan siber yang mencoba untuk mencari kata sandi dengan menebak secara berulang-ulang kombinasi kata sandi yang mungkin digunakan untuk masuk ke dalam suatu sistem atau perangkat jaringan. Serangan ini sering kali difokuskan pada protokol seperti SSH (Secure Shell) atau Telnet yang digunakan untuk mengakses perangkat jaringan. Serangan ini dapat dilakukan dengan bantuan perangkat lunak otomatis yang dapat menguji ribuan atau bahkan jutaan kombinasi kata sandi dalam waktu yang sangat singkat.

Serangan brute force merupakan ancaman yang serius karena dapat berhasil jika kata sandi yang digunakan oleh pengguna atau administrator jaringan kurang kuat atau mudah ditebak. Penggunaan kata sandi yang lemah dapat menyebabkan kebocoran data sensitif atau bahkan pengambilalihan akses ke sistem yang sangat penting. Oleh karena itu, proteksi yang efektif terhadap serangan brute force sangat penting.

MikroTik, sebagai solusi jaringan yang populer, memiliki fitur-fitur keamanan yang dapat digunakan untuk melindungi perangkat dari serangan brute force. Ini

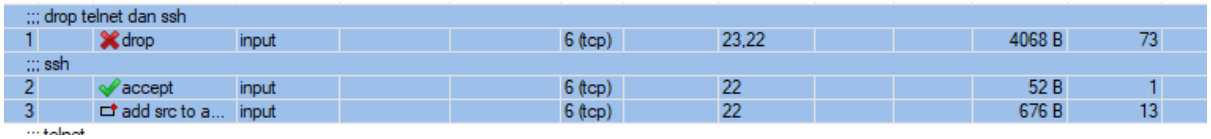
termasuk pembatasan jumlah upaya masuk yang diperbolehkan, pemantauan aktivitas login yang mencurigakan, serta konfigurasi yang kuat terkait dengan pengguna dan kata sandi. Selain itu, penggunaan metode otentikasi yang lebih aman, seperti kunci SSH (SSH keys) alih-alih kata sandi, juga dapat membantu dalam mencegah serangan brute force

Pentingnya melindungi sistem dari serangan brute force attack dengan menggunakan MikroTik adalah untuk menjaga integritas dan keamanan jaringan. Dengan mengambil langkah-langkah yang tepat, organisasi dapat mencegah ancaman ini dan memastikan bahwa kata sandi yang digunakan di jaringan mereka cukup kuat dan tidak dapat dengan mudah ditebak oleh penyerang. Hal ini membantu melindungi data sensitif dan menjaga keandalan operasi jaringan.



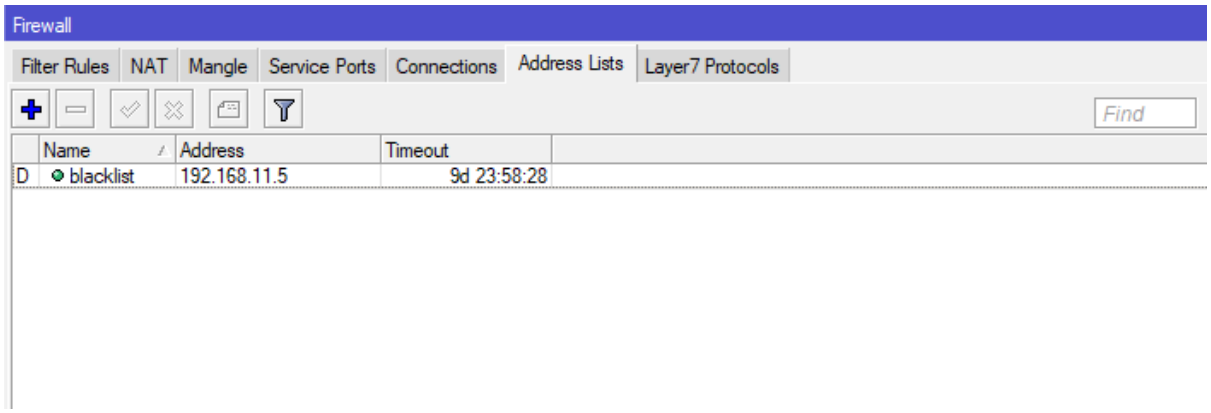
Gambar 4. 5 Percobaan SSH mencoba login berkali-kali

Pada penelitian ini, diawali dengan melakukan percobaan SSH dengan mencoba login berkali-kali Pada dasarnya, serangan ini melibatkan upaya menyambung ke perangkat atau server melalui protokol SSH dengan berulang kali mencoba kombinasi kata sandi yang berbeda. Penyerang berharap dapat menebak kata sandi yang benar dan mendapatkan akses ke sistem yang mereka targetkan.



Gambar 4. 6 Traffic Percobaan Login

Terdapat trafik percobaan login. Lalu lintas upaya login terjadi dalam konteks serangan brute force, situasi yang mencerminkan upaya penyerang untuk menemukan lubang dalam keamanan jaringan dengan berulang kali menebak kata sandi yang benar. Dalam serangan brute force, penyerang secara otomatis akan mencoba berbagai kombinasi kata sandi yang berbeda, berharap berhasil mendapatkan akses ke sistem atau perangkat dengan menebak kata sandi yang valid. Lalu lintas dari upaya koneksi ini sering kali muncul sebagai lonjakan lalu lintas yang tidak biasa di jaringan. Hal ini mungkin menunjukkan bahwa sistem sedang ditargetkan oleh penyerang yang berusaha mendapatkan akses ke akun atau perangkat tertentu. Mendeteksi dan merespons lalu lintas ini dengan cepat sangat penting untuk mencegah akses tidak sah ke sistem dan melindungi data sensitif.



Gambar 4. 7 IP masuk kedalam Blacklist

IP masuk blacklist karena gagal login berkali kali dan di blok 10 hari. Memasukkan alamat IP ke dalam daftar hitam karena beberapa kali gagal login dan diblokir selama 10 hari merupakan langkah keamanan penting untuk melindungi jaringan dari serangan brute force. Dalam serangan ini, ketika alamat IP berulang kali mencoba masuk dengan kata sandi yang salah, sistem secara otomatis mengenali aktivitas ini sebagai potensi serangan. Sebagai tanggapan, alamat IP yang dimaksud dimasukkan ke dalam daftar

hitam, sehingga aksesnya ke sistem atau jaringan diblokir untuk jangka waktu tertentu, dalam hal ini 10 hari.

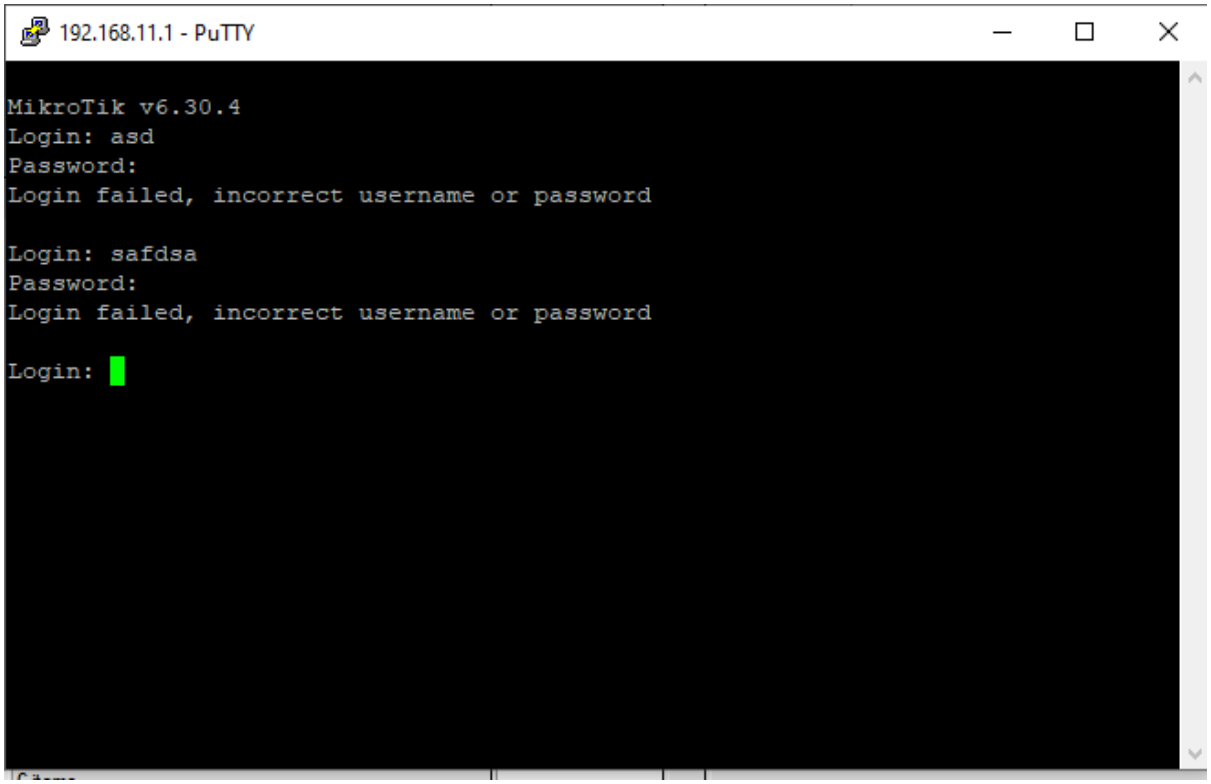
Tindakan ini dimaksudkan untuk mencegah serangan brute force dan menghindari risiko akses tidak sah ke sistem. Alamat IP yang masuk daftar hitam tidak dapat lagi mencoba masuk atau mengakses sistem selama periode pemblokiran. Hal ini memberikan perlindungan tambahan, memungkinkan administrator jaringan mengambil langkah-langkah yang diperlukan untuk mengidentifikasi ancaman dan meningkatkan keamanan.

Langkah-langkah keamanan tersebut merupakan cara yang efektif untuk mengurangi risiko serangan brute force dan memitigasi potensi ancaman terhadap jaringan. Dengan menerapkan kebijakan yang memblokir alamat IP agar tidak masuk berulang kali, organisasi dapat menjaga keamanan data dan sistem mereka serta menghindari kerusakan yang dapat terjadi akibat berbagai serangan jaringan.

Gambar 4. 8 Percobaan Masuk Kembali

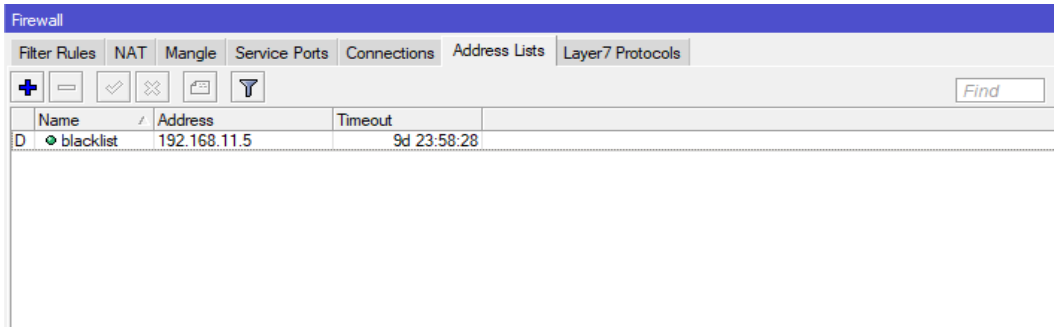
Upaya penyambungan ulang yang gagal karena alamat IP diblokir merupakan konsekuensi dari tindakan keamanan ketat yang dimaksudkan untuk melindungi sistem dari serangan brute force. Dalam konteks serangan ini, ketika sebuah alamat IP

melakukan beberapa kali upaya login yang gagal, sistem akan mengambil tindakan tegas dengan memasukkan alamat IP tersebut ke dalam daftar hitam. Dampaknya, alamat IP yang dimaksud tidak lagi memiliki akses ke sistem atau jaringan dalam jangka waktu yang telah ditentukan.



Gambar 4. 9 Pengujian dengan Telnet login berkali-kali

Pengujian dengan Telnet dalam konteks serangan brute force adalah salah satu tantangan terbesar dalam keamanan siber. Mencegah serangan ini memerlukan perhatian yang cermat terhadap langkah-langkah keamanan yang ketat dan pemantauan aktivitas login yang mencurigakan. Langkah-langkah ini merupakan bagian integral dari perlindungan sistem dan data sensitif dari risiko akse tidak sah. Pengujian Telnet, yang melibatkan beberapa upaya koneksi dalam serangan brute force, adalah contoh spesifik tindakan yang dilakukan penyerang untuk mencoba menemukan kerentanan keamanan dalam jaringan. Serangan brute force pada protokol Telnet biasanya melibatkan penyerang yang mencoba membobol perangkat jaringan dengan menebak kata sandi yang benar dengan mencoba banyak kombinasi kata sandi yang berbeda. Penyerang berharap mendapatkan akses ke sistem dengan menebak kata sandi yang valid, yang dapat memberikan akses penuh ke perangkat atau jaringan yang ditargetkan.



Gambar 4. 10 IP masuk kedalam Blacklist

Dalam konteks serangan brute force yang berfokus pada upaya login melalui Telnet, tindakan keamanan yang ketat seperti memasukkan alamat IP ke daftar hitam setelah sejumlah upaya login yang gagal merupakan salah satu respons yang penting. Alamat IP yang mencoba masuk beberapa kali dengan kata sandi yang salah dapat dianggap sebagai potensi serangan, dan jaringan akan merespons dengan memasukkan alamat IP tersebut ke dalam daftar hitam.

Efek dari tindakan ini adalah untuk jangka waktu tertentu, dalam hal ini 10 hari, alamat IP tidak lagi diperbolehkan untuk mencoba koneksi. Ketika penyerang mencoba menyambung kembali setelah diblokir, upaya tersebut akan gagal karena sistem telah membuat alamat IP tidak aktif. Ini adalah langkah keamanan yang penting untuk mencegah serangan brute force dan menghindari risiko akses sistem yang tidak sah.

Gambar 4. 11 Percobaan Login Kembali

No.	Pengujian Serangan Brute Force Attack	Port	Hasil	
			Sebelum ada firewall	Setelah ada firewall
1	Uji coba serangan ke-1	22	✓	×
		23	✓	×
2	Uji coba serangan ke-2	22	✓	×
		23	✓	×
3	Uji coba serangan ke-3	22	✓	×
		23	✓	×
4	Uji coba serangan ke-4	22	✓	×
		23	✓	×
5	Uji coba serangan ke-5	22	✓	×
		23	✓	×

Tabel 4.2.2 Hasil Pengujian Blackbox Brute Forece Attack

Notes :

× = Tidak dapat login karena port di tutup oleh firewall

✓ = dapat login karena tidak ada keamanan jaringan

Mencoba login setelah alamat IP diblokir dalam upaya Telnet adalah tindakan yang tidak akan efektif karena langkah-langkah keamanan ketat yang telah diterapkan untuk menangani serangan brute force. Dalam situasi ini, ketika alamat IP mencoba masuk beberapa kali dengan kata sandi yang salah, jaringan akan merespons dengan memasukkan alamat IP tersebut ke dalam daftar hitam, sehingga akses diblokir selama jangka waktu yang telah ditentukan.

Ketika seseorang atau entitas yang sah mencoba menyambung kembali setelah diblokir, mereka akan mendapati bahwa upaya mereka telah gagal. Ini adalah konsekuensi yang ditetapkan oleh langkah-langkah keamanan yang dimaksudkan untuk mencegah serangan brute force. Tindakan ini tidak hanya melindungi sistem dari upaya login yang mencurigakan, namun juga memberikan waktu kepada administrator jaringan untuk menilai situasi dan mengambil tindakan respons yang diperlukan. Upaya koneksi

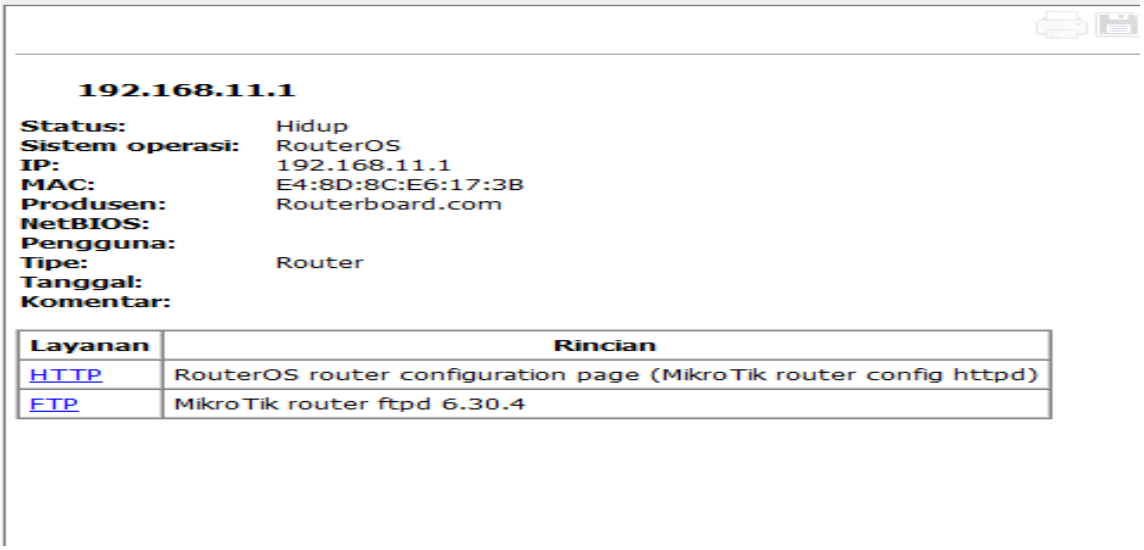
ulang yang gagal setelah pemblokiran IP adalah bukti efektivitas langkah-langkah keamanan untuk melindungi sistem dari serangan brute force. Ini juga mengingatkan penyerang bahwa serangan mereka telah teridentifikasi dan terbatas. Oleh karena itu, konsekuensi ini merupakan langkah penting untuk menjaga keamanan jaringan dan mencegah akses tidak sah ke sistem.

4.2.3. Penyerangan Port Scanning

Keamanan jaringan komputer merupakan suatu hal yang sangat penting, begitu pula pentingnya informasi yang terkandung dalam jaringan tersebut. Pemindaian port adalah langkah pertama dalam serangan pada jaringan komputer. Berkat pemindaian port yang berhasil, penyerang dapat melanjutkan serangannya pada jaringan komputer. (Anif, 2015: 25).

Serangan port scanning adalah teknik yang digunakan oleh penyerang dunia maya untuk memeriksa port yang terbuka pada perangkat atau jaringan. Penyerang mencoba mengidentifikasi port yang dapat digunakan untuk menyusup ke sistem, yang dapat menjadi titik masuk untuk serangan lainnya. Dalam serangan ini, penyerang menemukan port mana yang aktif dan berpotensi rentan terhadap eksploitasi.

Teknik port scanningini dapat menjadi bagian dari persiapan menghadapi serangan yang lebih besar atau langkah awal dalam menemukan kerentanan keamanan. Penyerang berupaya mengumpulkan informasi jaringan penting, seperti layanan yang berjalan, versi perangkat lunak yang digunakan, dan konfigurasi sistem. Informasi ini kemudian dapat digunakan untuk merancang serangan yang lebih spesifik.

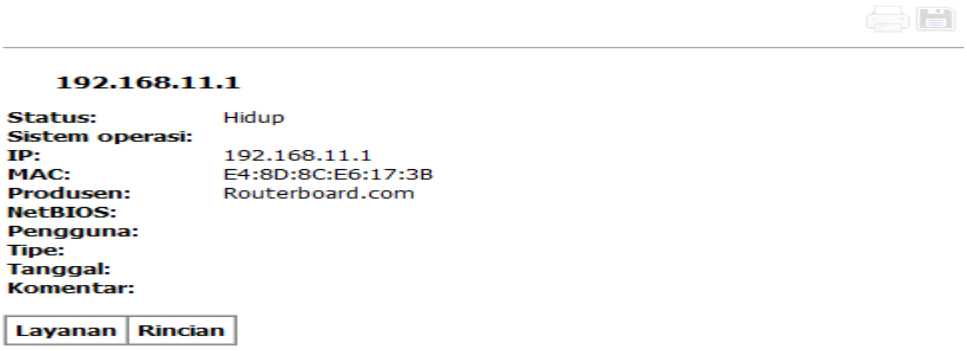


Gambar 4. 12 Celah pada Port

Sebelum ada firewall, ketika port HTTP dan FTP dibuka, sistem atau jaringan menjadi lebih rentan terhadap serangan dan ancaman dunia maya. Por terbuka berarti layanan HTTP (digunakan untuk website) dan FTP (File Transfer Protocol) dapat diakses tanpa hambatan dari luar jaringan. Ini bisa menjadi masalah serius karena penyerang dapat mengeksploitasi port tersebut untuk mencoba membobol sistem atau jaringan.

Menyebarkan firewall adalah salah satu cara untuk mengatasi masalah ini. Firewall memungkinkan Anda menentukan aturan dan kebijakan keamanan yang dapat memblokir akses yang tidak diinginkan ke port tertentu. Dalam kasus port HTTP dan FTP, firewall dapat digunakan untuk membatasi akses hanya kepada pengguna yang berwenang atau memantau lalu lintas yang mencurigakan.

Dengan firewall, Perusahaan dapat mengontrol akses ke port yang rentan, mengurangi potensi risiko, dan meningkatkan keamanan jaringan. Dengan kata lain, firewall adalah lapisan pertahanan penting untuk melindungi sistem dan data dari serangan serta memitigasi potensi pelanggaran keamanan. Sehingga tahap selanjutnya adalah memakai firewall.



Gambar 4. 13 Setelah Pemasangan Firewall

No.	Pengujian Port Scanning	Hasil sebelum ada firewall				Hasil setelah ada firewall			
		Port 20	Port 21	Port 80	Port 443	Port 20	Port 21	Port 80	Port 443
1	Uji coba serangan ke-1	✓	✓	✓	✓	×	×	×	×
2	Uji coba serangan ke-2	✓	✓	✓	✓	×	×	×	×
3	Uji coba serangan ke-3	✓	✓	✓	✓	×	×	×	×
4	Uji coba serangan ke-4	✓	✓	✓	✓	×	×	×	×
5	Uji coba serangan ke-5	✓	✓	✓	✓	×	×	×	×
6	Uji coba serangan ke-6	✓	✓	✓	✓	×	×	×	×
7	Uji coba serangan ke-7	✓	✓	✓	✓	×	×	×	×
8	Uji coba serangan ke-8	✓	✓	✓	✓	×	×	×	×

Tabel 4.2.3 Hasil Pengujian Blackbox Port Scanning

Notes :

× = Port tertutup

✓ = Port terbuka

Setelah menerapkan firewall, jaringan atau sistem perusahaan akan menjadi lebih aman dan tidak akan ada port terbuka yang dapat dieksploitasi oleh penyerang. Firewall bertindak sebagai lapisan pertahanan pertama, yang mampu mengatur lalu lintas masuk dan keluar jaringan. Hal ini memungkinkan Anda mengontrol dengan cermat port mana yang boleh diakses dari luar, serta menutup port yang tidak digunakan atau tidak boleh dibuka.

Dengan firewall yang efektif, dapat memblokir akses tidak sah ke port penting, sekaligus membiarkan lalu lintas yang sah mengalir dengan lancar. Hal ini membuat jaringan perusahaan lebih tahan terhadap berbagai jenis serangan, termasuk serangan pemindaian port yang mencoba menemukan port terbuka. Tanpa port terbuka, Perusahaan mengurangi risiko akses tidak sah dan menjaga keamanan sistem dan data. Menerapkan firewall yang baik merupakan langkah penting dalam meminimalkan ancaman dunia maya dan menjaga integritas jaringan. Hal ini memberikan perlindungan tambahan dan memastikan bahwa hanya lalu lintas resmi yang diizinkan untuk berkomunikasi melalui port yang ditentukan, menjadikan jaringan lebih aman dan andal.

BAB V
PENUTUP

5.1. Kesimpulan

Pada Penelitian “Manajemen Ancaman dan Keamanan Jaringan Melalui Penggunaan Firewall dengan Mikrotik Pada PT. Dinamika Mediakom” beserta hasil yang telah dilakukan dapat ditarik kesimpulan bahwa :

1. Firewall berjalan dengan fungsinya terhadap serangan DDoS, Brute Force Attack, dan Port Scanning.
2. Firewall dapat membantu dalam mengamankan jaringan dari berbagai ancaman siber.

5.2. Saran

Berdasarkan penelitian, direkomendasikan agar perusahaan mengadopsi pendekatan komprehensif terhadap manajemen keamanan jaringan, termasuk penerapan kebijakan keamanan yang tepat, penggunaan teknologi keamanan seperti firewall dan sistem deteksi intrusi, dan pelatihan keamanan siber secara berkala untuk semua pengguna jaringan. Penelitian ini juga menunjukkan bahwa penerapan dan pengujian firewall secara hati-hati sangat penting untuk memastikan efektivitasnya dalam melindungi jaringan dari berbagai ancaman dunia maya. Perusahaan harus memperbarui kebijakan dan teknologi keamanan mereka secara rutin untuk mengimbangi ancaman dunia maya yang terus berkembang. Dengan menerapkan rekomendasi ini, perusahaan dapat meningkatkan keamanan jaringan mereka dan melindungi aset digital mereka dari berbagai ancaman siber.

DAFTAR PUSTAKA

Achmad, R., Manullang, E. V., & Sanmas, E. R. (2020). Rancang Bangun Aplikasi Deteksi Dan Penanganan Serangan DDOS Dan Port Scanning Memanfaatkan Snort Pada Jaringan Komputer. *Jurnal Teknologi Informasi*, *8*(1), 44-53.

Afikah, N., & Mukmin, C. (2022, October). Analisa Perbandingan Kinerja Router Terhadap Variasi Serangan Ddos. In *Bina Darma Conference on Computer Science (BDCCS)* (Vol. 4, No. 2, pp. 282-290).

Anif, Muhammad, Sindung HW Sasono, and Mokhamad Daman Huri. "Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang." *TELE* 13.1 (2015).

ASTARI, A. A. (2018). ImplemenTasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik. Simki-Techsain Vol. 02 No. 01 Tahun 2018 ISSN 2599, 3011.

Alfred, A., & Chandra, J. C. (2018). Pemanfaatan Firewall pada jaringan komputer SMK Fadilah. IDEALIS: InDonEsiA journaL Information System, 1(5), 422-428.

Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. Jurnal Teknoinfo, 12(2), 72-75.

Fachri, F. (2023). Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *10*(1), 51-58.

Gutama, D. H., Setiawan, R. A., & Estetikha, A. K. A. (2022). Penanganan Serangan Brute Force dan Port Scanning Pada Router Mikrotik. *Jurnal Sistem Informasi dan Teknologi Informasi*, *1*(2), 1-13.

Kohar, A., & Putro, H. P. (2014). Ancaman Keamanan pada Sistem Informasi Manajemen Rumah Sakit. In Seminar Nasional Informatika Medis (SNIMed).

Hassan Rizky Putra Sailellah. (2023). Pengertian Firewall dalam Jaringan Komputer dan Jenis-Jenisnya.https://it.telkomuniversity.ac.id/pengertian-firewall-dalam-jaringan-komputer-dan-jenis-jenisnya/

Hendarsyah, D. (2012). Keamanan Layanan Internet Banking Dalam Transaksi Perbankan. IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita, 1(1), 12-33.

Hermawan, R. (2015). Analisis konsep dan cara kerja serangan komputer Distributed Denial Of Service (Ddos). *Faktor Exacta*, *5*(1), 1-14.

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim Informasi dan Teknologi*, 115-123.

Langobelen, E. S. R. O. B., Rachmawayi, R. Y., & Iswayudi, C. (2019). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta. Jurnal Jarkom, 7(2), 95-102.

Mancill, T. (2002), Linux Routers : A Primer for Network Administrator, 2nd ed., Prentice Hall.

Mancill, T. (2002). Linux routers. Prentice Hall Professional Technical Reference.

Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa, 2(01), 14-20.

Okpatrioka, O. (2023). Research And Development (R&D) Penelitian Yang Inovatif Dalam Pendidikan. Dharma Acariya Nusantara: Jurnal Pendidikan, Bahasa dan Budaya, 1(1), 86-100.

Purbo, O. W. (2000), Linux Untuk Warung Internet, Jakarta: Elex Media Komputindo.

Risqiwati, D., & Irawan, E. A. (2018). Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server. *Techno. Com*, *17*(4), 347-354

. Rusydianto, M. R., Budiman, E., & Setyadi, H. J. (2017, September). Implementasi Teknik Hacking Web Server Dengan Port Scanning Dalam Sistem Operasi Kali Linux. In *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi E-ISSN* (Vol. 2, No. 2).

Suharmanto, A. Y., Lumenta, A. S., & Najoan, X. B. (2018). Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi. Jurnal Teknik Informatika, 13(3).

Sofana, I. (2013). MEMBANGUN JARINGAN KOMPUTER (Mudah membuat Jaringan Komputer wire&wireles untuk Pengguna Windows dan Linux). Bandung: Informatika.

Syafrizal, M. (2007, November). ISO 17799: Standar Sistem Manajemen Keamanan Informasi. Seminar Nasional Teknologi (Vol. 2007, pp. 1-10).

Tanutama, L. (1996), Jaringan Komputer, Jakarta: Elex Media Komputindo.