BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, harddisk, dan sebagainya. Suatu jaringan komputer terdiri dari komputer, *software,* dan perangkat jaringan yang bekerja bersama dalam satu ruang lingkup yang disebut jaringan (Saputro et al., 2020). Keamanan jaringan penting dan harus selalu menjadi perhatian, baik *Local Area Network* (LAN) maupun jaringan Nirkabel atau *wireless* yang terhubung ke internet pada dasarnya tidak aman dan selalu rentan terhadap peretasan. Karena data harus melewati beberapa terminal untuk mencapai tujuannya, hal ini menciptakan kemungkinan bagi pengguna lain yang tidak bertanggung jawab untuk mengubah, mengganti, merusak, atau bahkan mencuri data. Namun, masalah keamanan jaringan sering kali kurang diperhatikan. Untuk meningkatkan keamanan jaringan, administrator hanya berusaha menggunakan pertahanan terbaik sejauh ini, seperti *firewall* dan sistem deteksi intrusi (IDS). Mayoritas *hacker* menggunakan port terbuka sistem untuk menyerang sistem jaringan. Serangan Dos atau ddos, yang tertuju pada *host* atau komputer target dengan sejumlah besar paket yang datang dari berbagai *host*, adalah ilustrasi dari jenis serangan ini.

Keamanan jaringan adalah sebuah sistem yang dibangun agar jaringan komputer dapat berjalan dengan baik dan terhindar dari ancaman baik dari luar maupun dari dalam yang dapat merusak sistem jaringan dan menyebabkan jaringan tidak dapat berkerja sehingga dapat mengganggu operasional sebuah organisasi yang sangat tergantung dengan jaringan komputer. Keamanan jaringan dapat dilakukan dengan cara memberikan proteksi atau perlindungan pada router sebagai pengatur lalu lintas data di jaringan. Proteksi dan keamanan pada router sangatlah penting untuk menjaga kelangsungan jaringan komputer sebuah organisasi. Terutama untuk menjaga router Mikrotik dari segala macam akses ilegal yang mencoba untuk masuk ke sistem jaringan komputer dan mengelola jaringan pada router milik sebuah organisasi (Novianto et al. 2023).

Penelitian mengenai keamanan jaringan pernah dilakukan oleh Randi, Ruuhwan, Kelvin Ajie Nugraha, pada tahun 2020 mengenai "Implementasi Keamanan Jaringan Menggunakan Metode *Port Blocking* dan *Port Knocking* Pada Mikrotik RB-941". Penelitian ini berisi tentang menerapkan keamanan jaringan melalui pemblokiran *port* dan metode *port knocking* serta mencegah penyerang mengakses *router* Mikrotik, kekurangan dari penelitian ini yaitu kecepatan yang kurang memadai untuk objek penelitiannya karena kecepatan sinyalnya masih 50Mbps dan itu di bagi-bagi ke berbagai gedung yang ada di objek penelitian ini. Selanjutnya penelitian keamanan jaringan juga pernah dilakukan oleh Januar Al Amin tahun 2020 mengenai "Implementasi Keamanan Jaringan Dengan *IP Table* Sebagai *Firewall* Menggunakan Metode *Port Knocking*". Penelitian ini berisi tentang metode *Port Knocking* yang bisa menutup semua informasi *port* dengan menggunakan Aplikasi *Iptables* dan memberikan hak akses berupa kombinasi

ketukan yang sudah di tentukan. Server akan meng-*overwrite* aturan *firewall* dengan aturan baru yang dibuat berdasarkan konfigurasi *IPtables,* dan langsung membuka *port* tujuan, dan *client* dapat mengakses *port* tujuan. kekurangan dari penelitian ini yaitu untuk melindungi informasi *port* harus ditutup pada server, dan *client* tertentu harus diberi akses untuk membuka *port* dan layanan melalui proses otentifikasi. Orang yang tidak diberi kewenangan tidak dapat mengakses informasi *port* itu sendiri.

Port knocking adalah metode sederhana yang memberi akses *remote* tanpa meninggalkan *port* 22 dalam keadaan terbuka, dengan begitu memberikan perlindungan kepada server dari serangan *port scanning*, DDOS *attack* dan *brute force* (Ernawati et al., 2022.) Cara kerja *port knocking* yaitu menutup *port* dan hanya *user* tertentu saja yang dapat mengakses dengan cara melakukan *knock* terlebih dahulu pada *port* yang dituju. Sedangkan *port blocking* adalah tindakan menutup *port* yang mencegah *host* mengakses *port* tersebut, menyembunyikan layanan jarak jauh di belakang *firewall,* dan hanya *client* tertentu yang diizinkan mengakses port tertentu setelah *client* berhasil mengautentikasi terhadap *firewall*. Konsepnya adalah mengizinkan akses ke *port* tersebut untuk menemukan layanan, dan penutup *port* menggunakan *firewall* untuk menjalankan aksinya. *Firewall* merupakan sebuah sistem atau sebuah perangkat yang memberi akses pada lalu lintas di jaringan komputer yang dianggap aman untuk dilewati dan melakukan pencegahan terhadap lalu lintas di jaringan yang dianggapnya tidak aman (Novianto et al., 2023).

Kantor Dinas Kesehatan Kabupaten Tanah Datar adalah Lembaga Kesehatan yang memiliki berbagai program khusus untuk mengurangi penyakit

yang ada dalam Masyarakat. Dalam hal itu kantor ini juga memerlukan koneksi jaringan internet dalam Upaya memberi informasi kepada Masyarakat khusunya di wilayah Tanah Datar mengenai program-program baru tentang Kesehatan. Hal ini membuat perangkat keras dan perangkat lunak komputer termasuk juga jaringan tergolong tinggi digunakan oleh Kantor Dinas Kesehatan Kabupaten Tanah Datar, ini karena, saat ini ada suatu masalah bagi banyak penguna untuk dipelajari dan diakses. Kurangnya keamanan jaringan pada router Mikrotik, pengaturan *proxy* sistim Mikrotik akan menimbulkan masalah jika ada orang yang mengubah pengaturan pada router. Hal ini mengganggu kecepatan sinyal internet pengguna lain, dan membutuhkan keamanan jaringan, yaitu *port knocking* dan *port blocking*.

Solusi untuk mengatasi agar *user* tidak bisa masuk ke gedung untuk merubah settingan router mikrotik yaitu caranya mengimplementasikan metode keamanan jaringan yang menggunakan metode *port blocking* dan *port knocking*.

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu **"IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN METODE PORT KNOCKING DAN PORT BLOCKING PADA ROUTER MIKROTIK DI KANTOR DINAS KESEHATAN KABUPATEN TANAH DATAR"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas dapat disimpulakan permasalahan yang akan dibahas pada laporan ini sebagai berikut :

1. Bagaimana *Port Knocking* dan *Port Blocking* bisa mengamankan akses ke router Mikrotik di Kantor Dinas Kesehatan Kabupaten Tanah Datar?

2. Bagaimana Mengimplementasikan *Port Knocking* dan *Port Blocking* pada Keamanan router Mikrotik di Kantor Dinas Kesehatan Kabupaten Tanah Datar?

1.3 Hipotesa

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan perumusan masalah yang ada dapat dikemukakan beberapa hipotesa sebagai berikut :

1. Diharapkan metode *Port Knocking* dapat membantu pengendalian orang-orang yang terhubung ke jaringan Kantor Dinas Kesehatan Kabupaten Tanah Datar dan tindakan pengendalian yang dilakukan akan memungkinkan deteksi serta pemantauan orang-orang yang terhubung ke jaringan.
2. Diharapkan dengan mengunakan metode *Port Blocking* dapat mencegah serangan dari luar dan menjaga integritas serta kerahasiaan data kesehatan yang sensitif.

1.4 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka peneliti memberikan batasan masalah yaitu :

1. Hanya mengimplementasikan *Port Knocking* dan *Port Blocking* pada Mikrotik.
2. Hanya melakukan penelitian pada objek penelitian di Kantor Dinas Kesehatan Kabupaten Tanah Datar.
3. Analisis keamanan dilakukan pada fitur keamanan dari *port knocking* dan *port blocking.*

1.5 Tujuan Penelitian

Dalam melaksanakan penelitian ini tujuan yang ingin dicapai diantaranya adalah :

1. Memahami tentang metode *Port Knocking* dan *Port Blocking* pada keamanan jaringan.
2. Menganalisa dampak implementasi *Port Knocking* dan *Port Blocking* terhadap keamanan jaringan yang di terapkan pada Kantor Dinas Kesehatan Kabupaten Tanah Datar.
3. Merancang mekanisme *Port Knocking* dan *Port Blocking* pada *router* MikroTik guna memberikan perlindungan terhadap serangan dan upaya akses yang tidak sah.
4. Membangun keamanan jaringan menggunakan metode *Port Knocking* dan *Port Blocking* pada router mikrotik di Kantor Dinas Kesehatan Kabupaten Tanah Datar.
5. Menguji metode *Port Knocking* dan *Port Blocking* supaya dapat mencegah akses illegal terhadap router mikrotik di Kantor Dinas Kesehatan Kabupaten Tanah Datar.

1.6 Manfaat Penelitian

Manfaat penelitian yang dilakukan oleh peneliti diharapkan dapat memberikan dampak yang lebih baik setelah melakukan penelitian ini. Adapun manfaat dari penelitian ini adalah yaitu :

1. Dapat mengoptimalkan keamanan jaringan komputer yang ada di Kantor Dinas Kesehatan Kabupaten Tanah Datar.
2. Sebagai solusi untuk mengamankan router mikrotik dari hak akses yang illegal.

1.7 Gambaran Umum Objek Penelitian

Gambaran objek penelitian secara umum merinci kerangka konseptual suatu penelitian, membahas karakteristik, sifat, dan relasi antar variabel yang relevan untuk memahami fenomena tersebut. Teori ini memberikan landasan bagi peneliti untuk merumuskan pertanyaan penelitian, mengidentifikasi variabel penting, dan merancang metode yang sesuai untuk menggali lebih dalam dalam pemahaman terhadap objek penelitian.

1.7.1 Sekilas Tentang Kantor Dinas Kesehatan Kabupaten Tanah Datar

Dinas Kesehatan Kabupaten Tanah Datar merupakan Organisasi Perangkat Daerah (OPD) Pemerintah Kabupaten Tanah Datar yang dibentuk berdasarkan Peraturan Daerah No. 45 Tahun 2016 tanggal 28 Desember tentang Kedudukan, Susunan organisasi, Tugas dan Fungsi Tata Kerja Dinas Daerah dan merupakan unsur pelaksana urusan daerah dibidang Kesehatan berdasarkan kewenangan yang dimiliki pemerintah daerah sesuai dengan ketentuan peraturan perundang-undangan yang berlaku yang berada dibawah dan bertangung jawab kepada bupati melalui Sekretaris Daerah Dinas Kesehatan. Kantor ini terletak di jalan Sultan Alam Bagarsyah, Pagaruyung, Pagar Alam, Kabupaten Tanah Datar, Sumatera Barat. Kantor ini dikelola oleh personel yang terdiri dari Kepala Kantor, Sekretaris, staff administrasi, petugas Kesehatan, manajer program Kesehatan dan juga ahli Kesehatan.

Gambar 1. 1 Dinas Kesehatan Kabupaten Tanah Datar

Pada Kantor Dinas Kesehatan Kabupaten Tanah Datar terdiri dari bangunan kantor utama, ruang rapat, area administratif, ruang kerja untuk staff. Kantor ini memiliki berbagai fasilitas termsuk kantor pusat, laboratorium Kesehatan, pusat Kesehatan Masyarakat, fasilitas ini digunakan untuk layanan Kesehatan, pengujian penyakit, serta pemantauan dan pelaporan data Kesehatan. Salah satu fokus kegiatan kantor ini yaitu pencegahan penyakit, ini mencakup kampanye vaksinasi, penyuluhan Kesehatan kepada Masyarakat, dan langkah-langkah lain untuk mengurangi penyebaran penyakit menular.

1.7.2 Visi dan Misi Kantor Dinas Kesehatan Kabupaten Tanah Datar

1. Visi

   Visi Pembangunan Kesehatan di Kabupaten Tanah Datar adalah

”Terwujudnya Masyarakat Tanah Datar yang Sehat, Mandiri, dan Berkeadilan”

2. Misi

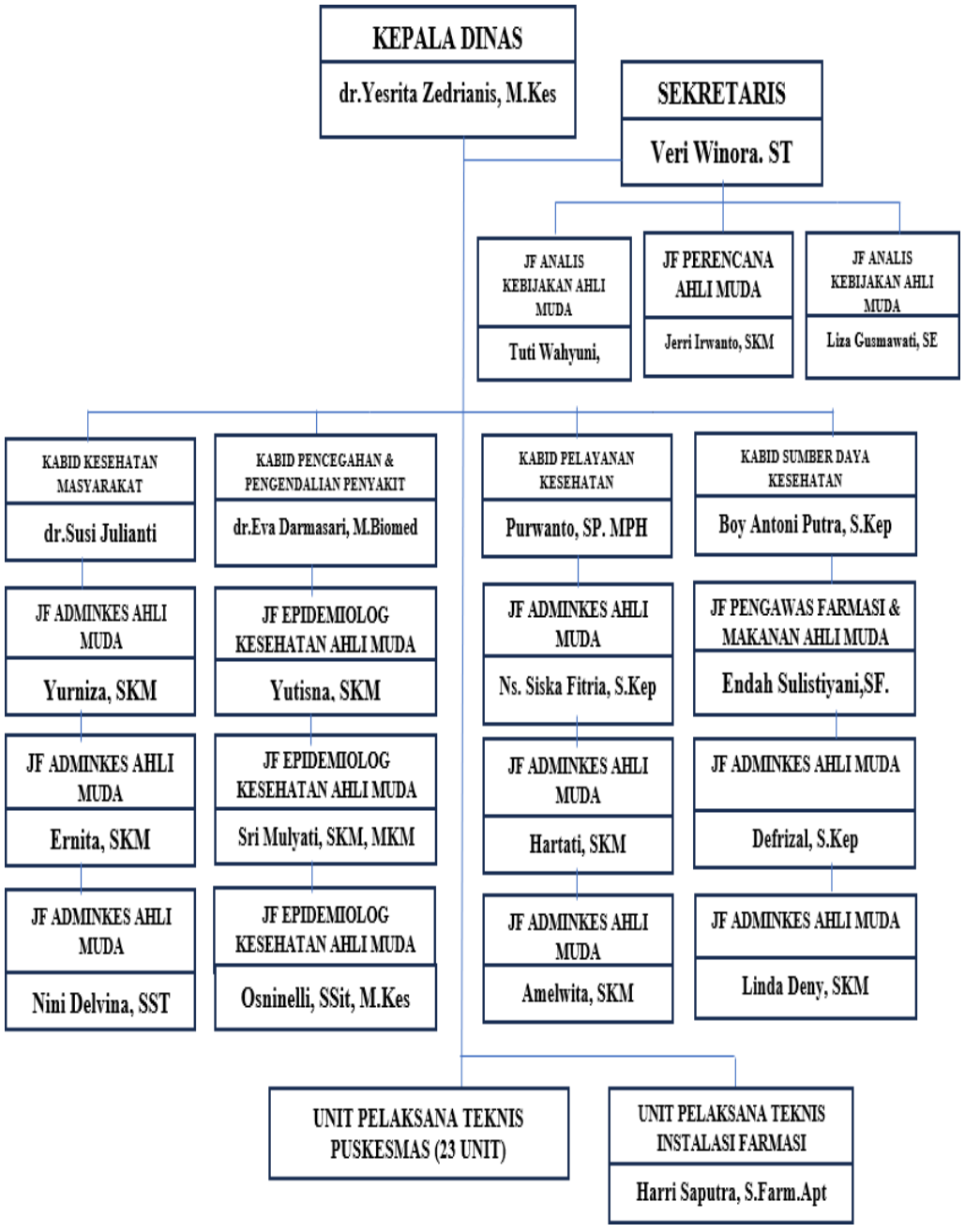
Misi Pembangunan Kesehatan di Kabupaten Tanah Datar adalah sebagai berikut :

a. Meningkatkan derajat Kesehatan Masyarakat melalui pemberdayaan masyarakat, termasuk swasta dan masyarakat mandiri
b. Melindungi kesehatan masyarakat dengan menjamin tersedianya upaya kesehatan yang paripurna, merata, dan masyarakat mandiri.
c. Menjamin ketersediaan dan pemerataan sumber daya kesehatan.
d. Menciptakan tata kelola kepemerintahan yang baik.
e. Meningkatkan kerjasama lintas sektor dalam penyelenggaraan pembangunan kesehatan, dan penjabaran tersebut telah diselaraskan dengan tujuan Pembangunan bidang kesehatan secara nasional.

1.7.3 Struktur Organisasi Kantor Dinas Kesehatan Kabupaten Tanah Datar

Struktur organisasi adalah kerangka yang menentukan bagaimana aktivitas dalam suatu perusahaan atau organisasi dikelola, dikoordinasikan, dan diarahkan untuk mencapai tujuan yang telah ditetapkan. Struktur ini mencerminkan hubungan hierarkis, aliran komunikasi, dan distribusi tanggung jawab di antara berbagai posisi dan departemen. Dengan adanya struktur organisasi yang jelas, sebuah organisasi dapat berfungsi lebih efektif dan efisien, memastikan setiap anggota memahami peran dan tanggung jawab mereka, serta mendukung pengambilan keputusan yang lebih cepat dan tepat.

Struktur organisasi diharapkan dapat memberikan pemahaman yang jelas mengenai tugas, wewenang dan tanggung jawab Dinas Kesehatan Kabupaten Tanah datar. Adapun struktur organisasi Kantor Dinas Kesehatan Kabupaten Tanah Datar dapat dilihat pada gambar 1.2 sebagai berikut :



Sumber : Kantor Dinas Kesehatan Kabupaten Tanah Datar

Gambar 1. 2 Struktur Organisasi DINKES Tanah Datar

BAB II

LANDASAN TEORI

2.1 Keamanan Jaringan

Keamanan jaringan adalah istilah yang luas dan banyak mencakup teknologi, perangkat maupun proses. Dalam istilah sederhana, sistem keamanan jaringan adalah proses untuk mengenali dan mencegah seseorang yang tidak mempunyai izin untuk mengakses ke sebuah jaringan. Tujuan dari keamanan jaringan tersebut agar mengantisipasi adanya resiko ancaman pencurian data maupun pengrusakan fisik pada komputer (Tito Brades dan Irwansyah, 2021). Jenis-jenis layanan yang terdapat pada mikrotik diantaranya API (*Application Programmable Interface*), API-SSL, FTP (*File Transfer Protocol*), SSH (*Secure Shell*), Telnet, Winbox, WWW (*Word Wide Web*), dan WWW-SSL.

Keamanan jaringan merupakan salah satu kajian keamanan komputer yang berfokus pada Infrastruktur jaringan. Sehingga dapat dikatakan keamanan jaringan merupakan bagian dari keamanan komputer dan juga dapat dipandang sebagai bagian dari *cybersecurity*. Keamanan jaringan pada intinya adalah mengendalikan akses terhadap sumberdaya jaringan. Akses jaringan dikontrol agar bisa diakses oleh siapa saja yang berhak dan menghalangi orang atau subjek yang tidak terdaftar untuk mengaksesnya. Prinsip keamanan jaringan di klasifikasikan menjadi 3 bagian:

1. Kerahasiaan (*Confidentiality*), mengacu pada kerahasiaan suatu objek, dimana objek tersebut dilindungi dari akses pihak luar. Istilah ini juga mengacu pada informasi pribadi yang diberikan kepada pihak untuk tujuan tertentu lainnya dan

hanya digunakan untuk keperluan tersebut. Informasi pribadi misalnya nama, nomor, kata sandi komputer, agama, dan lain-lain.

2. Integritas (*Integrity*), mengacu pada objek yang tetap asli, artinya objek tidak berubah sepanjang jalan hingga mencapai tujuan objek. Misalnya, pesan email yang dikirim oleh seseorang bisa jadi dicegat di tengah jalan, isinya berubah dan kemudian mengirimkan yang baru kepenerima yang sebenarnya sehingga informasi yang diterima oleh penerima berubah dari yang dimaksudkan oleh pengirim. Bentuk serangan pada aspek ini termasuk virus, *trojan*, atau pengguna lain selama komunikasi.
3. Ketersediaan (*Availability*), berarti ketersediaan sumber daya atau sumber daya yang benar sehingga pengguna memiliki hak akses pada waktu yang tepat dan tidak ada masalah.

2.2 Konsep Dasar Jaringan

Konsep dasar jaringan komputer melibatkan penghubungan dan komunikasi antara beberapa perangkat komputer untuk berbagi sumber daya, seperti data, informasi, perangkat keras, dan perangkat lunak. Berikut adalah beberapa konsep dasar yang perlu dipahami dalam jaringan komputer :

1. Media Transmisi

   Merupakan medium fisik nirkabel yang digunakan untuk mengirimkan data antara simpul-simpul dalam jaringan. Contoh media transmisi adalah kabel tembaga, serat optik, dan gelombang radio.

2. Protokol

   Merupakan aturan dan prosedur yang mengatur komunikasi antara simpul-simpul dalam jaringan. Protokol ini memastikan bahwa data dikirimkan dengan

benar dan jaringan. Protokol ini memastikan bahwa data dikirimkan dengan benar dan diinterpretasikan dengan benar oleh penerima. Contoh protokol jaringan termasuk TCP/IP, HTTP, dan FTP.

3. Simpul (*Node*)

   Simpul (*Node*) merupakan perangkat dalam jaringan, seperti komputer, printer, server, atau router, yang dapat mengirim atau menerima data.

4. Topologi Jaringan

   Secara umum, topologi jaringan mengacu pada susunan fisik atau logis dari simpul-simpul atau perangkat dalam jaringan komputer, serta cara mereka terhubung satu sama lain. Topologi jaringan menentukan pola komunikasi antara perangkat-perangkat tersebut.

5. *IP Address*

   Merupakan alamat unik yang diberikan kepada setiap perangkat dalam jaringan untuk dapat diidentifikasi dan berkomunikasi satu sama lain menggunakan protokol TCP/IP. Alamat IP terdiri dari sejumlah angka yang membedakan perangkat dalam jaringan.

6. *Subnetting*

   Merupakan proses membagi sebuah jaringan IP besar menjadi beberapa *subnet* yang lebih kecil. Dalam jaringan komputer, setiap perangkat yang terhubung ke jaringan menggunakan alamat IP unik. *Subnetting* memungkinkan administrator jaringan untuk membagi alamat IP yang besar menjadi bagian-bagian yang lebih kecil, yang dikenal sebagai *subnet*, untuk mengoptimalkan penggunaan alamat IP. Dalam *subnetting*, blok alamat IP yang besar dibagi menjadi beberapa subnet dengan menggunakan *subnet mask.*

7. *Routing*

   Routing merupakan proses pengiriman paket data melalui jaringan dengan menggunakan perangkat jaringan yang disebut router. Router bertanggung jawab untuk menentukan rute terbaik yang harus diambil oleh paket data untuk mencapai tujuan yang dituju.

8. *Firewall*

   Merupakan sistem keamanan yang digunakan untuk melindungi jaringan dari ancaman eksternal dan mengontrol akses ke jaringan. *Firewall* dapat membatasi lalu lintas jaringan berdasarkan aturan yang ditentukan, memantau aktivitas jaringan, dan mencegah akses yang tidak sah atau berbahaya.

9. Protokol *Wireless*

   Protokol *Wireless* mengacu pada seperangkat aturan dan standar yang mengatur komunikasi nirkabel antar perangkat di jaringan. Protokol ini memastikan bahwa perangkat nirkabel dapat berkomunikasi secara efektif dan memahami satu sama lain dalam lingkungan jaringan nirkabel.

10. VLAN (*Virtual Local Area Network*)

    VLAN adalah Sebuah teknologi yang memungkinkan perangkat di jaringan dikelompokkan ke dalam beberapa jaringan virtual yang terpisah secara logis, meskipun mereka mungkin berada di jaringan fisik yang sama. VLAN membantu mengelola dan meningkatkan keamanan jaringan.

2.3 Sifat – Sifat Jaringan Komputer

Sifat-sifat jaringan komputer menyatakan bahwa keberhasilan dan efisiensi sebuah jaringan komputer bergantung pada beberapa karakteristik utama, di antaranya adalah *Scalability, Resource Sharing, Connectivity, dan Reliability.*

1. *Scalability* adalah jaringan komputer yang dapat di skalakan atau diukur sesuai dengan kebutuhan pengguna jaringan komputer.
2. *Resource Sharing* digunakan untuk saling berbagi satu dengan yang lain, dan memakainya secara bersamaan dengan segala sumber daya yang tersedia.
3. *Connectivity* adalah jaringan komputer yang memiliki sifat mudah dihubungkan ke semua pengguna komputer serta pengguna komputer itu sendiri juga dapat terhubung ke dalam jaringan komputer yang telah tersedia.
4. *Reliability* berfungsi mengirimkan paket data yang dikirim oleh pengirim yang akan sampai kepada penerima dengan baik.

2.4 Jenis-jenis Jaringan Komputer

Jaringan komputer adalah struktur yang memungkinkan perangkat komputer saling terhubung untuk berbagi informasi dan sumber daya. Terdapat beberapa jenis-jenis jaringan komputer yang umum digunakan, antara lain :

1. *Local Area Network* (LAN).

   Local Area Network (LAN) adalah jaringan komputer yang terdiri dari beberapa perangkat komputer yang terhubung melalui media kabel atau nirkabel dalam suatu area terbatas seperti di dalam gedung, kampus, atau area lainnya dengan jarak terbatas (Nathan Nurdadyansyah, dkk. 2021). Jaringan ini digunakan untuk berbagi sumber daya seperti *printer, file*, dan koneksi internet antara pengguna dalam jaringan yang sama, dan kecepatan transmisi jaringan ini dapat mencapai 1 sampai 100 megabit perdetik.

2. *Metropolitan Area Network* (MAN).

   Metropolitan Area Network (MAN) adalah jaringan komputer yang mencakup area geografis yang lebih besar dari *Local Area Network* (LAN), tetapi lebih

kecil dari *Wide Area Network* (WAN). Jaringan ini biasanya mencakup area seperti kota atau wilayah perkotaan yang luas, dan terdiri dari beberapa gedung atau lokasi yang terhubung secara bersama-sama untuk memungkinkan komunikasi dan berbagi sumber daya antar penguna.

3. *Wide Area Network* (WAN).

   Wide Area Network (WAN) adalah jaringan komputer yang mencakup area geografis yang luas, yang terhubung melalui teknologi jaringan seperti satelit, *leased line*, atau teknologi nirkabel. Jaringan ini mempunyai karakteristik seperti jarak yang jauh, koneksi yang lambat, dan biaya koneksi yang relative tinggi.

4. *Personal Area Network* (PAN)

   Personal Area Network (PAN) biasanya digunakan untuk menghubungkan perangkat pribadi dengan perangkat lainnya karena memiliki area kecil, biasanya di sekitar smartphone, laptop, atau perangkat Bluetooth.

5. Internet.

   Internet merupakan akronim dari *interconnection network* yang berarti berbagai komputer yang terhubung dengan bermacam-macam tipe jaringan dengan cakupan ruang seluruh dunia. Dengan internet semua orang di seluruh penjuru dunia bisa mendapatkan informasi yang sama dalam waktu yang bersamaan pula. Namun terkadang banyak orang menjadikan kesempatan untuk menyebar informasi yang salah (*hoax*) yang bisa berdampak buruk pada suatu individu maupun organisasi. (Khashaaisha Al Fikri dan Djuniadi. 2021).

2.5 Macam-macam Keamanan Jaringan Komputer

Jaringan komputer memiliki berbagai aspek dan fungsi masing-masing, begitu juga dengan sistem keamanan jaringan juga dirancang sesuai dengan fungsi

Dan tujuannya masing-masing, diantaranya :

1. Web *Security.*

   Web menjadi bagian yang sangat penting dalam kemajuan teknologi. Web *Security* berperan dalam melindungi alat pencarian atau website. Selain itu, web *security* juga punya peran yang sangat penting terhadap *e-commerce* yang menyimpan ribuan bahkan jutaan data para pelanggan. Bentuk dari web *security* biasanya seperti *secure socket layer* yang digunakan sebagai alat untuk meningkatkan keamanan sebuah website. Seperti situs web yang sudah dipasang sertifikat SSL, bisa ditandai dengan ikon gembok pada bagian *address bar browser*.

2. *E-mail Security.*

   Selain melalui website, pencurian data juga marak terjadi melalui email. Beberapa informasi krusial di simpan dalam email, maka dari itu email *security* sangatlah penting. Email *security* sendiri bekerja dengan cara memblokir serangan-serangan yang membahayakan dan berpotensi mencuri data-data penting. Umumnya, email *security* juga dilengkapi dengan sistem *sofware* antispam yang melindungi semua penggunanya.

3. *Wireless Security*.

   Saat ini, hampir semua perangkat terhubung secara *wireless* atau nirkabel. Jaringan nirkabel ini juga menjadi salah satu bagian yang rentan diserang oleh orang yang tidak bertanggungjawab. Keamanan jaringan nirkabel sangatlah rendah sebab jaringan nirkabel hanya memiliki konfigurasi dan jenis enkripsi yang sangat lemah. *Wireless Security* biasanya digunakan untuk mengantisipasi serangan virus dari luar.

4. *Application Security*.

   Application Security juga sangat penting sebab aplikasi juga menyimpan banyak data pengguna dan seringkali menjadi sasaran pencurian data. *Application Security* akan membuat tingkat keamanan yang lebih tinggi lagi dan terbebas dari serangan *cyber*.

5. *Endpoint Security.*

   Perangkat komputer yang digunakan bisa menjadi sasaran dari pencurian data. *Endpount security* bisa berfungsi sebagai alat keamanan pada perangkat pribadi yang terhubung dalam jaringan bisnis.

6. *Firewall*.

   Firewall bekerja seperti perisai untuk mengamankan jaringan komputer. Selain itu, untuk jaringan komputer internal dari sebuah jaringan eksternal juga perlu dicurigai. Jika menggunakan *firewall*, *traffic* jaringan bisa diperiksa berdasarkan beberapa protokol. Bahkan *firewall* juga bisa digunakan untuk memblokir *traffic* yang berpotensi membahayakan.

7. *Data Loss Prevention*.

   Data Loss Prevention merupakan jenis sistem keamanan jaringan komputer yang berfungsi untuk menjaga beberapa data sensitif. Sistem Data *Loss Prevention* memiliki rancangan agar sistem bisa bekerja secara otomatis. Saat menggunakan sistem tersebut juga bisa mempermudah dalam proses pemeriksaan data pada jaringan komputer tersebut.

8. *Behavioral Analytics*.

   Sistem keamanan ini diciptakan untuk mengetahui apa saja aktivitas dari orang yang ingin menggunakan akses ilegal. Salah satu cara untuk mengatasi aktivitas-aktivitas mencurigakan adalah dengan *anomaly detection engines*. *Tools* tersebut memiliki fungsi untuk melakukan analisis pada suatu jaringan. Setelah itu pengguna internet juga diberikan notifikasi saat melakukan aktivitas-aktivitas mencurigakan dan pelanggaran.

9. Antivirus dan *Malware*.

   Antivirus dan *malware* adalah *tools* yang paling populer dan banyak digunakan. Kedua *tools* ini bekerja dengan menghapus semua virus dan *malware* yang sudah tertanam pada perangkat yang digunakan. Namun untuk *malware* lebih berbahaya dibandingkan virus, sebab *malware* tidak hanya menyerang perangkat namun juga jaringan.

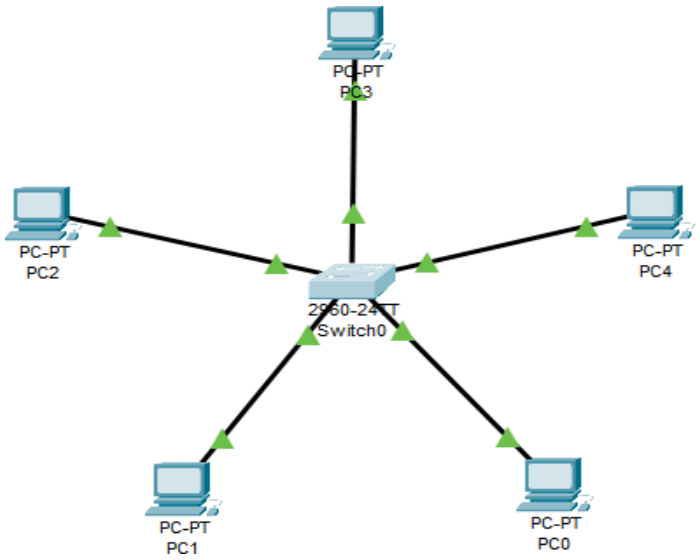
2.6 Topologi Jaringan

Topologi jaringan adalah suatu bentuk struktur jaringan yang dibangun atau dipasang sesuai dengan persyaratan dan digunakan untuk menghubungkan komputer ke komputer lain melalui media kabel atau nirkabel. Topologi jaringan dapat dikategorikan ke dalam jenis yang berbeda tergantung pada kebutuhan dan perangkatnya. Berikut beberapa topologi yang tersedia :

1. Topologi *STAR*

   Topologi *star*, atau topologi bintang, adalah salah satu bentuk konfigurasi jaringan komputer di mana setiap perangkat terhubung ke sebuah perangkat sentral yang disebut *hub* atau *switch*. Dalam topologi ini, *hub* atau *switch* berfungsi sebagai pengendali lalu lintas data, mengarahkan komunikasi antar

perangkat yang terhubung. Setiap perangkat hanya memiliki satu koneksi ke *hub* atau *switch*, membentuk pola yang menyerupai bintang.

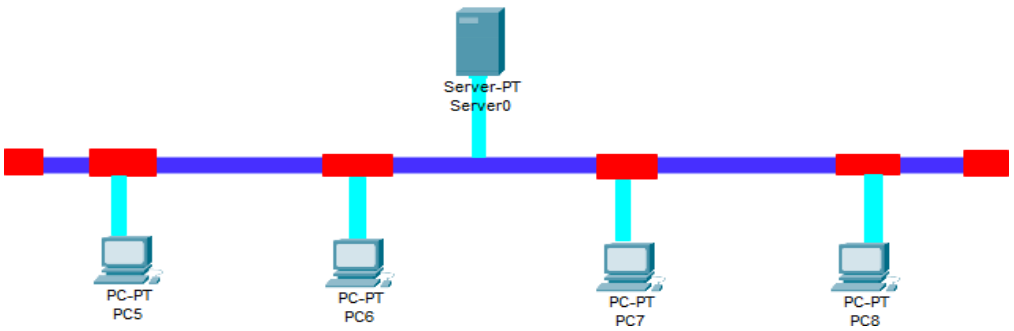


(Sumber : Bambang Kelana, dkk. 2019)

Gambar 2. 1 Topologi *STAR*

2. Topologi *BUS*

Topologi *bus* dapat dikatakan sebagai topologi jadul. Topologi ini hanya menggunakan kabel *backbone* koaksial yang berjalan pada di sepanjang *node client*, dan kabel koaksial memiliki konektor T di ujungnya sebagai kabel ujung ke ujung.

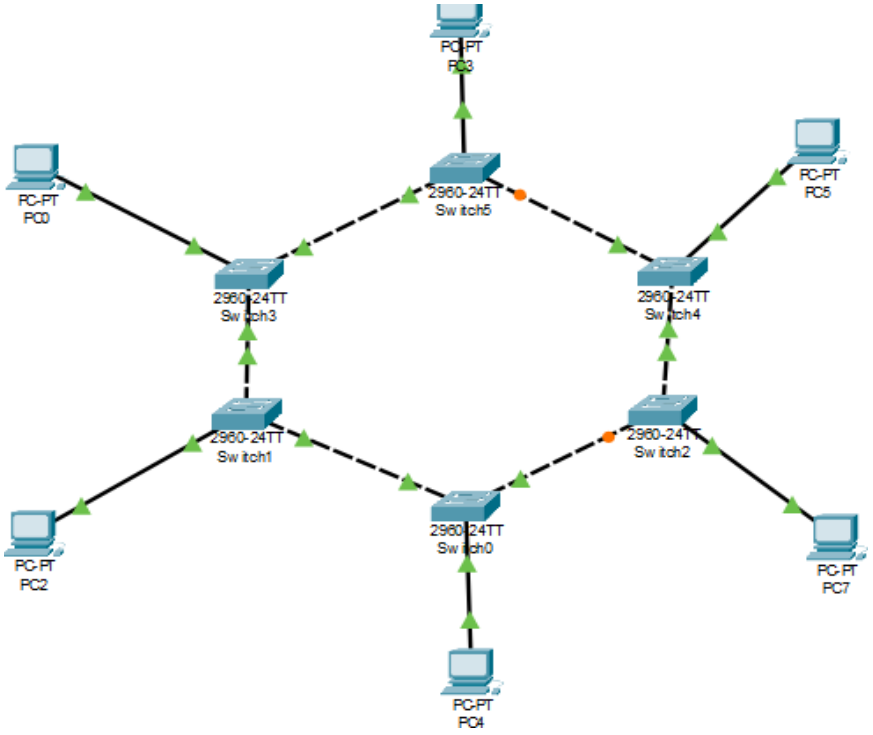


(Sumber : Bambang Kelana, dkk. 2019)

Gambar 2. 2 Topologi *BUS*

3. Topologi *RING*

Topologi *ring* merupakan topologi yang menghubungkan satu PC ke PC lainnya tanpa menggunakan *HUB/switch*. Dalam proses instalasi hanya menggunakan LAN *Card* yang tersedia dalam PC.

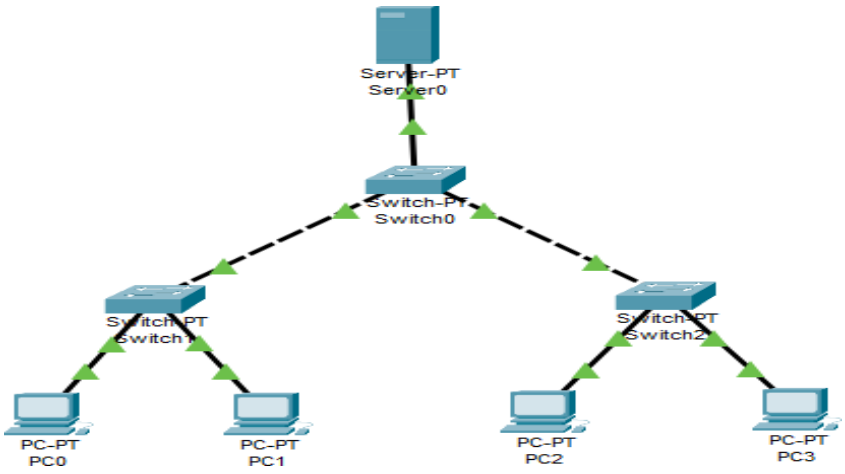


(Sumber : Bambang Kelana, dkk. 2019)

Gambar 2. 3 Topologi *RING*

4. Topologi *TREE*

Topologi *tree* merupakan gabungan topologi *star* dan *bus*, bahkan bisa juga ditambahkan untuk *ring*. Beberapa infrastruktur yang terlibat pada topologi ini membuat topologi ini menjadi lebih kompleks dan memerlukan instalasi khusus. Topologi *tree* menggunakan *backbone* sama halnya pada topologi *bus*, *backbone* berfungsi sebagai jalur tulang punggung jaringan

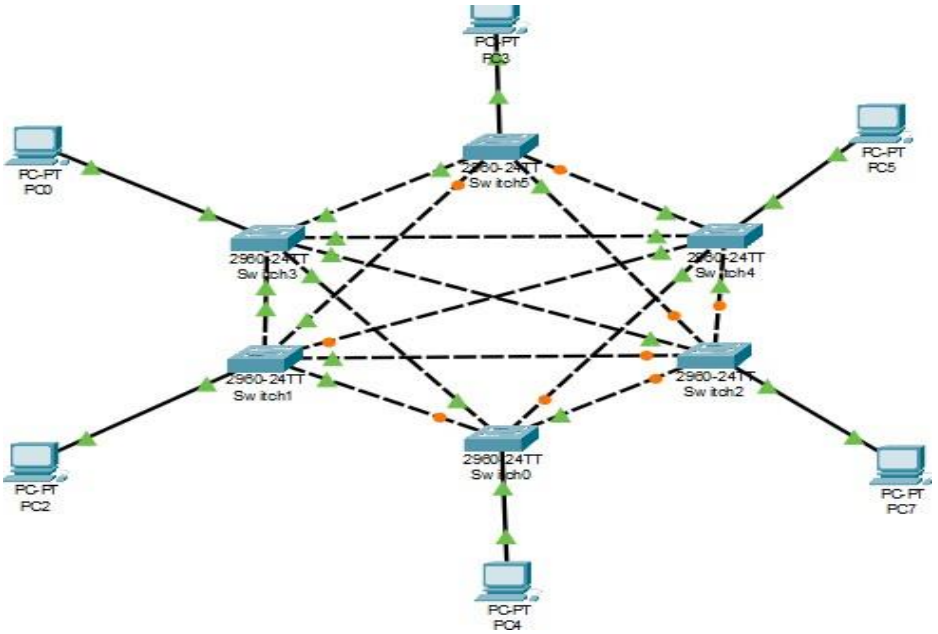


(Sumber : Bambang Kelana, dkk. 2019)

Gambar 2. 4 Topologi TREE

5. Topologi *MESH*

Ini adalah topologi untuk memilih beberapa rute jaringan. Topologi *mesh* memiliki sejumlah rute yang bertindak sebagai jalur cadangan jika jalur lainnya gagal.

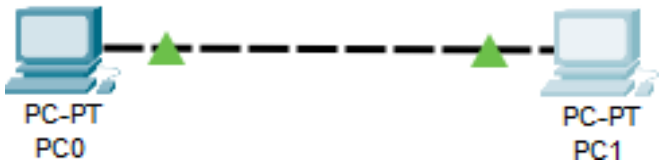


(Sumber : Bambang Kelana, dkk. 2019)

Gambar 2. 5 Topologi *MESH*

6. Topologi *PEER TO PEER*

Topologi *peer to peer* adalah jaringan komputer sederhana yang biasanya hanya menggunakan dua komputer yang terhubung melalui kabel perantara. Jaringan *peer to peer* sering digunakan untuk bertukar data antar PC.



(Sumber : Bambang Kelana, dkk. 2019)

Gambar 2. 6 Topologi *PEER TO PEER*

2.7 Firewall

Firewall yang berfungsi sebagai dinding atau partisi untuk membatasi jumlah komputer dalam jaringan internet, merupakan suatu perangkat keamanan yang menjaga komputer-komputer dalam jaringan dari berbagai bahaya. *Firewall* hadir dalam dua jenis berbasis perangkat lunak dan berbasis perangkat keras. Di antara banyak tugas yang dilakukan oleh *firewall* adalah pelarangan konten yang tidak diinginkan, pengamanan informasi pribadi, pemantauan *bandwidth*, dan akses VPN (*Virtual Private Network*). Sementara itu, *firewall* dapat dibagi menjadi tiga kategori: perangkat lunak, perangkat keras, dan *firewall* berbasis *cloud* (Tito Brades dan Irwansyah, 2021).

2.8 Port Knocking

Port knocking adalah konsep menyembunyikan layanan jarak jauh di dalam sebuah *firewall* yang memungkinkan akses ke *port* tersebut hanya untuk mengetahui *service* setelah *client* berhasil diautentikasi ke *firewall*. Hal ini dapat membantu untuk mencegah pemindai untuk mengetahui *service* apa saja yang

tersedia di *host* dan juga berfungsi sebagai pertahanan terhadap serangan *zero-day* (Santoso Nugroho Adhi, dkk. 2022). *Firewall* berfungsi untuk mengirimkan paket atau koneksi tertentu ke perangkat jaringan, seperti protokol TCP, UDP, dan ICMP. Sehingga untuk masuk dan menggunakan akses ke *port* tertentu yang telah dibatasi, maka *user* harus mengetuk terlebih dahulu dengan memasukkan *rule* yang harus dilakukan terlebih dahulu. *Rule* yang hanya diketahui oleh pihak administrator jaringan. Sebuah sistem harus memiliki keseimbangan antara keamanan dan fleksibilitas. Dengan menggunakan firewall, maka secara langsung administrator dapat mendefinisikan *user* yang dapat dipercaya dan yang tidak dapat dipercaya dengan menggunakan alamat IP sebagai kriteria filter.

Metode *port knocking* menjelaskan bahwa intergritas keamanan sangatlah penting untuk ditingkatkan, celah-celah keamanan yang terdapat pada jaringan dapat dilihat oleh orang yang tidak bertanggung jawab dan dapat menjadi ancaman yang patut diperhatikan. Salah satu bentuk keamanan jaringan yang sering digunakan oleh seorang administrator jaringan dalam pengelolaan server yaitu melalui *remote login* seperti *Secure Shell* (SSH).

Alur kerja dari *port knocking* diilustrasikan yaitu sebuah komputer server tidak akan menyediakan *port* terbuka untuk pengguna jaringan dan server juga akan mengawasi segala macam upaya untuk koneksi dapat masuk kedalamnya. Untuk memulai koneksi *client*, dimulai dengan cara koneksi ke server dengan beberapa urutan ke *well defined set of ports*, yang mana akan mengirimkan paket SYN atau *synchronous* ke *port* yang telah ditetapkan sebelumnya dalam *knock* atau ketukan. Proses *knock* inilah yang menyebabkan sebuah *port* mengetuknya, sedangkan yang terjadi pada server, yaitu server tidak akan memberikan respons terlebih dahulu

kepada *client* selama fase *knock*, namun secara tidak diketahui dari server akan menerjemahkan yaitu *decodes* dan *decrypt* pada serangkaian urutan *port-port* untuk dapat diperiksa otentifikasinya. Maka server akan mengeksekusi perintah yang diterima sehingga server dapat merespon dan *client* dapat melakukan transfer data.

2.9 Port Blocking

Metode *port blocking* pertama kali muncul dengan penggunaan *firewall* pada awal 1980-an. *Firewall* digunakan untuk melindungi jaringan dari ancaman eksternal dengan membatasi akses ke sumber daya jaringan berdasarkan berbagai kriteria, termasuk nomor *port*. Pada tahun 1990-an, metode *port blocking* menjadi lebih umum karena meningkatnya kompleksitas dan kebutuhan keamanan jaringan. Perusahaan mulai menyadari betapa pentingnya melindungi jaringan mereka dari ancaman yang semakin canggih. Protokol komunikasi seperti Protokol Kontrol Transmisi (TCP) dan Protokol Datagram Pengguna (UDP) menggunakan *port* untuk memudahkan komunikasi. Pada awalnya, beberapa *port* diatur untuk berbagai aplikasi dan layanan, seperti *port* 80 untuk *port* standar HTTP dan *port* 21 untuk *port* standar FTP. Metode *port blocking* menggunakan informasi ini untuk mengontrol akses.

Port Blocking adalah tindakan menutup *port* dan mencegah akses *host* ke *port* tersebut. *Port Blocking* menggunakan *firewall* untuk melakukan tindakannya. *Firewall* sendiri merupakan suatu sistem atau perangkat yang memungkinkan akses terhadap lalu lintas pada jaringan komputer yang dianggap aman dan memblokir lalu lintas pada jaringan yang dianggap tidak aman (Novianto et al., 2023). Jika *firewall* telah diatur secara otomatis, klien tidak dapat mengakses semua *port* yang telah diblokir atau difilter. Jika klien mengirimkan permintaan ke server layanan,

server akan membalas permintaan klient sesuai dengan permintaan klien. *Port blocking* ini sangat efektif untuk menghentikan virus dari masuknya *port* yang tidak terpercaya ke jaringan.

Alur *port blocking* terdiri dari beberapa langkah yang digunakan untuk membatasi atau menghentikan akses ke jaringan atau layanan dengan cara memblokir penggunaan nomor *port* tertentu. Pertama, *firewall* atau perangkat keamanan jaringan dikonfigurasi untuk mengawasi lalu lintas data yang melewati jaringan. Kemudian, informasi header yang mengandung nomor *port* dipelajari oleh *firewall*, yang menunjukkan protokol dan layanan yang digunakan. Selanjutnya, *firewall* memeriksa nomor *port* ini dengan aturan atau kebijakan keamanan administrator jaringan. Jika nomor *port* tersebut diizinkan sesuai dengan aturan, lalu lintas dapat melanjutkan ke tujuannya. Namun, jika nomor *port* tersebut termasuk dalam daftar yang diblokir, *firewall* akan menghentikan lalu lintas dan mencegahnya mencapai tujuannya. Alur kerja ini memungkinkan administrator jaringan untuk memilih *port* mana yang ingin diblokir atau diizinkan, memberikan kontrol yang lebih ketat terhadap akses ke layanan dan sumber daya jaringan. Ini juga memungkinkan penyesuaian yang fleksibel sesuai dengan kebijakan keamanan dan kebutuhan khusus organisasi atau jaringan.

2.10 Mikrotik

Mikrotik merupakan suatu perangkat yang mengubah suatu komputer menjadi suatu rangkaian yang dapat melakukan berbagai tugas melalui koneksi internet sehingga suatu komputer dapat dengan mudah dikendalikan oleh komputer lain (Fakhri Khafif, 2021). Mikrotik dapat digunakan sebagai router *filtering*, *switching*, atau alat lainnya. Router mikrotik adalah satu solusi dari masalah

keamanan jaringan komputer dikarenakan fitur-fitur yang terdapat pada router mikrotik dapat digunakan dalam manajemen jaringan, sebagai perangkat jaringan yang bersifat *open source* dikarenakan router mikrotik ini dapat disesuaikan dengan *network* yang berbeda yakni bisa digunakan untuk *cable network* maupun *wireless network* yang memungkinkan siapa saja dapat merubahnya sesuai dengan kebutuhannya. Perangkat keras Mikrotik dapat berupa router PC (yang diinstal pada PC user) atau *board router* (dibangun langsung oleh Mikrotik), Saat ini terdapat beberapa versi *software* Mikrotik yang disebut dengan RouterOS.

2.11 Jenis-Jenis Mikrotik

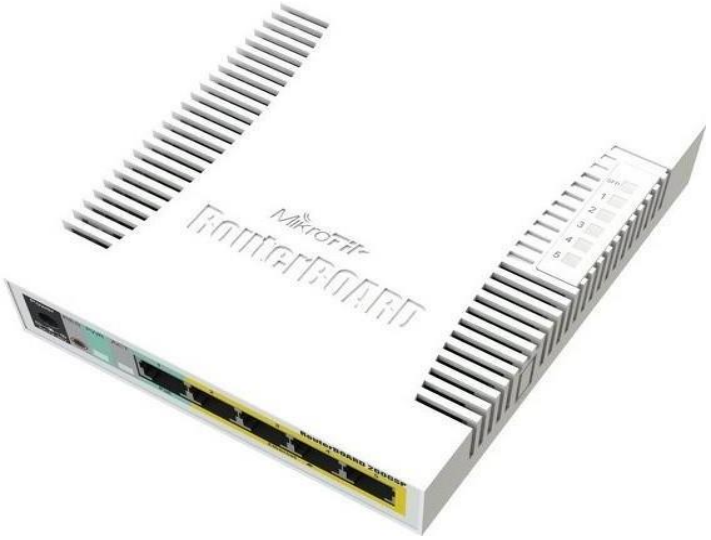
Mikrotik sebagai salah satu penyedia solusi jaringan terkemuka menawarkan berbagai jenis perangkat dan fitur yang dapat membantu dalam membangun dan mengelola jaringan dengan efisien. Jenis *router* mikrotik dalam jaringan komputer terdiri atas :

1. Mikrotik *RouterOS*

   Mikrotik *routerOS* adalah perangkat lunak yang mengubah komputer menjadi *router*. Instalasi Mikrotik RouterOS pada router *Cisco* mirip dengan *Cisco IOS*, namun memerlukan emulator seperti GNS3 dan lainnya untuk menginstalnya secara manual. Pada dasarnya *RouterOS* adalah sistem operasi yang memanfaatkan kernel Linux v2 yang disebut Mikrotik *RouterBOARD*.

2. Mikrotik *Routeboard*

   Mikrotik *RouterOS* tidak hanya dapat diinstal pada PC tetapi juga pada perangkat keras khusus yang disebut *routerboard*. Biasanya saat membeli *routerboard* Mikrotik, sudah dilengkapi dengan *RouterOS* yang terinstal.

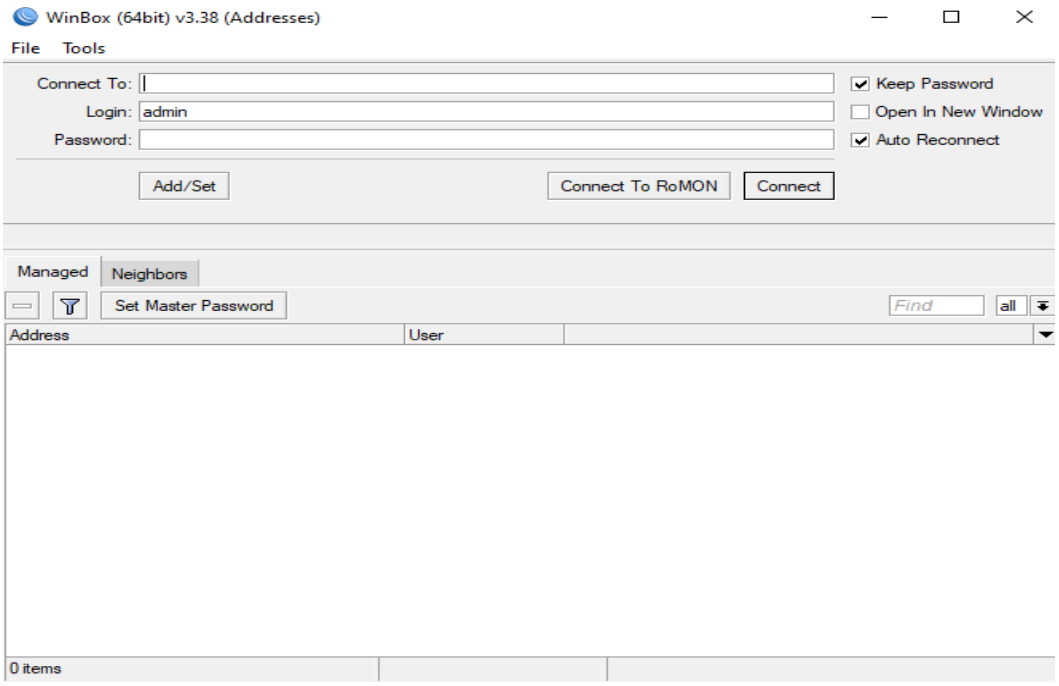


(Sumber : www.Citraweb.com)

Gambar 2. 7 RouterBoard Mikrotik

2.12 Winbox

Winbox adalah keefektifan yang digunakan untuk koneksi dan konfigurasi Mikrotik menggunakan alamat MAC atau protokol IP (Fakhri Khafif, 2021). Winbox menyediakan GUI yang mempermudah pengguna untuk mengelola dan mengkonfigurasi perangkat mikrotik. Dengan menggunakan winbox, *user* dapat melakukan berbagai konfigurasi, seperti pengaturan jaringan, *firewall*, *routing*, manajemen pengguna, dan lainnya. *Software* ini memberikan akses yang mudah dan cepat ke berbagai fitur *RouterOS* tanpa perlu menggunakan antarmuka baris perintah. Winbox mempunyai beberapa kelebihan, dengan kata lain, ada banyak fitur untuk mengonfigurasi *proxy*, dan perangkat lunak ini memudahkan pemeliharaan dan pengelolaan *proxy* yang memakainya. Winbox umumnya digunakan oleh administrator jaringan dan pengelola sistem untuk mengelola perangkat Mikrotik dengan lebih efisien.



(Sumber : Tito Brades dan Irwansyah, 2021)

Gambar 2. 8 Tampilan Awal Winbox versi 3.38

2.13 VirtualBox

Oracle VirtualBox adalah perangkat lunak virtualisasi yang dapat diinstal pada sistem operasi Windows, Linux, MacOS, dan Solaris. Dengan menggunakan VirtualBox, pengguna dapat membuat dan menjalankan mesin virtual pada perangkat keras mereka. Mesin virtual ini memungkinkan pengguna untuk menjalankan beberapa sistem operasi yang berbeda secara bersamaan, baik itu sistem operasi yang sama atau berbeda (Ridho Akbar Nuryadin, dkk. 2023). *User* dapat dengan mudah mengelola sumber daya mesin virtual seperti memori, penyimpanan, jaringan, dan perangkat I/O.

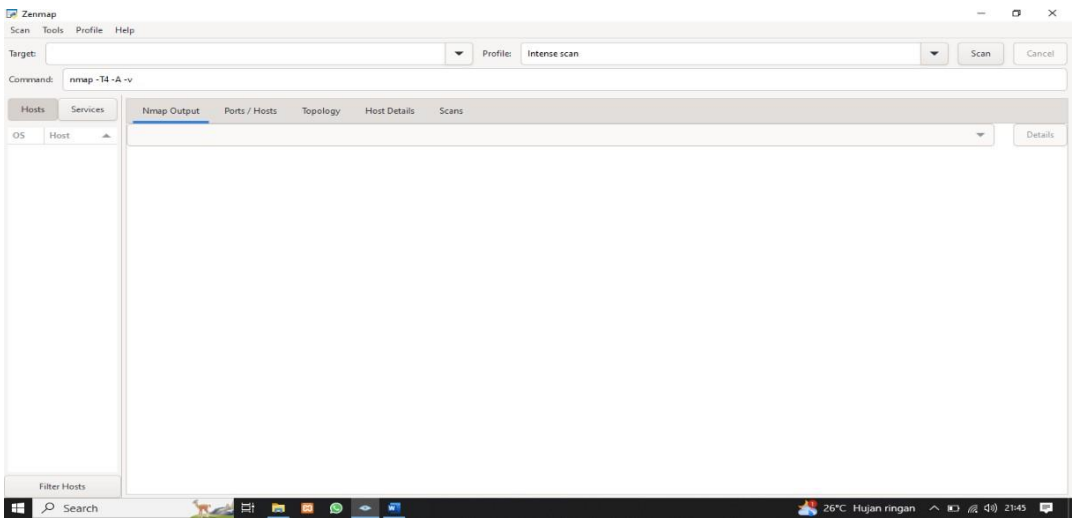
2.14 PuTTY (*Phonetic Transcription*)

PuTTY suatu aplikasi *open source* yang sering digunakan untuk melakukan remote akses SSH dari jarak jauh, remote akses tentunya masih terkoneksi dengan

jaringan internet. Aplikasi ini biasanya digunakan untuk mengakses komputer *server*, komputer server umumnya terletak ditempat yang jauh, dengan aplikasi ini, kita bisa mengelola *server* tersebut tanpa harus mendatanginya secara fisik.

2.15 NMAP (*Network Mapper*)

Network Mapper (NMAP) adalah adalah alat investigasi dan audit keamanan jaringan sumber terbuka. Nmap menggunakan paket IP mentah untuk mengidentifikasi *host* yang terhubung ke jaringan Anda, termasuk layanan tertentu (nama dan versi aplikasi), sistem operasi (dan versi) tertentu, jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya (Rendro Dwi Bayu, dkk. 2020). Fungsi utama Nmap adalah untuk memindai *port*. Pemindaian *port*, menurut definisi, adalah sejumlah aktivitas pengujian menggunakan alat otomatis (dalam hal ini Nmap). Sebuah *scanner* sebenarnya adalah pemindai *port* TCP/IP, sebuah program yang menyerang *port* TCP/IP dan layanannya (*Telnet*, FTP, *http*, *https*) dan mencatat respons komputer target. Dengan cara ini, pengguna program pemindai dapat memperoleh informasi berharga dari *host* target.



(Sumber : Tito Brades dan Irwansyah, 2021)

Gambar 2. 9 Tampilan Awal NMAP

Output dari Nmap adalah daftar *host* target yang diperiksa dan informasi tambahan tergantung pada opsi yang digunakan. Hal kunci dari informasi ini adalah "Tabel *Port* yang Menarik". Tabel ini mencantumkan nomor *port* dan protokol, nama layanan, dan status. Status dapat terbuka, terfilter, tertutup, atau tanpa filter. "Terbuka" berarti aplikasi pada komputer target mendengarkan koneksi/paket pada *port* ini.

2.16 Wireshark

Wireshark adalah alat yang dirancang untuk menganalisa paket data yang ada di jaringan internet. Salah satu fitur Wireshark adalah *Network Packet Analyzer*, yang dapat menangkap semua data yang ada saat komunikasi data di jaringan internet dan menampilkan data tersebut sedetail mungkin.

Fungsi wireshark yang utama adalah sebagai administrator jaringan untuk dapat melacak apa yang terjadi didalam jaringan miliknya atau untuk memastikan jaringannya bekerja dengan baik, serta tidak ada yang melakukan hal-hal buruk pada jaringan itu.

2.17 *Transmission Control Protocol dan Internet Protocol* (TCP/IP).

Arsitektur TCP/IP menggunakan model refrensi DARPA (*Defense Advanced Research Project Agency*) yang awalnya merupakan protokol yang dikembangkan dari proyek ARPANET yang dimulai oleh Departemen Pertahanan Amerika Serikat. Protokol ini dikembangkan sebelum model OSI (*Open System Interconnection*). Namun lapisan-lapisan pada TCP/IP tidak sama dengan lapisan-lapisan yang dimiliki oleh OSI. Protokol TCP/IP hanya dibuat atas empat lapisan, yaitu : *network*, internet, *transport* dan *application*.

1. *Network Layer* (Lapisan Jaringan)

   Menyediakan *frame-frame* data yang dikirim ke media jaringan. Lapisan ini bertaggung jawab untuk mengelola semua hal yang dibutuhkan paket IP.

2. *Internet Layer* (Lapisan Internet)

   Menyediakan *Routing* dan pembuatan paket dengan teknik *encaptulation*. Fungsi utama lapisan internet adalah seleksi rute dalam sebuah jaringan. Selain itu, lapisan ini juga bertanggung jawab menyelesaikan sebuah paket *swictching*

3. *Trasnsport Layer* (Lapisan Transport)

   Ada perbedaan penting antara lapisan jaringan dan lapisan *transport*, setiap *node* membutuhkan lapisan *transport.* Lapisan ini juga ada protokol yang dapat digunakan untuk mengirimkan data yaitu *User Diagram Protokol* (UDP) dan *Protokol Kontrol Transmisi* (TCP).

4. *Application Layer* (Lapisan Aplikasi)

   Lapisan aplikasi pada TCP/IP setara dengan tiga lapisan yang terdapat pada model OSI. Format data pada level ini biasanya disebut dengan pesan. Komunikasi pada *later* ini sama seperti pada *transport layer* yaitu *end-to-end*. Beberapa protokol yang ada pada lapisan ini sebagai berikut :

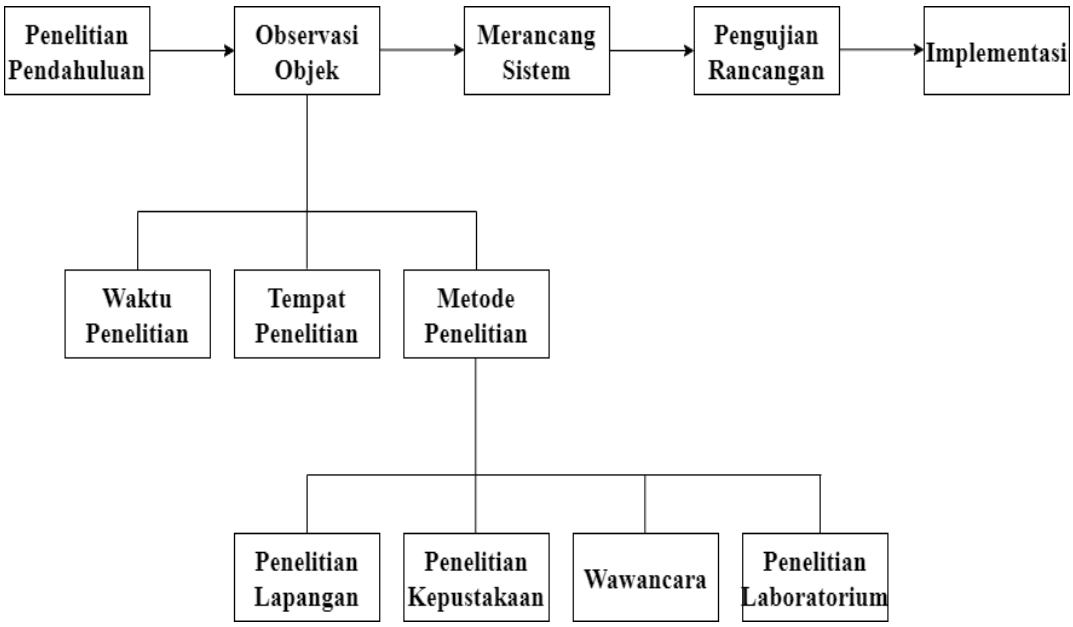
   - HTTP (*Hyper Text Transfer Protocol*) yang digunakan untuk layanan web.
   - *Telnet* yang berfungsi untuk melakukan remote pada suatu host.
   - FTP (*File Transfer Protokol*) yang digunakan untuk keperluan *file sharing.*

BAB III

METODOLOGI PENELITIAN

3.1 Kerangka Kerja Penelitian

Agar langkah- langkah yang diambil penulis dalam penelitian ini tidak melenceng dari pokok pembahasan dan lebih mudah dipahami, maka urutan langkah- langkah akan dibuat secara sistematis sehingga dapat dijadikan pedoman yang jelas dan mudah untuk menyelesaikan permasalahan yang ada. Urutan langkah- langkah yang akan dibuat pada penelitian ini dapat dilihat pada Gambar 3.1 berikut :



Gambar 3. 1 Kerangka Penelitian

3.2 Tahapan Penelitian

Dalam penelitian ini, tahapan penelitian didedikasikan untuk memperoleh informasi yang relevan dan menerapkannya untuk menarik kesimpulan. Berikut tahapan-tahapan yang dilalui dalam penelitian untuk memperoleh kesimpulan.

a. Penelitian pendahuluan

Penelitian pendahuluan merupakan langkah awal melakukan suatu penelitian dengan terlebih dahulu menganalisa masalah-masalah yang akan dikembangkan. Dalam melakukan analisa dapat menentukan rancangan solusi dalam penyeleseian masalah. Tujuan yang akan diterapkan dapat membantu menjaga dan meningkatkan keamanan jaringan pada Kantor Dinas Kesehatan Kabupaten Tanah Datar.

b. Observasi Objek

Observasi objek adalah kegiatan pengamatan secara langsung terhadap suatu objek atau fenomena dengan menggunakan indera manusia atau alat bantu untuk mengumpulkan informasi dan data yang dapat digunakan untuk analisis atau pemahaman lebih lanjut terkait karakteristik, perilaku, atau sifat dari objek tersebut.

Mengenai aspek-aspek yang terkait dengan proses pengumpulan data pada objek penelitian ini, berikut adalah beberapa hal yang perlu diperhatikan :

1. Waktu Penelitian

   Waktu penelitian didefinisikan sebagai jumlah waktu yang dialokasikan untuk melakukan penyelidikan atau investigasi sistematis terhadap suatu topik atau pertanyaan penelitian dengan tujuan mengumpulkan data, menganalisis informasi, dan membuat kesimpulan yang dapat meningkatkan pemahaman tentang topik penelitian. Proses penelitian memiliki rentang waktu yang berlangsung dari Oktober 2023 hingga Juni 2024. Untuk lebih jelas rentang waktu penelitian dapat dijelaskan pada Tabel 3.1 berikut :

Tabel 3. 1 Waktu Penelitian

Kegiatan/ Waktu	Minggu ke	Penelitian Pendahuluan	Observasi Objek	Merancang Sistem	Pengujian Rancangan	Implementasi
Oktober 2023	1					
	2					
	3					
	4					
November 2023	1					
	2					
	3					
	4					
Desember 2023	1					
	2					
	3					
	4					
Januari 2024	1					
	2					
	3					
	4					
Februari 2024	1					
	2					
	3					
	4					
Maret 2024	1					
	2					
	4					
April 2024	1					
	2					
	3					
	4					
Mei 2024	1					
	2					
	3					
	4					
Juni 2024	1					
	2					
	3					
	4					

2. Tempat Penelitian

   Tempat penelitian adalah lokasi atau wilayah khusus yang dipilih untuk melakukan studi, eksperimen, atau pengumpulan data dalam rangka mendapatkan pemahaman mendalam atau informasi yang relevan terkait dengan suatu topik penelitian. Pelaksanaan penelitian ini dilakukan oleh penulis pada Kantor Dinas Kesehatan Kabupaten Tanah Datar. Alamat dari kantor ini yaitu di jalan Sultan Alam Bagarsyah, Pagaruyung, Pagar Alam, Kabupaten Tanah Datar, Sumatera Barat.

3. Metode Penelitian

   Metode penelitian adalah serangkaian langkah atau prosedur sistematik yang digunakan untuk merencanakan, mengumpulkan, menganalisis, dan menyajikan data guna memahami fenomena atau menjawab pertanyaan penelitian dengan cara yang objektif dan terstruktur. Dalam melakukan penelitian ini, metode-metode yang penulis lakukan adalah sebagai berikut:

   a. Penelitian Lapangan (*Field Research*)

      Untuk mencapai hasil penelitian yang optimal, diperlukan pelaksanaan penelitian lapangan, yang melibatkan observasi langsung di Kantor Dinas Kesehatan Kabupaten Tanah Datar.

   b. Penelitian Kepustakaan (*Library Research*)

      Dalam penelitian ini, penulis juga menggunakan jenis penelitian kepustakaan (*library research*) yaitu serangkaian kegiatan yang dilakukan dengan cara menelusuri berbagai kajian pusataka, metode pengumpulan data pustaka, penelitian kepustakaan. Penelitian Pustaka ini dilakukan untuk mempelajari sumber-sumber tersebut yang akan

mendukung penulisan pada penelitian ini. Sumber-sumber tersebut berupa buku dan hasil penelitian. Untuk hasil penelitian yang menjadi referensi dapat berupa jurnal ilmiah, laporan penelitian, dan skripsi. Termasuk dalam kategori ini bahan bahan yang dipublikasikan secara online (akses internet). Penelitian yang dilakukan untuk mengumpulkan data sekunder dengan membaca buku-buku, jurnal, literatur-literatur yang ada kaitannya dengan penelitian yang dijadikan sebagai bahasa referensi. Hal ini dimaksudkan untuk mendapatkan data- data yang lebih akurat dan terpercaya.

c. Wawancara (*Interview*)

Agar memperoleh data dan informasi terkait penggunaan jaringan di Kantor Dinas Kesehatan Kabupaten Tanah Datar, penulis melakukan wawancara langsung dengan pihak-pihak yang terkait agar mendapatkan data-data yang diperlukan.

d. Penelitian Laboratorium (*Laboratory Research*)

Penelitian ini bertujuan untuk menginvestigasi penerapan metode *port knocking* dan *port blocking* di Kantor Dinas Kesehatan Kabupaten Tanah Datar menggunakan perangkat komputer. Dalam konteks ini, spesifikasi perangkat keras yang digunakan meliputi :

1. Laptop Acer Aspire, sebagai Server
    - Prosessor Intel (R) Core (TM) i3-6006U CPU @2.00 GHz
    - Memory 12 GB.
    - SSD 256 GB
    - Harddisk 1 TB.

2. Laptop Hp Elitebook 830, sebagai PC Admin
    - Prosessor Intel (R) Core (TM) i7-8000U CPU @2.4 GHz.
    - Memory 8 GB.
    - SSD 256 GB
3. Laptop Lenovo Ideapad slim, sebagai PC Client
    - Prosessor Intel (R) Core (TM) i7-12000U CPU @2.6 GHz.
    - Memory 8 GB.
    - SSD 256 GB
4. Mikrotik rb941-2nd
5. Tiga (3) unit kabel LAN RJ45

Sedangkan perangkat lunak yang digunakan dalam penelitian ini antara lain:

1. Sistem Operasi Windows 10 dan Windows 11
2. Microsoft Office 2021.
3. Winbox.
4. Putty
5. Web Browser

3.3 Merancang Sistem

Merancang sistem merupakan awal sebelum sistem itu bisa digunakan. Dalam rancangan ini meliputi bagaimana menggunakan metode *port knocking* dan *port blocking*. Hasil ini nantinya menghasilkan sebuah sistem yang dapat digunakan untuk keamanan jaringan dengan penerapan metode *port knocking* dan *port blocking* pada Kantor Dinas Kesehatan Kabupaten Tanah Datar.

3.4 Pengujian Rancangan

Dalam proses pengujian rancangan ini akan dilakukan pengujian untuk memastikan bahwa sistem telah berjalan dengan benar dan sesuai dengan perancangan yang telah dilakukan. Dalam hasil ini, kepentingan utama adalah kemampuan memonitor hasil dari penerapan metode *port knocking* dan *port blocking* di Kantor Dinas Kesehatan Kabupaten Tanah Datar.

3.5 Implementasi

Implementasi merupakan fase dimana sistem yang telah direncanakan pada tahap sebelumnya diaplikasikan, baik berupa perangkat lunak (*software*) maupun perangkat keras (*hardware*) yang telah disiapkan. Dengan penerapan sistem tersebut, hasilnya dapat dioperasikan dan dimanfaatkan secara optimal sesuai dengan kebutuhan yang telah ditetapkan. Tujuan dari implementasi ini adalah untuk mengkonfigurasi rancangan sehingga dapat memberikan masukan yang sesuai bagi Kantor Dinas Kesehatan Kabupaten Tanah Datar.

BAB IV

ANALISA DAN PERANCANGAN

4.1 Analisa Sistem

Analisa sistem adalah tahap penting dalam penerapan sistem karena tahap ini mengevaluasi kinerja sistem secara keseluruhan dan menemukan masalah untuk mengidentifikasi kekurangan dan hambatan sistem. Pada akhirnya, tahap ini menghasilkan kesimpulan dari analisis untuk menentukan apakah sistem layak untuk digunakan atau tidak.

4.1.1 Analisa Sistem Yang Berjalan

Pada penelitian ini, Kantor Dinas Kesehatan Kabupaten Tanah Datar belum terdapat sistem keamanan untuk mencegah akses pihak lain memasuki sistem jaringan yang memungkinkan terjadinya kebocoran data pada Kantor Dinas Kesehatan Kabupaten Tanah Datar, sehingga data-data itu nantinya dapat disalah gunakan oleh pihak ketiga atau *hacker*.

4.1.2 Alternatif Pemecahan Masalah

Alternatif pemecahan masalah dalam mengatasi masalah tersebut lalu peneliti menerapkan metode *port knocking* dan *port blocking* untuk membuka atau menutup akses ke *port* tertentu dengan menggunakan *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu, supaya hanya orang-orang karyawan atau staff Kantor Dinas Kesehatan Kabupaten Tanah Datar yang bisa mengakses router mikrotik.

4.2 Perancangan

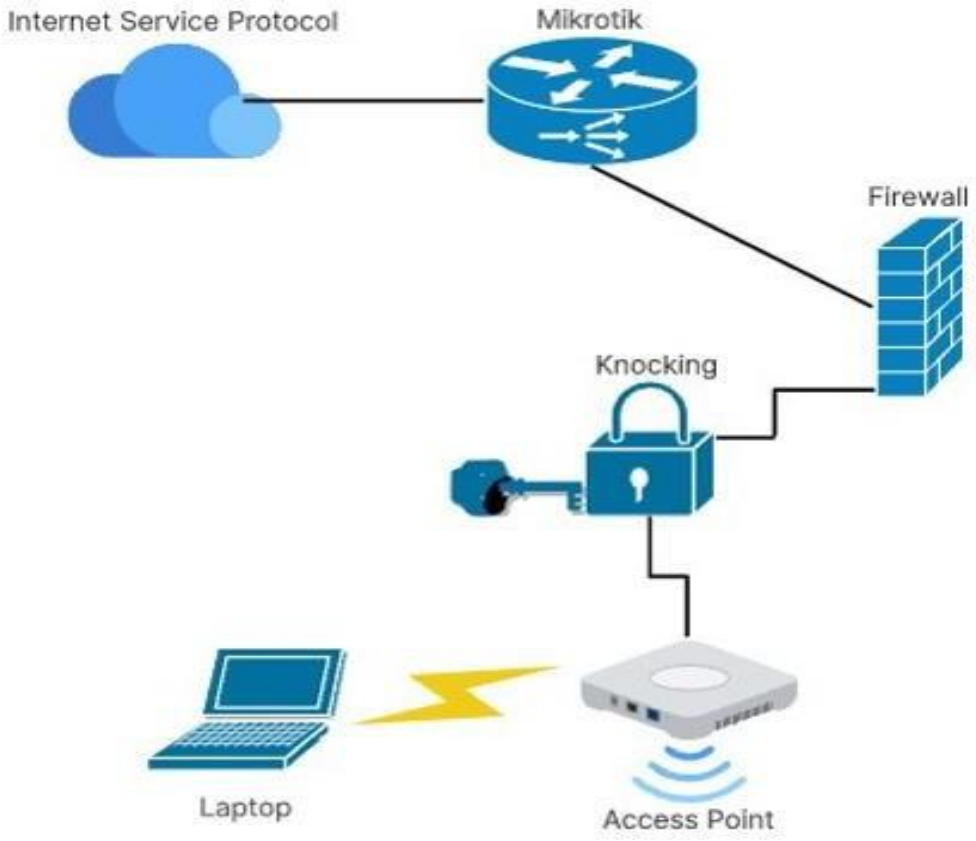
Untuk membuat susunan sistem yang akan menggunakan metode *port knocking* dan *port blocking* di Kantor Dinas Kesehatan Kabupaten Tanah Datar, tahap perancangan berfungsi sebagai penentuan. Tahap ini memberikan gambaran rancangan bangun yang lengkap sebagai pedoman.

4.2.1 Perancangan Topologi

Perancangan topologi adalah proses penting dalam pengembangan jaringan komputer yang efisien, aman, dan dapat diandalkan. Topologi jaringan menggambarkan bagaimana berbagai perangkat dalam suatu jaringan diatur dan terhubung satu sama lain. Pilihan topologi yang tepat akan mempengaruhi kinerja, skalabilitas, dan keamanan jaringan secara keseluruhan untuk mengetahui alur sistem metode *port knocking* dan *port blocking* dalam perancangan topologi yang digunakan.

4.2.1.1 Perancangan Topologi *Port Knocking*

Gambar 4.1 dibawah menunjukkan implementasi yang akan digunakan, yang dimulai dari *user*/labtop ke server, yang memungkinkan untuk membuat aturan menggunakan metode keamanan jaringan *port knocking* pada *router* mikrotik yang sudah terhubung ke jaringan internet. Setelah itu, perangkat yang harus terhubung ke jaringan dihubungkan untuk memungkinkan metode keamanan jaringan *port knocking*. Untuk autentikasi topologi *port knocking* ini terdapat 1 PC/labtop admin serta 1 *router* mikrotik. Dalam jaringan tersebut terdapat beberapa layanan jaringan seperti: FTP, SSH, WINBOX, dan WWW untuk bisa mengakses server jaringan mikrotik.



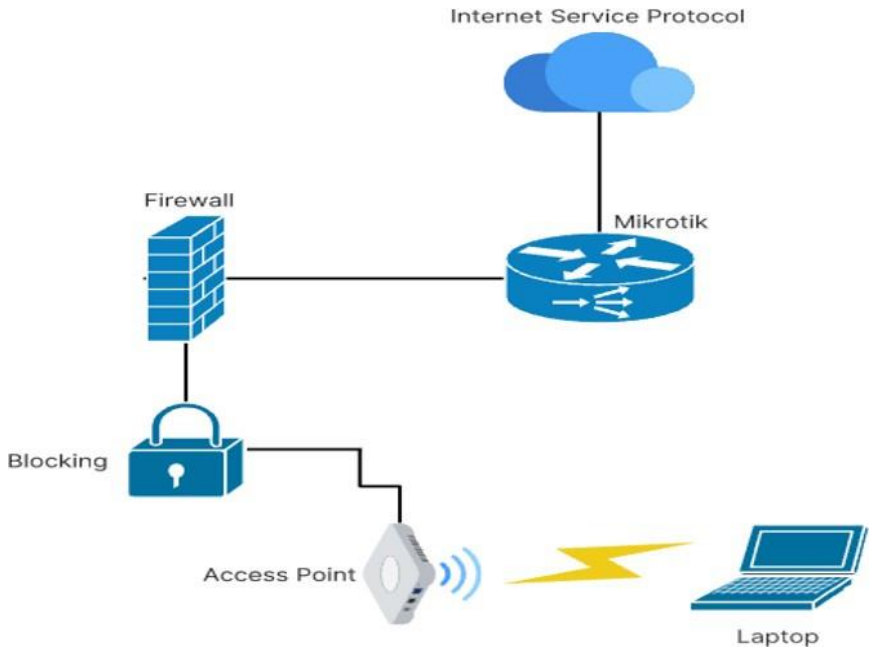
(Sumber : Randi Rizal, dkk. 2020)

Gambar 4. 1 Topologi *Port Knocking*

4.2.1.2 Perancangan Topologi *Port Blocking*

Perancangan yang dibuat untuk *port blocking* adalah keamanan yang memungkinkan seseorang mengakses suatu sistem dengan mengakses sejumlah *port* tertentu dalam urutan tertentu sebelum mendapatkan izin untuk terhubung ke *port* tujuan yang sebenarnya (Randi Rizal, dkk. 2020). Ide di balik aturan ini adalah bahwa hanya orang yang tahu urutan atau akses *port* yang benar yang dapat mengakses layanan atau *port* tujuan.

Gambar 4.2 memberikan penjelasan bahwa terdapat *user* sebuah PC/laptop yang menjadi admin untuk menguji server mikrotik yang sudah diamankan menggunakan *port knocking*.



(Sumber : Randi Rizal, dkk. 2020)

Gambar 4. 2 Topologi *Port Blocking*

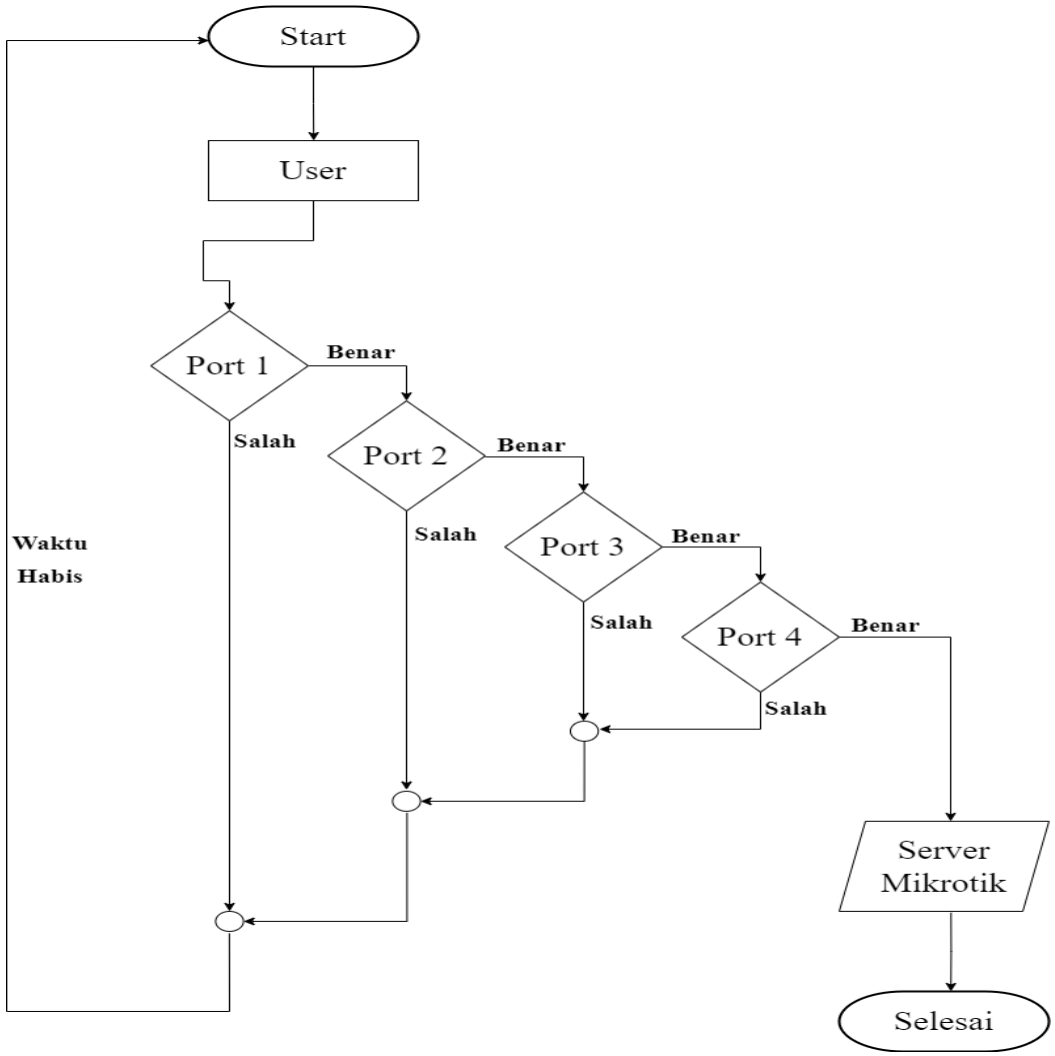
Aturan yang dibuat untuk *port blocking* adalah memblokir akses atau komunikasi melalui saluran komunikasi. Administrator jaringan dapat memilih untuk memblokir *port-port* tertentu yang dianggap berisiko atau tidak perlu dalam hal ini (Randi Rizal, dkk. 2020).

4.2.2 Perancangan *Flowchart*

Perancangan *flowchart* adalah proses penting dalam visualisasi alur kerja, prosedur, atau sistem yang kompleks menjadi gambar yang sederhana dan mudah dimengerti. *Flowchart*, atau diagram alir, menggunakan berbagai simbol seperti kotak, panah, dan lingkaran untuk menggambarkan langkah-langkah dan keputusan dalam suatu proses. Ini membantu dalam mengidentifikasi dan menganalisis setiap tahapan, memungkinkan pemahaman yang lebih baik serta meningkatkan efisiensi dan efektivitas dalam implementasi.

4.2.2.1 **Perancangan *Flowchart Port Knocking***

Untuk mengetahui alur proses yang dilakukan saat menerapkan metode *port knocking* untuk keamanan jaringan, *flowchart* tentunya diperlukan. Sistem usulan penelitian ini menggunakan protokol TCP untuk melakukan autentikasi, seperti yang digambarkan dalam diagram *flowchart port knocking* pada gambar 4.3. Jika seseorang mencoba mengakses layanan jaringan server, mereka harus melakukan autentikasi terlebih dahulu untuk membuka *port* yang tertutup karena kondisi awal port layanan dikonfigurasi dalam keadaan *closed* atau tertutup.

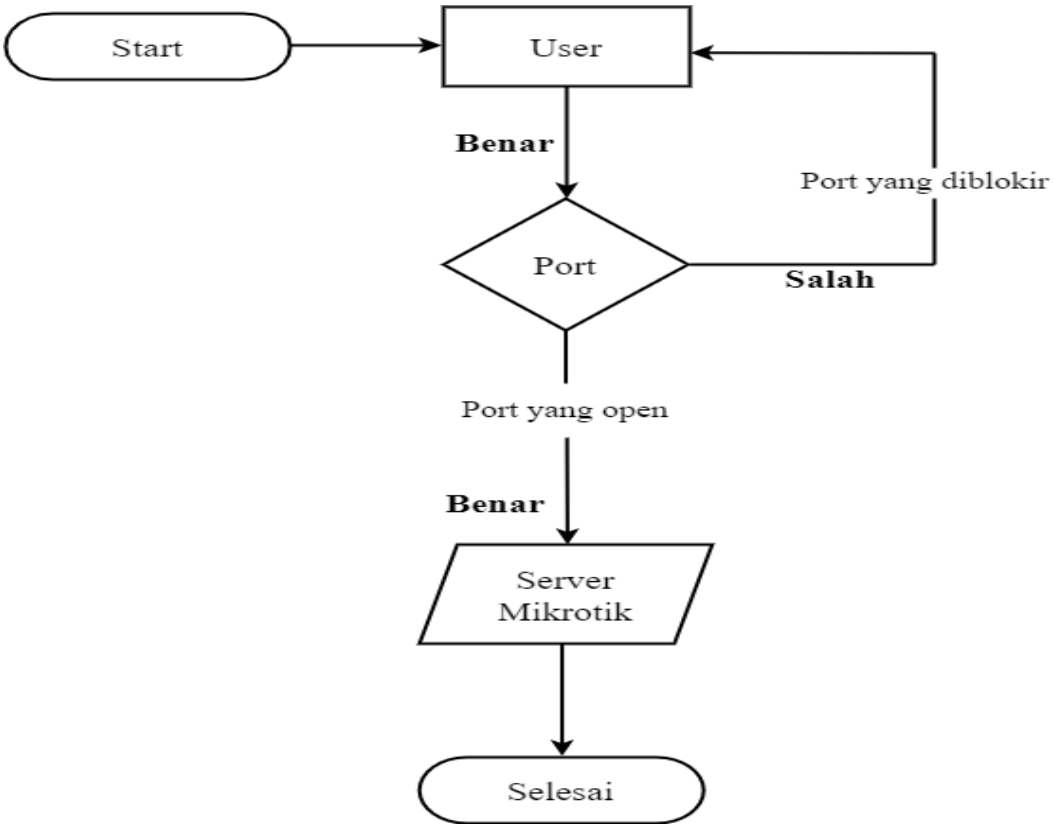


(Sumber : Randi Rizal, dkk. 2020)

Gambar 4. 3 Flowchart Port Knocking

4.2.2.2 Perancangan *Flowchart Port Blocking*

Untuk pengamanan *port blocking*, *flowchart* tetap menggunakan *port* tcp untuk mengamankan router mikrotik. Namun, untuk jenis pengamanan ini, orang yang ingin masuk ke router mikrotik haruslah orang yang memiliki akses langsung ke mikrotik. Ini karena dengan menutup *port* layanan service untuk masuk ke router mikrotik, layanan tersebut tidak dapat mengakses router mikrotik secara otomatis, seperti yang ditunjukkan pada Gambar 4.4.



(Sumber : Randi Rizal, dkk. 2020)

Gambar 4. 4 Flowchart Port Blocking

4.2.3 Perancangan Perangkat Keras

Perangkat keras atau *hardware* yang digunakan terdiri dari bagian-bagian komponen yang mendukung implementasi protokol keamanan *port knocking* dan

port blocking di jaringan. Perangkat keras atau *hardware* yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Laptop Acer Aspire One 14 Z476
2. Laptop Hp Elitebook 830
3. Laptop Lenovo ideapad slim
4. Mikrotik Rb941-2n
5. Tiga (3) unit kabel LAN RJ45

4.2.4 Perancangan Perangkat Lunak

Perangkat lunak atau *software* difungsikan untuk membuat perangkat keras yang terhubung bisa digunakan sesuai fungsi dari masing-masing perangkat keras. Perangkat lunak atau *software* yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Windows 10 dan windows 11
2. Winbox v3.38
3. Putty
4. Microsoft Office Word 2021
5. Web Browser

4.3 Data IP Address Yang Digunakan

IP Addess diperlukan oleh peniliti dalam melakukan penelitian yang dimana akan digunakan pada tahap perancangan, implementasi dan pengujian menerapkan metode *port knocking* dan *port blocking* nantinya untuk mengatasi masalah yang sedang dialami pada sistem yang sedang berjalan pada Kantor Dinas Kesehatan Kabupaten Tanah Datar.

Tabel 4. 1 *IP Address* yang Digunakan

IP Address	Keterangan
10.20.30.1	Server
172.18.1.1	Komputer Admin
192.168.10.2 – 192.168.10.254	Komputer *Client*

(Sumber : Kantor Dinas Kesehatan Kabupaten Tanah Datar)

IP address yang digunakan komputer admin dan komputer *client* pada Kantor Dinas Kesehatan Kabupaten Tanah Datar yaitu menggunakan IP *class* B dan *class* C, sedangkan server menggunakan IP *class* A untuk kebutuhan jaringan dan perangkat yang digunakan pada sistem yang sedang berjalan pada Kantor Dinas Kesehatan Kabupaten Tanah Datar.

4.4 Analisa Proses

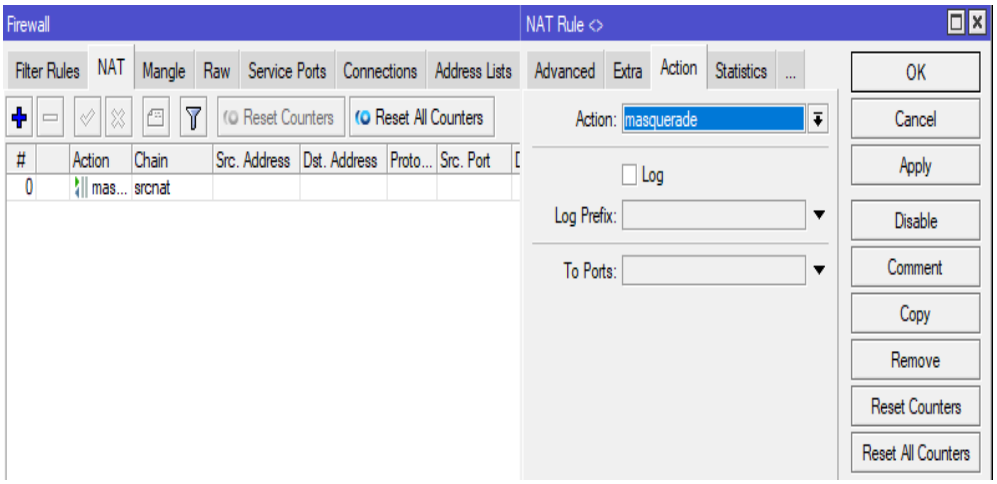
Data yang sudah diperoleh dari tempat penelitian yaitu Kantor Dinas Kesehatan Kabupaten Tanah Datar akan dilakukan penulusuran dengan menggunakan metode *port knocking* dan *port blocking* untuk mendapatkan kesimpulan dari proses penerapan metode yang digunakan oleh peneliti.

4.4.1 Metode *Port Knocking*

Proses metode *Port Knocking* melibatkan *Mikrotik* dan winbox dalam penggunaan dan penerapannya. Metode perancangan *Port Knocking* adalah langkah awal dalam melakukan implementasi metode keamanan jaringan *port knocking*. Berikut langkah perancangan metode *port knocking* sebagai berikut :

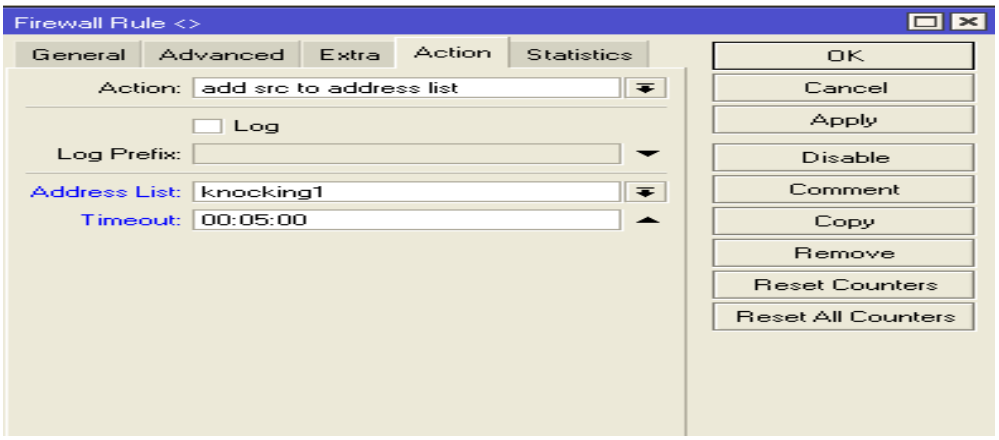
1. Menambahkan NAT *rule*

   Digunakan untuk membuat aturan untuk pengubahan *IP address* pengirim maupun penerima. Pada penerapan ini NAT *Rule* dibutuhkan agar *host* bisa terhubung dengan jaringan internet dan bisa saling berkomunikasi. Menambahkan satu aturan dengan *action masquerade*, agar tujuan dari NAT *rule* bisa dilakukan pada jaringan Kantor Dinas Kesehatan Kabupaten Tanah Datar



Gambar 4. 5 Penambahan NAT Rule

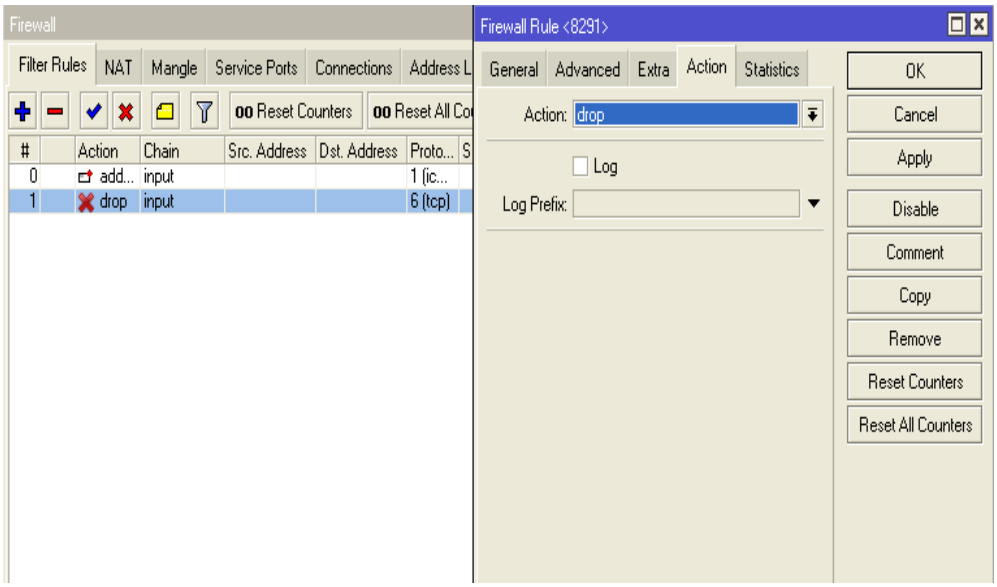
2. Membuat *input rule* pertama sebagai aturan awal masuk pada *router* sebagai penerapan keamanan jaringan metode *port knocking*.



Gambar 4. 6 Pembuatan Filter Rule Pertama

3. Menambahkan *Filter Rule* Kedua

Penambahan *input rule* kedua berfungsi untuk perintah lanjut dalam mengakses pada router.



Gambar 4. 7 Pembuatan Filter Rule Kedua

Pembuatan *filter rule* kedua pada gambar 4.7 bertujuan jika seseorang mencoba masuk pada keamanan jaringan tanpa melakukan ICMP, maka akan ditolak akses masuknya, meskipun mencoba terus menerus.

4.4.2 Metode *Port Blocking*

Proses metode *Port Blocking* juga melibatkan *Mikrotik* dan *WinBox* dalam penggunaan dan penerapannya dalam mengamankan *port* yang terbuka pada sisi komputer *client* dalam penelitian yang dilakukan.

Tahapan settingan metode *Port Blocking* yaitu juga melibatkan dua atau lebih kompter yang dimana menggunakan satu komputer *server* dan sisanya menggunakan komputer admin serta *client* target dalam mengamankan *port* yang terbuka yang akan dilakukan seperti pada tahap berikut :

1. *Filter Rule*

Membuat *filter rule* baru pada komputer target admin dan *client* untuk melakukan kebijakan boleh atau tidaknya *ether* 2 dan *ether* 3 ada dalam sebuah jaringan.

2. *Action Drop*

Action drop dari *filter rule* untuk *blocking* akses pada *port* yang akan di *blocking* seperti *port* 22, 80 dan 8291 dari *ether* 2 dan *ether* 3 yaitu komputer target Admin dan *client* agar tidak bisa mengakses *port* yang sudah di *blocking*.

BAB V

IMPLEMENTASI DAN PENGUJIAN

5.1 Implementasi

Tahap implementasi adalah tahap dimana menggunakan metode keamanan jaringan *port knocking* dan *port blocking* yang telah dirancang atau sudah melakukan pengujian untuk tujuan mengetahui hasil yang dilakukan optimal dan sesuai dengan kebutuhan.

5.1.1 Impelementasi Sistem

Implementasi sistem adalah sistem yang siap dalam melakukan metode keamanan jaringan *port knocking* dan *port blocking*, maka dibutuhkan perangkat keras (*hardware)* dan perangkat lunak (*software*) dalam melakukan implementasi.

5.1.2 Aplikasi Pendukung

Untuk sebuah metode keamanan jaringan *port knocking* dan *port blocking* bisa berfungsi dengan menggunakan beberapa aplikasi pendukung sebagai berikut:

1. Mikrotik

   Mikrotik adalah perangkat keras dan perangkat lunak yang berfungsi sebagai router dan manajemen jaringan yang dapat digunakan untuk mengontrol, mengamankan, dan mengoptimalkan lalu lintas data pada suatu jaringan komputer. Kegunaan utamanya melibatkan distribusi lalu lintas data, manajemen *bandwidth*, keamanan jaringan, dan konfigurasi berbagai fitur jaringan seperti *firewall*, VPN, dan hotspot.

Gambar 5. 1 Tampilan Mikrotik

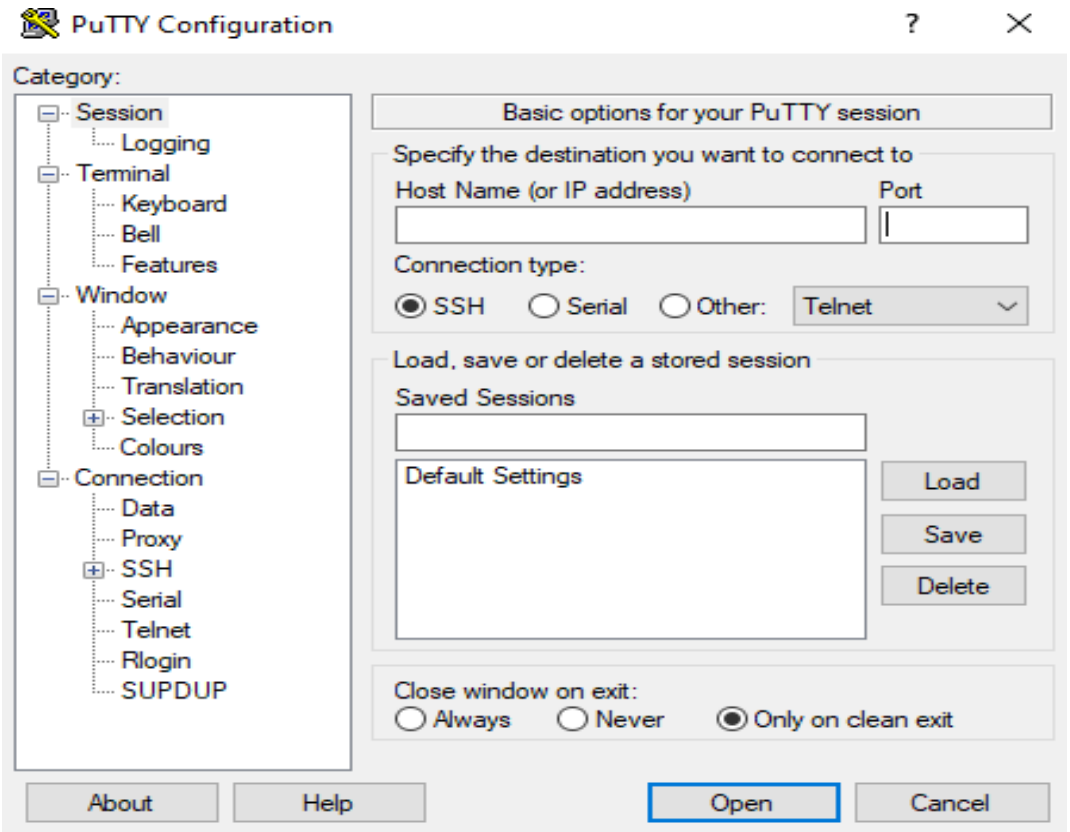
2. Winbox

   Winbox adalah aplikasi yang digunakan untuk mengatur RouterOS dengan cepat menggunakan *interfaces* yang mudah digunakan. Winbox dapat me-*remote* sebuah jaringan dengan mudah menggunakan web browser.

Gambar 5. 2 Tampilan Dalam Winbox

3. PuTTY

PuTTY (*phonetic transcription*) merupakan aplikasi akses jarak jauh (*remote access*) yang memanfaatkan protokol jaringan untuk membuat permintaan (*remote*) ke komputer server jarak jauh. Akses jarak jauh (*remote access*) ini menggunakan protokol jaringan dan digunakan untuk mengakses server dan jaringan melalui protokol SSH, Telnet, dan Rlogin. Hal ini memungkinkan pengguna untuk mengontrol server jarak jauh, memecahkan masalah jaringan, dan melakukan administrasi sistem jarak jauh. Oleh karena itu, PuTTY biasanya banyak digunakan oleh pemilik server untuk mengkonfigurasi server yang berjauhan satu sama lain dan memerlukan dukungan akses jarak jauh.



Gambar 5. 3 Tampilan Putty

5.2 Pengujian

Pengujian merupakan proses menjalankan sistem untuk melihat kerusakan atau kesalahan ketika sistem yang sudah di implementasikan pada Kantor Dinas Kesehatan Kabupaten Tanah Datar bisa berjalan dengan tujuannya. Pengujian dilakukan untuk memastikan metode *port knocking* dan *port blocking* berfungsi sesuai dengan rancangan yang dikonsepkan oleh penulis, sehingga dengan penerapan metode ini dapat mengamankan jaringan pada Kantor Dinas Kesehatan Kabupaten Tanah Datar.

5.2.1 Setting Metode *Port Knocking*

Konfigurasi metode *Port Knocking* bertujuan untuk mengelola *port* pada komputer admin agar *port* pada masing-masing komputer tersebut hanya administrator yang bisa mengakses komputer admin.

Tabel 5. 1 *Port* yang akan di *Knocking*

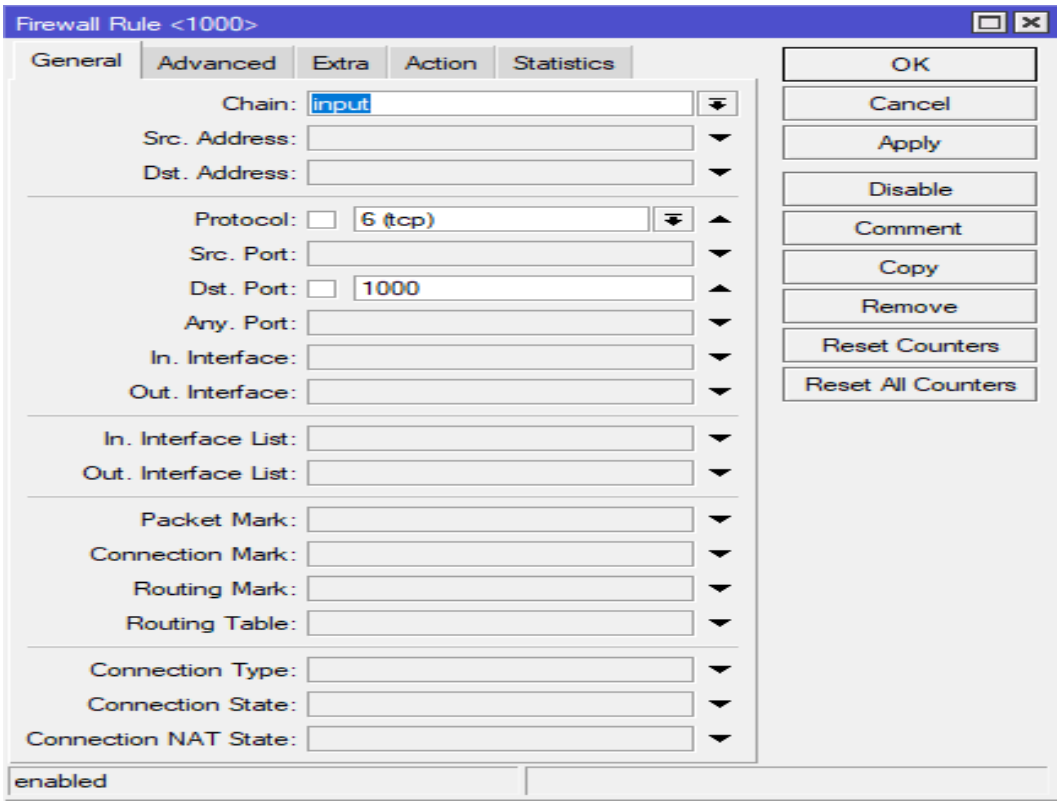
Port	IP Target	Keterangan
22	172.18.1.1	SSH
23	172.18.1.1	Telnet
80	172.18.1.1	HTTP
8291	172.18.1.1	Winbox

Berdasarkan tabel diatas maka peneliti ingin meng-*knocking port* SSH (22), Telnet (23), HTTP (80), dan Winbox (8291) pada router mikrotik Kantor Dinas Kesehatan Kabupaten Tanah Datar.

5.2.1.1 Setting *Port Knocking* 1000

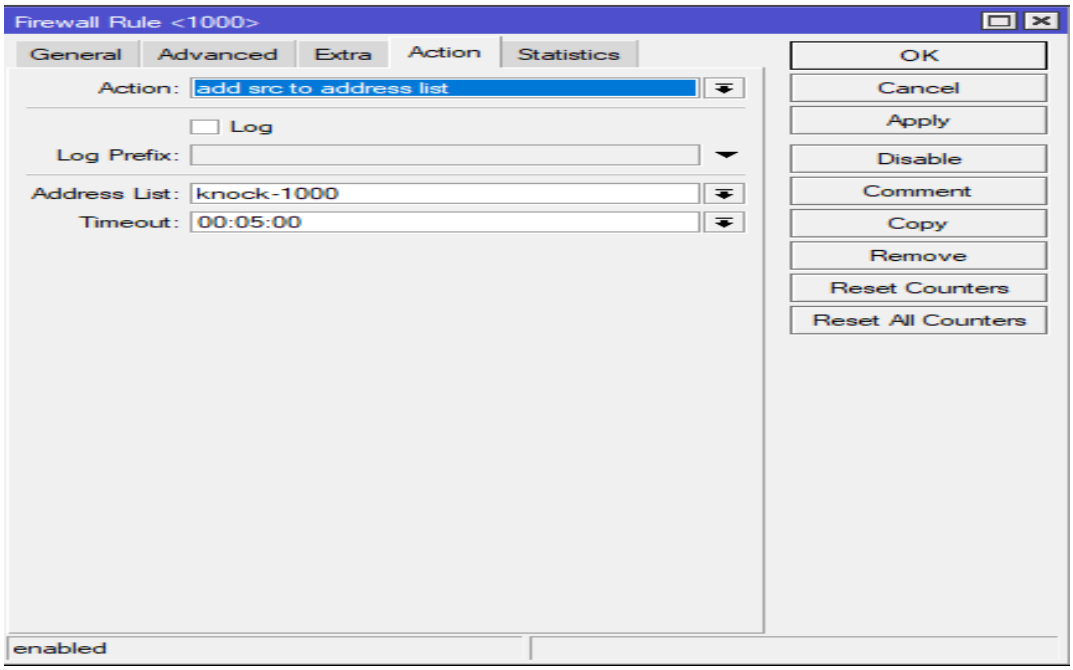
Peneliti akan mengkonfigurasi *port knocking* 1000 dengan cara pertama masuk ke menu IP, lalu pada menu IP pilih *FIREWALL* dan pilih *filter rules*, selanjutnya peneliti memilih simbol tambah berwarna biru pojok kiri atas untuk membuat rules-rules yang akan digunakan dalam mengkonfigurasi *knock* 1000.

Peneliti membuat *knock* 1000 dengan memilih tab GENERAL kemudian pada kolom *chain* diisi *input*, pada kolom protokol diisi tcp dan pada kolom dst.port diisi dengan 1000 seperti gambar 5.4 dibawah.



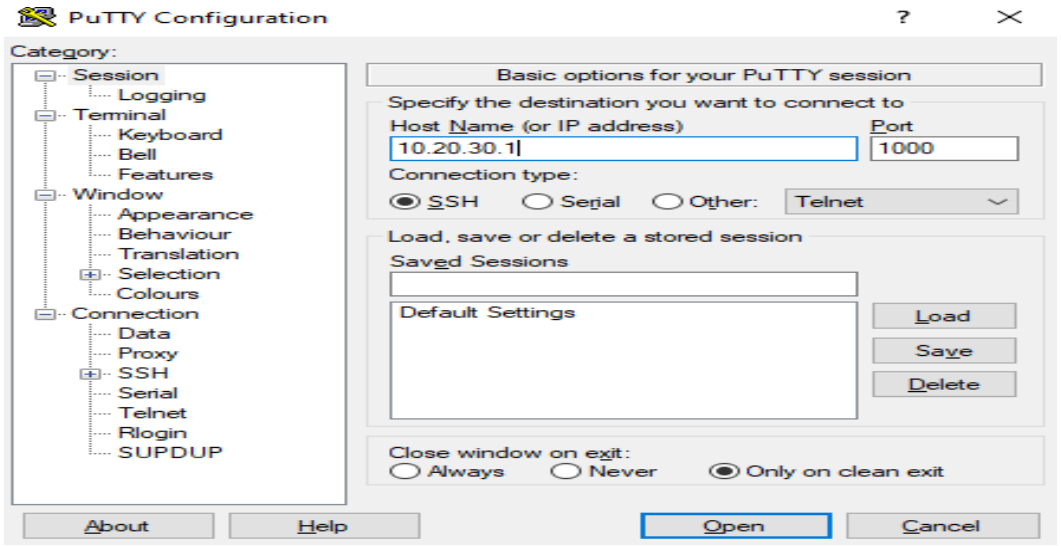
Gambar 5. 4 Konfigurasi *filter rules knock*-1000 tab general

Setelah pada tab GENERAL selesai, pindah ke tab action, dengan mengubah kolom action menjadi add src to address list, pada kolom address list diisi dengan knock-1000 dan berikan *timeout* 5 menit untuk menghindari penumpukan IP pada *address list* seperti gambar 5.5 berikut.

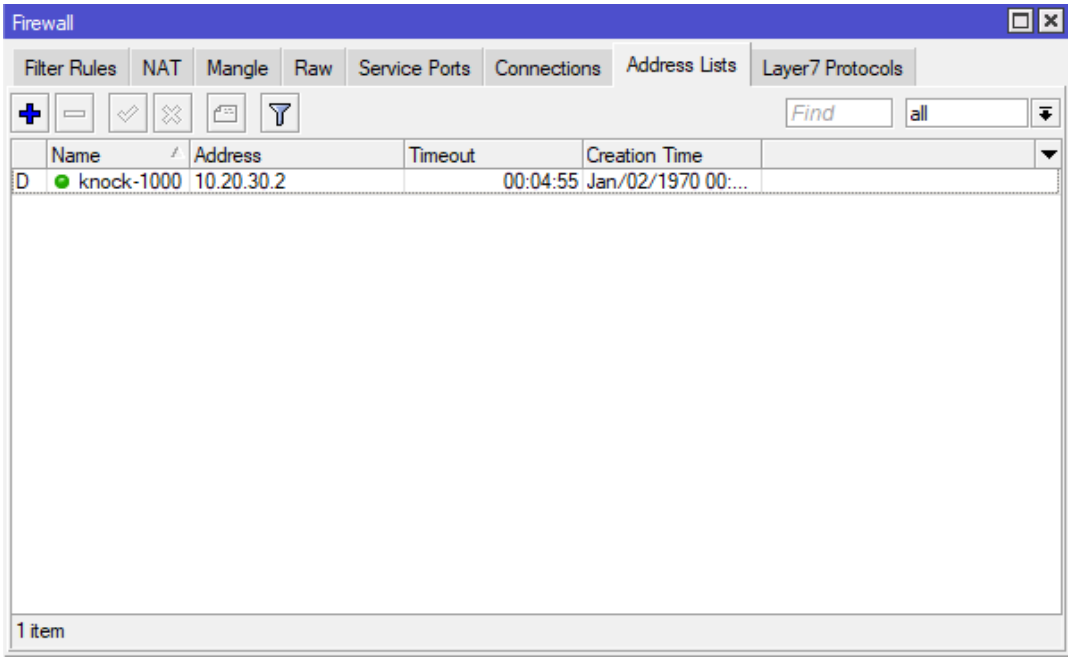


Gambar 5. 5 Konfigurasi *filter rules knock*-1000 tab action

Peneliti mencoba apakah konfigurasi *knock*-1000 berhasil dijalankan atau tidak, berjalan atau tidaknya *knock*-1000 dibantu dengan menggunakan applikasi putty. Pada aplikasi putty yaitu masukkan ip *ether*1 mikortik dengan tujuan port 1000, kemudian klik *open*. Selanjutnya tampilan dapat dilihat pada gambar 5.6 dan 5.7 berikut.



Gambar 5. 6 Testing *IP Address* di *Port* 1000

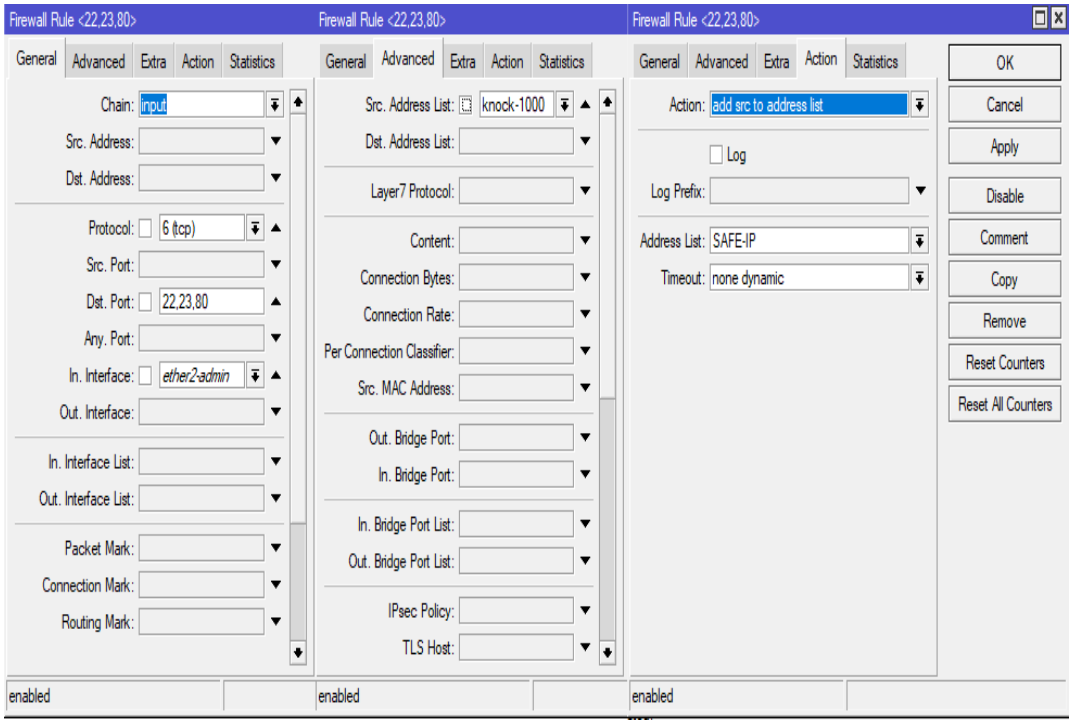


Gambar 5. 7 Hasil konfigurasi *Knock*-1000

Pada gambar 5.7 memperlihatkan *knock*-1000 sudah berhasil dan masuk ke dalam *address list* menu *firewall*. Selanjutnya peneliti membuat sebuah *rules* yang bernama SAFE IP, *rules* safe ip digunakan untuk ip yang meng-*knocking* terleih dahulu *knock*-1000 maka akan dapat mengakses mikrotik *port* yang ingin ditujunya tanpa adanya *timeout*.

5.2.1.2 Setting *Port Knocking* SAFE IP

Untuk konfigurasi *rules* SAFE IP yaitu pilih kembali simbol tambah berwarna biru pojok kiri atas, lalu pada tab general status chain ubah menjadi input, pilih protokol dengan tcp, di dst.port pilih *port* yang ingin diamankan, peneliti memilih *port* SSH (22), *port* Telnet (23) dan *port* HTTP (80) untuk diamankan, di tab advanced pada kolom src.address list pilih *knock*-1000, di tab *action* ubah kolom *action* menjadi add src to address list, pada kolom *address* buat menjadi SAFE IP.



Gambar 5. 8 Konfigurasi *Rules* SAFE IP

5.2.1.3 Setting *Port Knocking* PENYUSUP

Setelah membuat rules SAFE IP, selanjutnya peneliti membuat *rules* baru dengan nama PENYUSUP, *rules* penyusup digunakan untuk ip yang tidak meng-*knocking* terlebih dahulu *knock*-1000 maka bisa mengakses mikrotik *port* hanya dengan batasan waktu tertentu dan jika *timeout* sudah lewat, makai ip itu akan secara otomatis keluar sendiri. Ini membuat data-data yang ada dalam mikrotik menjadi aman.

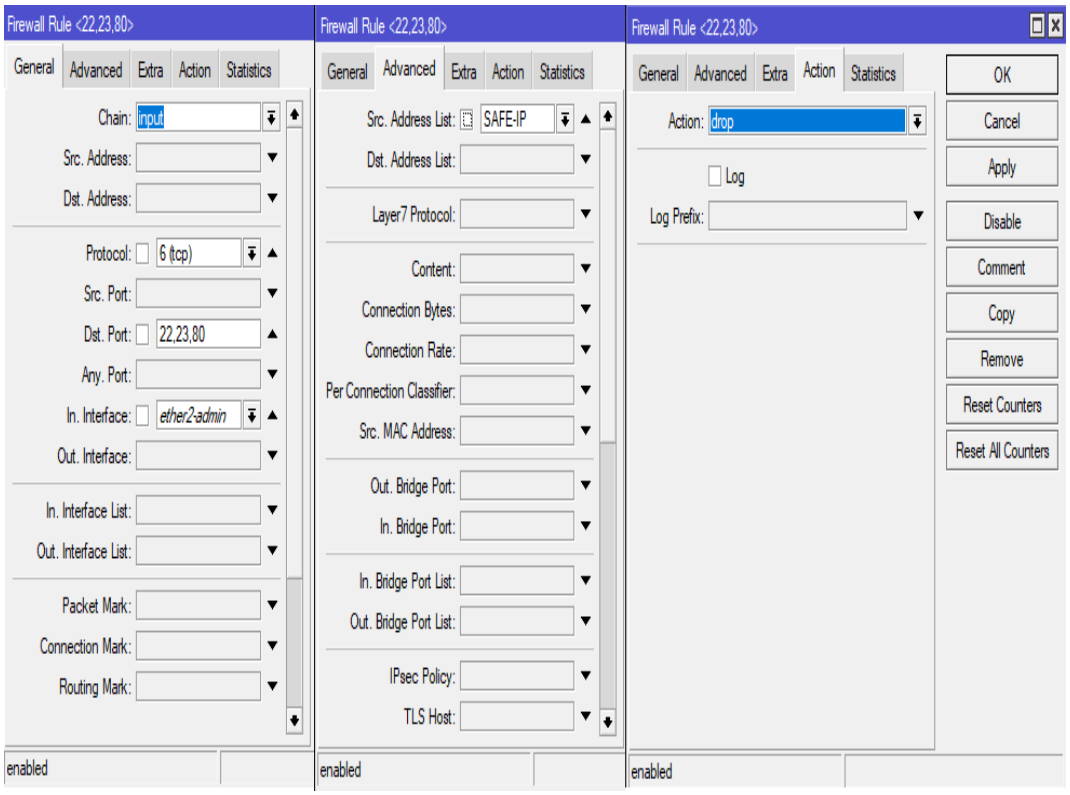
Untuk konfigurasi *rules* PENYUSUP yaitu pilih kembali simbol tambah berwarna biru pojok kiri atas, lalu pada tab general status chain ubah menjadi input, pilih protokol dengan tcp, di dst.port pilih *port* SSH (22), *port* telnet (23) dan HTTP (80) untuk diamankan, di tab advanced pada kolom src.address list pilih *knock*-1000 lalu klik simbol yang menunjukan tanda (!) artinya ini bukan yang melakukan

knock-1000, di tab *action* ubah kolom *action* menjadi add src to address list, pada kolom *address list* buat menjadi penyusup dan berikan *timeout* 10 menit.

5.2.1.4 Setting *Port Knocking* DROP IP

Setelah membuat *rules* PENYUSUP, selanjutnya peneliti membuat *rules* terakhir sebagai DROP IP, kegunaan dari drop ip yaitu data yang berasal dari *client* akan dibuang (*drop*) oleh router.

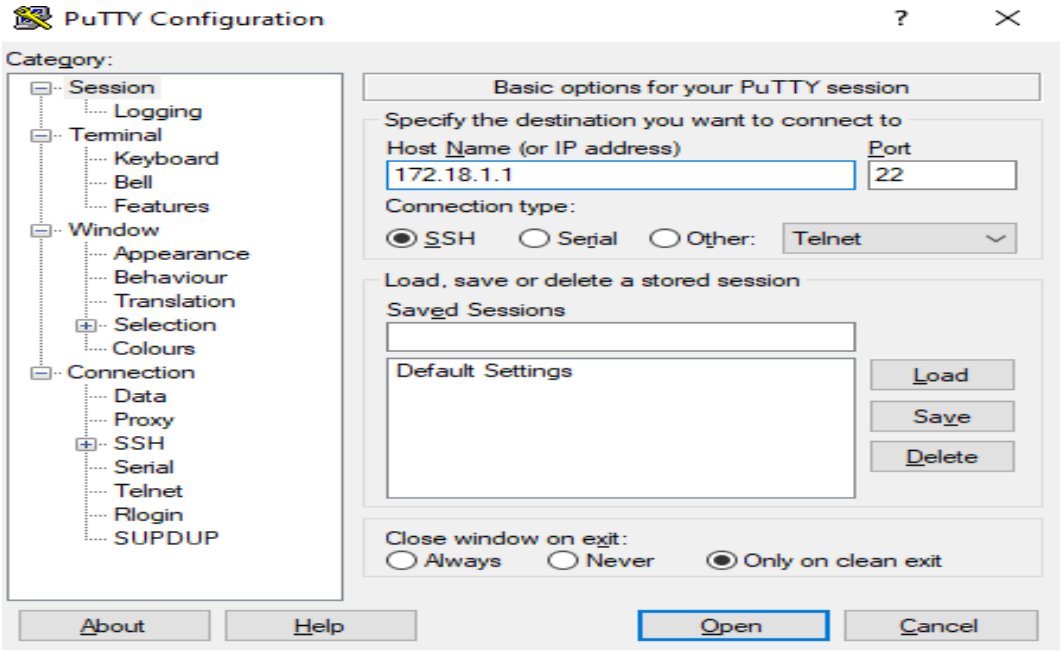
Untuk konfigurasi *rules* DROP IP, yaitu pilih kembali simbol tambah berwarna biru pojok kiri atas, lalu pada tab general status chain ubah menjadi input, pilih protokol dengan tcp, di dst.port pilih *port* SSH (22), telnet (23) dan HTTP (80) untuk diamankan, di tab *action* ubah kolom *action* menjadi drop, sehingga siapapun yang masuk tanpa masuk terlebih dahulu di *knock*-1000 atau tidak terdaftar didalam SAFE IP makan akan di DROP atau di BLOK.



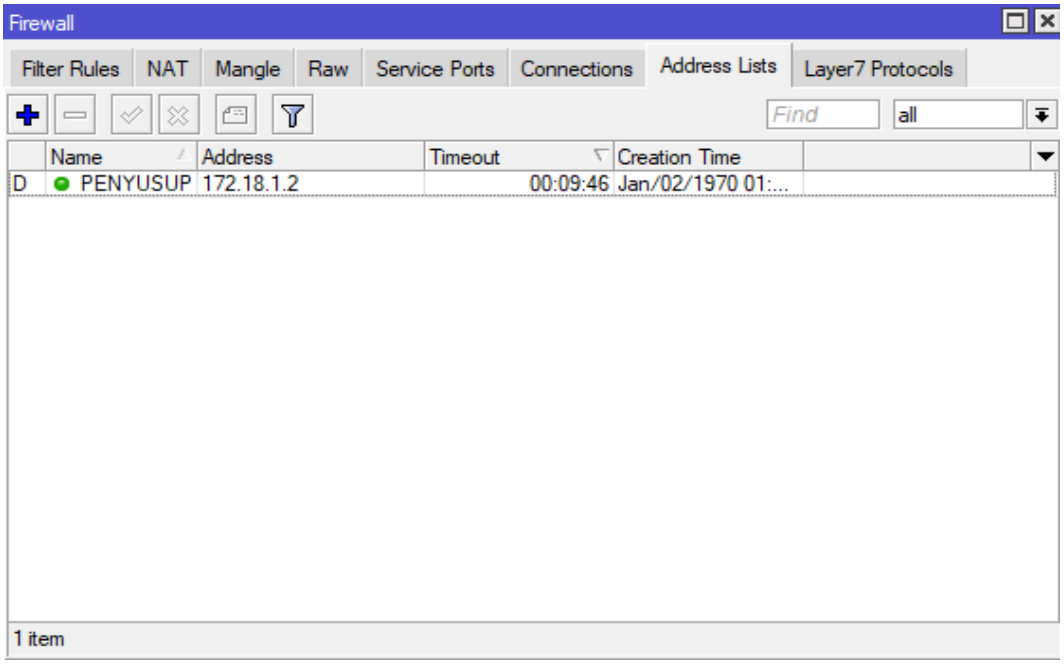
Gambar 5. 9 Konfigurasi *Rules* DROP IP

5.2.2 Pengujian Metode *Port Knocking*

Untuk mengetahui konfigurasi berhasil atau tidaknya peneliti mencoba menggunakan aplikasi putty pada komputer admin untuk membantu dalam mencoba hasil konfigurasi seperti pada gambar 5.10 dan 5.11 berikut :

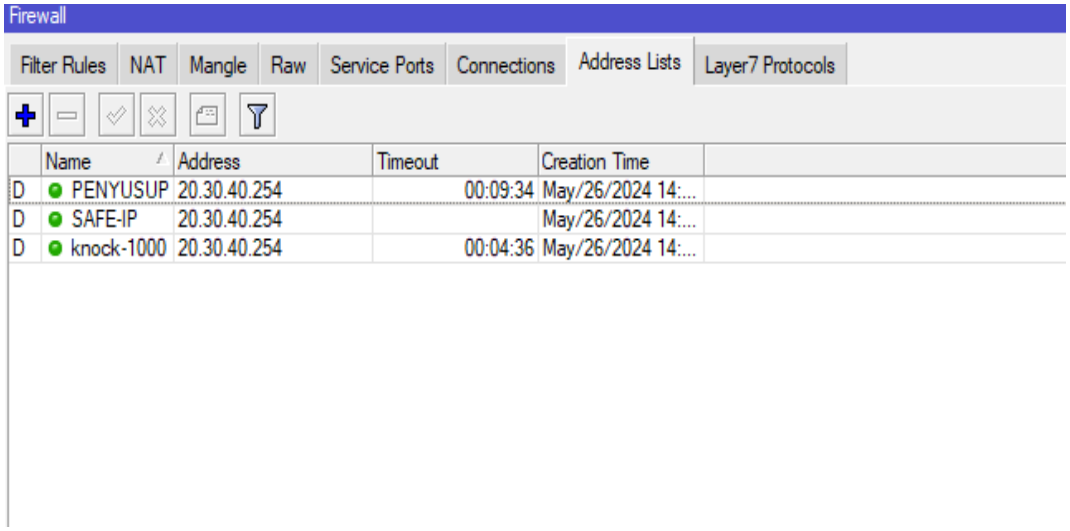


Gambar 5. 10 Percobaan dengan aplikasi puTTY



Gambar 5. 11 Percobaan Penyusup Masuk Langsung Ditolak

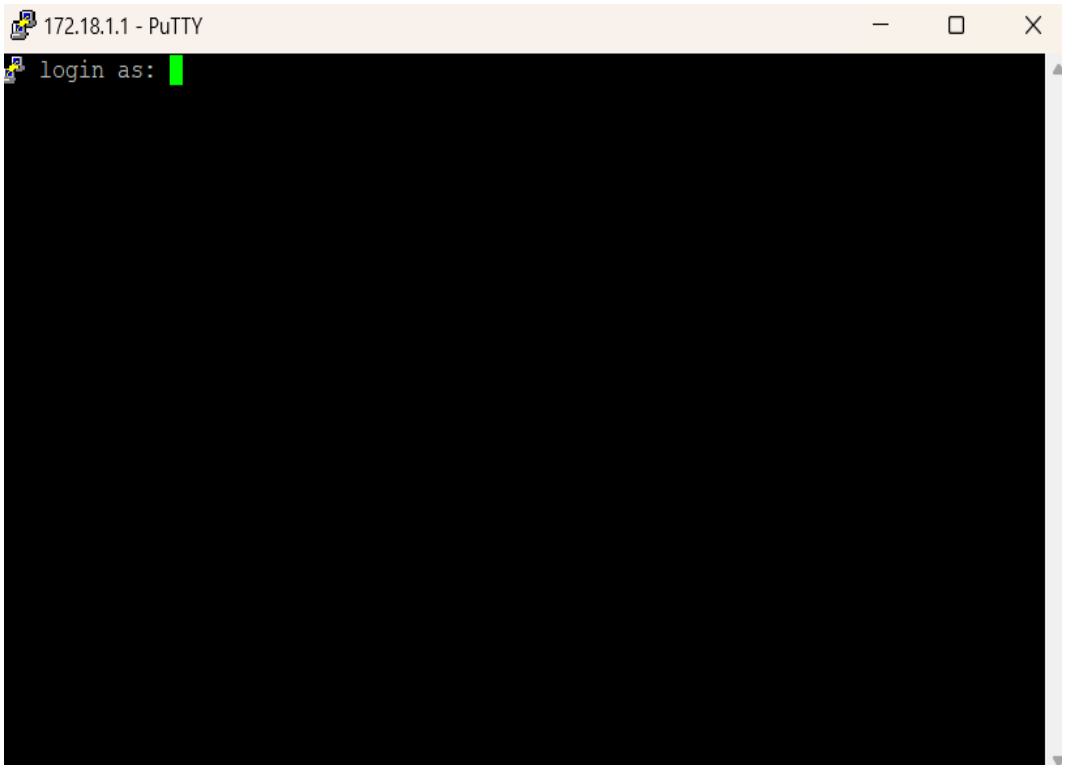
Pada gambar 5.11 peneliti mencoba untuk masuk kedalam mikrotik dengan menggunakan *port* 22 menggunakan alamat ip dari *ether*2 mikrotik tanpa masuk terlebih dahulu ke *port* 1000, juga dapat dilihat bahwa tanpa masuk terlebih dahulu ke *port* 1000 maka mikrotik akan mendrop hak akses dari *user* tersebut menjadi penyusup.



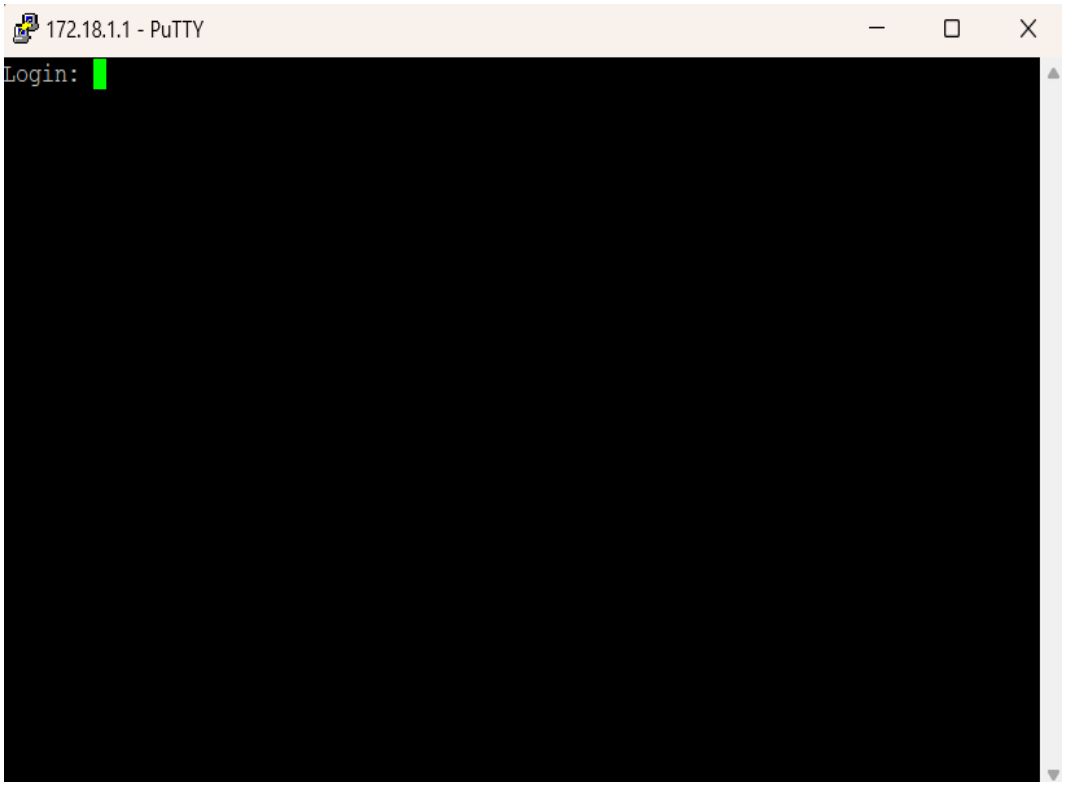
Gambar 5. 12 Pengujian Konfigurasi *Port Knocking*

Dalam memonitoring peneliti mengetahui tingkat keberhasilan dan kesalahan dari jaringan yang dibangun. Pada gambar 5.12 menunjukan bahwa pengujian dari berbagai konfigurasi *port knocking* menggunakan mikrotik, dan semua konfigurasi dari *knock* 1000.

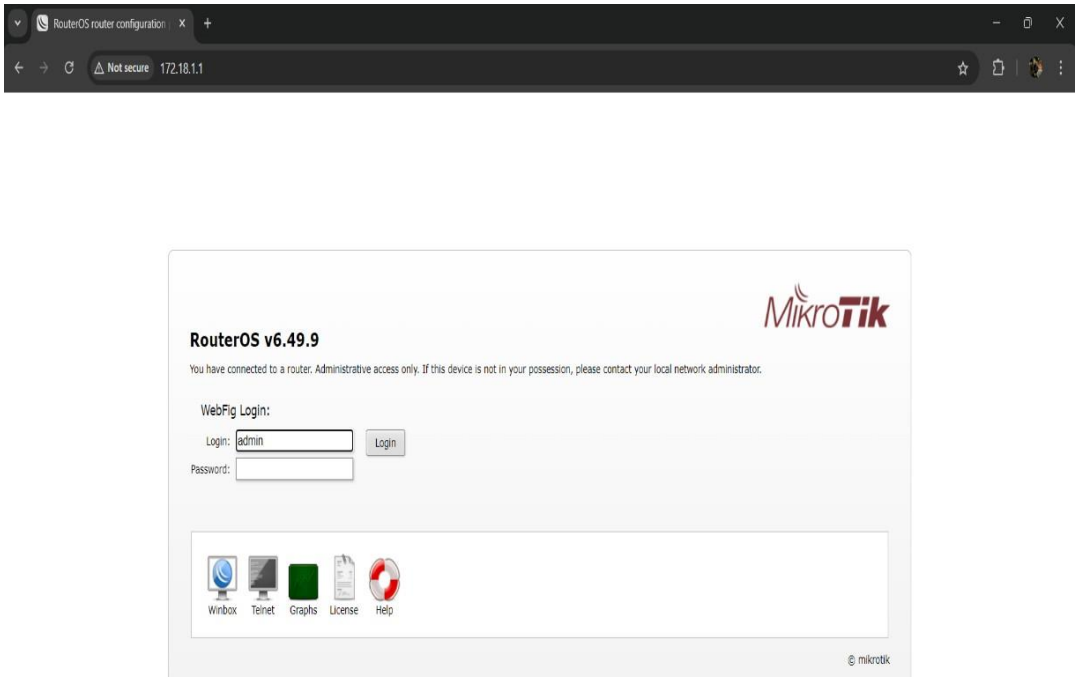
Pada pengujian *port* 22 (SSH), *port* 23 (telnet) dan *port* 80 (HTTP), peneliti menggunakan cara meng-*knocking* terlebih dahulu *port* 1000 melalui putty, maka jalan yang dilakukan oleh komputer admin ke mikrotik mendapatkan hak akses untuk *login* ke *port* 22, *port* 23 dan *port* 80 seperti gambar 5.13, 5.14 dan gambar 5.15 berikut :



Gambar 5. 13 Akses *Login Port* 22 (SSH) Diizinkan

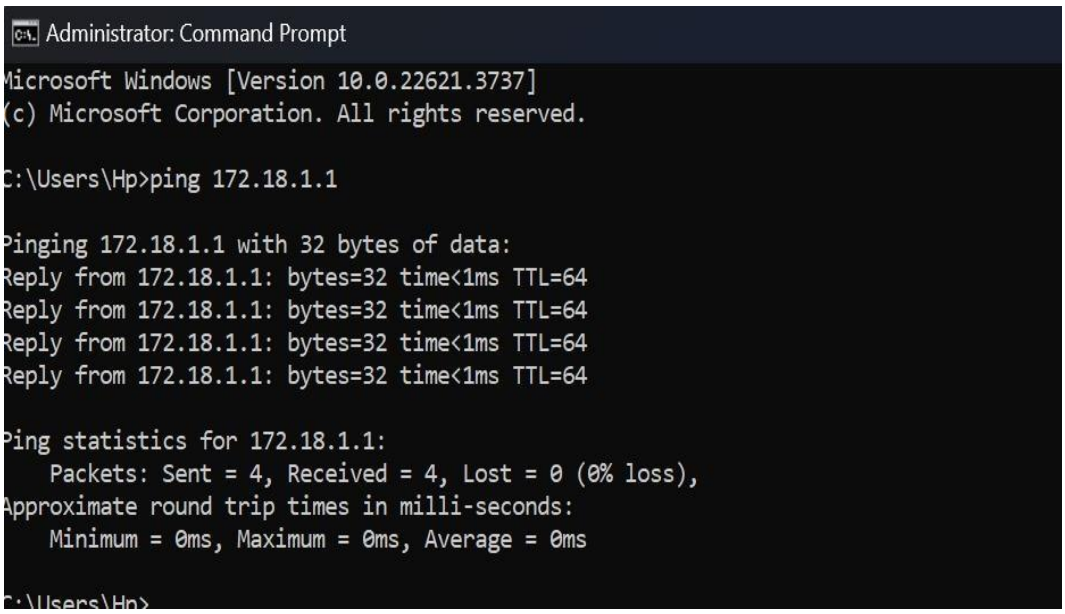


Gambar 5. 14 Akses *Login Port* 23 (Telnet) Diizinkan



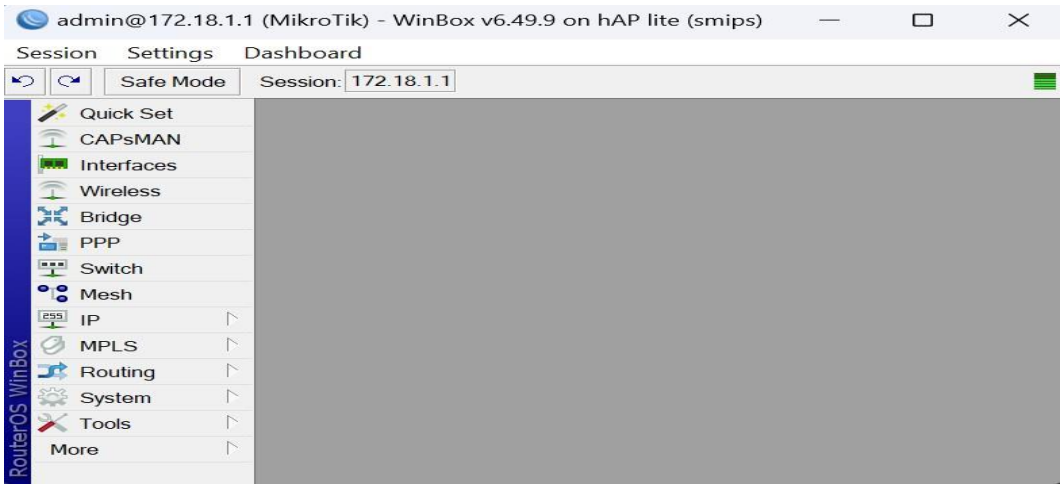
Gambar 5. 15 Akses *Login Port* 80 (HTTP) Diizinkan

Selanjutnya untuk pengujian *port knocking* pada port 8291 (winbox) dilakukan dengan cara ICMP terlebih dahulu pada *command Promt*, dengan perintah ping alamat *ether2* dari komputer Admin, ini berfungsi sebagai tanda pengenal pengakses berasal yang mencoba *login* pada *ip address* yang dipilih.



Gambar 5. 16 Tampilan ICMP Command Promt

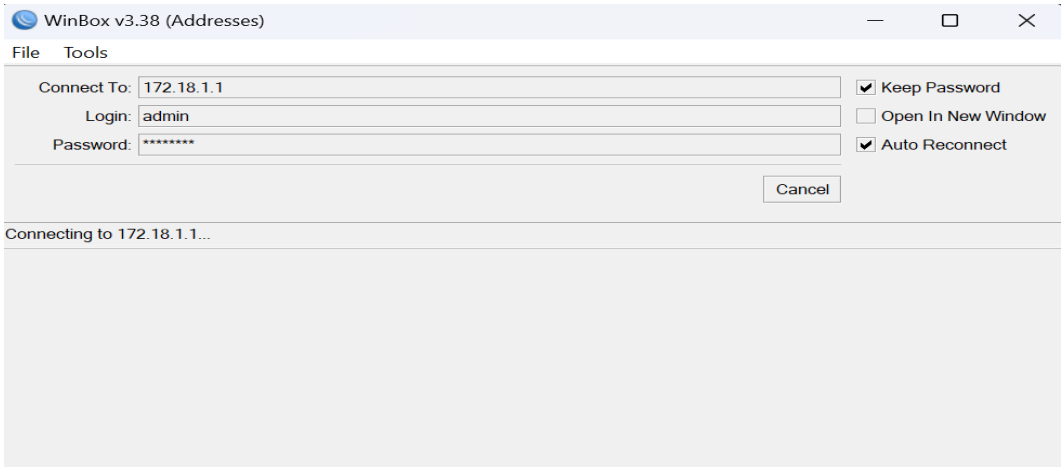
Penerapan dalam gambar 5.16 melakukan ICMP pada ip *ether2* yaitu 172.18.1.1, dan memunculkan *reply* untuk mendapatkan akses *login* pada ip 172.18.1.1.



Gambar 5. 17 Tampilan Akses *Login* Winbox

Pada gambar 5.17, proses login diizinkan setelah melakukan ICMP pada *command promt*, sehingga *user* yang *login* melalui komputer Admin bisa mengakses winbox untuk melakukan konfigurasi jaringan.

Apabila komputer Admin tidak melakukan ICMP sebelum *login*, maka akses untuk masuk kedalam winbox akan ditolak, seperti gambar 5.18 tidak bisa melakukan konfigurasi jaringan dan memunculkan pesan tidak bisa terhubung.



Gambar 5. 18 Tampilan Akses *Login* Ditolak Winbox

5.2.3 Setting Metode *Port Blocking*

Dalam pengujian awal pada simulasi ini belum diterapkannya rancangan usulan yang diberikan kepada Kantor Dinas Kesehatan Kabupaten Tanah Datar yaitu sebelum adanya penambahan keamanan jaringan *metode port knocking* dan *port blocking*. Konfigurasi metode *Port Blocking* bertujuan untuk mengelola *port* pada komputer target (*client*) agar *port* pada masing-masing komputer tersebut tidak bisa dibuka atau diakses oleh komputer target (*client*).

Tabel 5. 2 *Port* yang akan di *Blocking*

Port	IP Target	Keterangan	Sebelum di blocking
22	192.168.10.1	SSH	Terbuka
80	192.168.10.1	HTTP	Terbuka
8291	192.168.10.1	Winbox	Terbuka

Pada tabel 5.2 dijelaskan bahwa pada metode *port blocking* yang akan peneliti blok adalah *port* 22 (SSH), *port* 80 (HTTP) dan *port* 8291 (Winbox).

5.2.4 Pengujian Metode *Port Blocking*

Untuk mengetahui pengujian berhasil atau tidaknya, peneliti mencoba menjalankan semua *port* sebelum di *blocking* pada komputer *client* dan hasilnya dapat dilihat pada gambar 5.19, 5.20, dan gambar 5.21 berikut :

Gambar 5. 19 Pengujian awal *port* 22 sebelum diblok

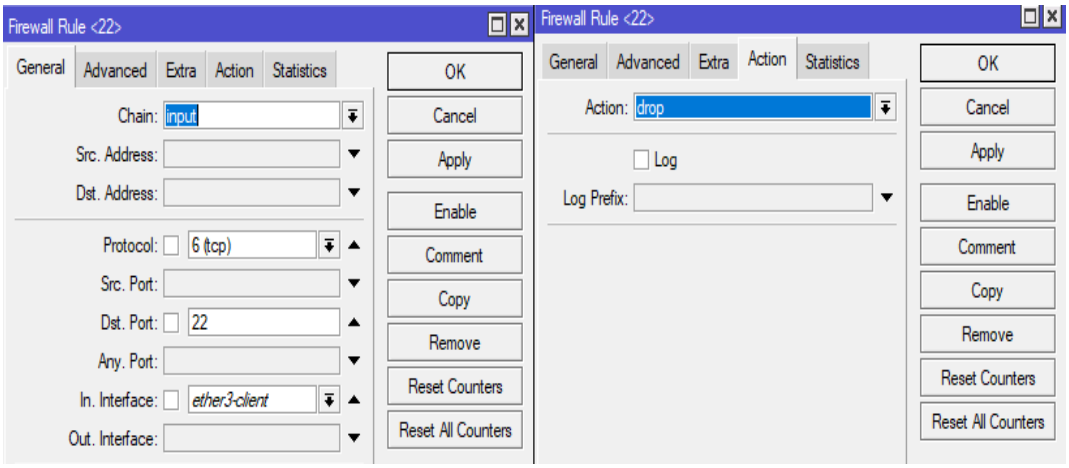
Gambar 5. 20 Pengujian awal *port* 80 sebelum diblok

Gambar 5. 21 Pengujian awal *port* 8291 sebelum diblok

Hasilnya memperlihatkan kondisi *port* yang masih terbuka pada komputer *client* sebelum diterapkannya metode *port blocking* dan semua *port* masih bisa diakses secara bebas oleh komputer *clinet*.

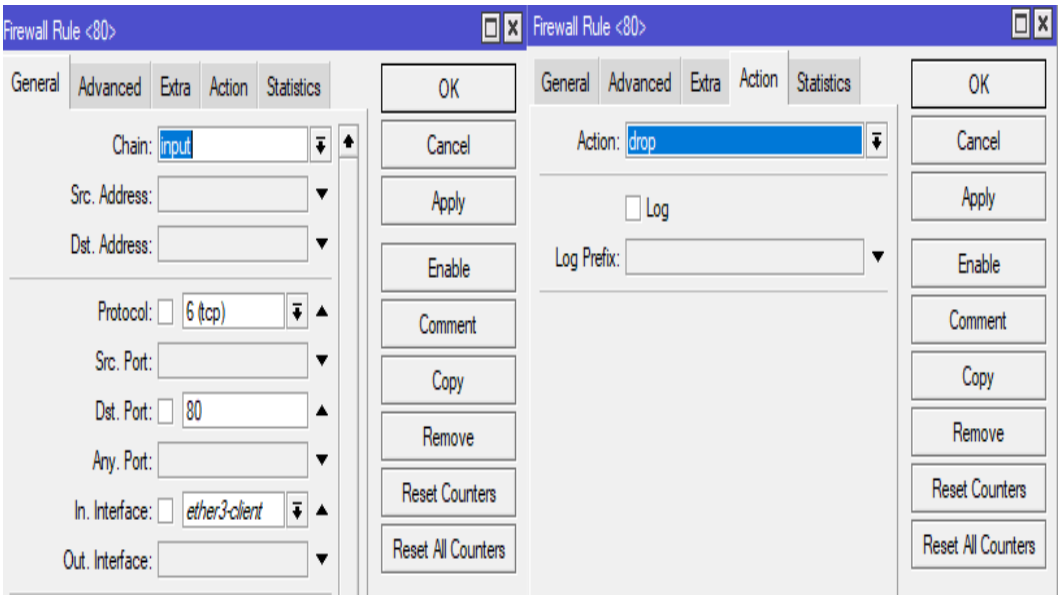
Oleh karena itu, peneliti melakukan metode *port blocking* dan menerapkan keamanan jaringan ini yang mana langkah awal peneliti adalah membuat *rules* baru

untuk mengamankan *port* 22 (SSH) dengan cara chain “input”, protocol “tcp”, mengisikan dst.port nya *port* 22 (SSH) untuk tujuan komputer *client*, dan pada tab *action* menu *action*, diisikan “drop” seperti gambar 5.22 berikut :



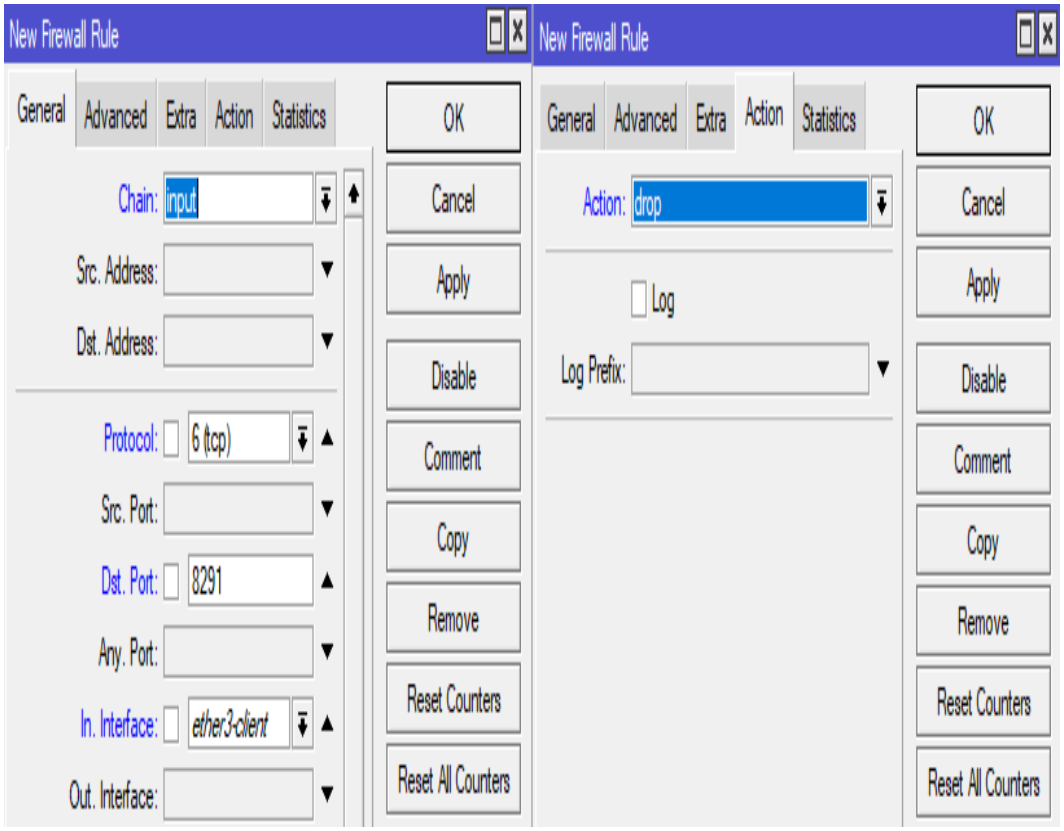
Gambar 5. 22 *Filter Rules Port Blocking Port* 22 (SSH)

Lalu seterusnya peneliti melakukan *port blocking* untuk *port* 80 (HTTP) dengan cara yang sama dan tujuan yang sama untuk memblok komputer *client* seperti memblok *port* 22 (SSH), tapi yang berbeda adalah pada dst.port nya diisikan dengan *port* 80 (HTTP) seperti gambar 5.23 berikut :



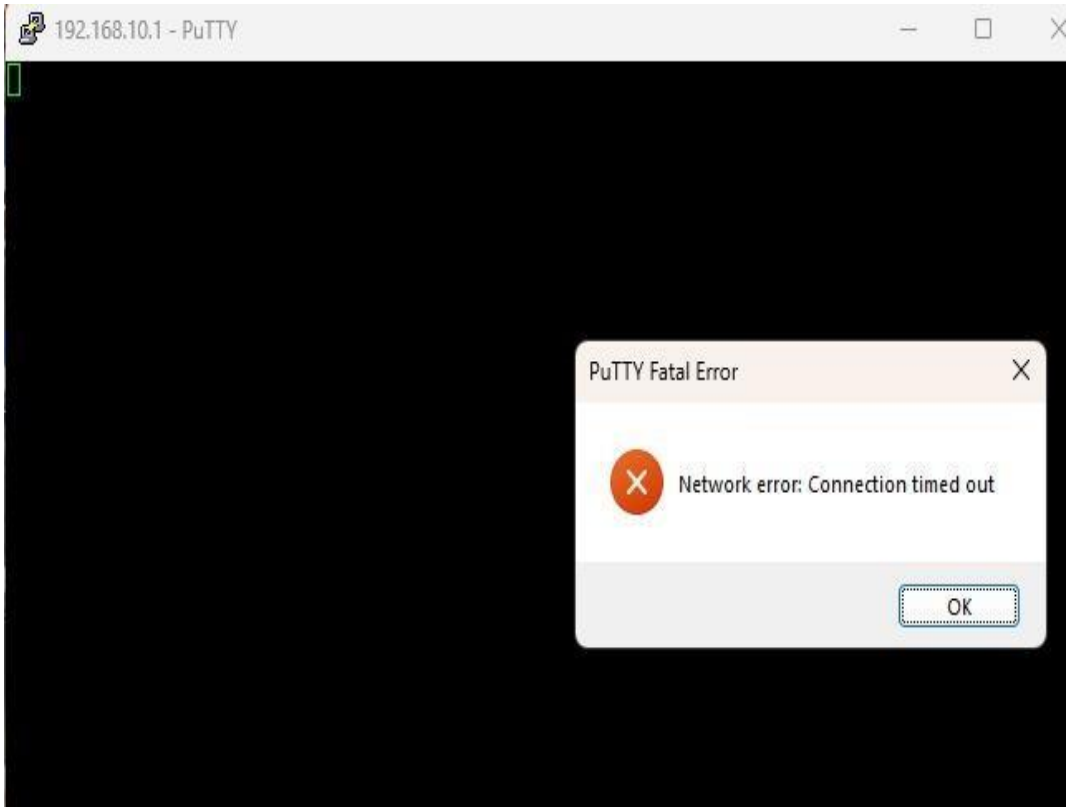
Gambar 5. 23 *Filter Rules Port Blocking Port* 80 (HTTP)

Terakhir peneliti melakukan *port blocking* untuk port 8291 (Winbox) dengan cara yang sama dan tujuan yang sama untuk memblok komputer *client* seperti memblok *port* 22 (SSH) dan *port* 80 (HTTP), tapi yang berbeda adalah pada dst.port diisikan dengan *port* 8291 (Winbox) seperti gambar 5.24 berikut :

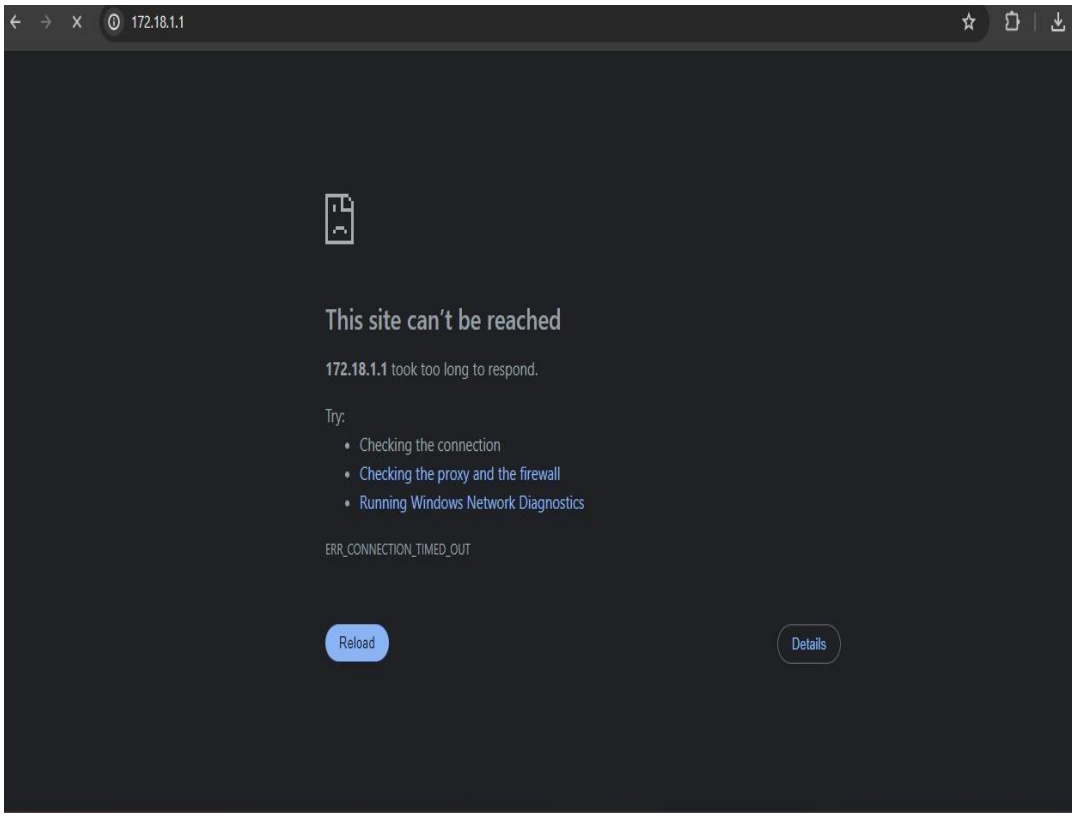


Gambar 5. 24 *Filter Rules Port Blocking Port* 8291 (Winbox)

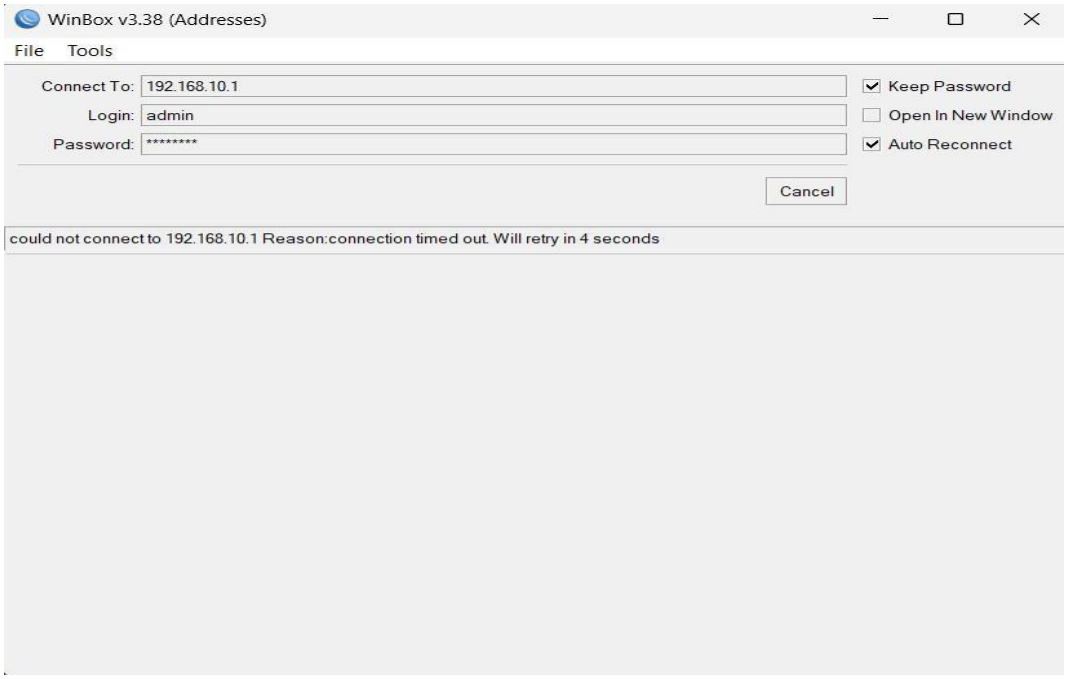
Setelah dilakukannya pembuatan *rules* untuk *port blocking*, gambar 5.25 berikut memperlihatkan hasil dimana kondisi *port* 22 (SSH) pada pengujian komputer *client* tidak dapat masuk atau diblok, gambar 5.26 menunjukan kondisi *port* 80 (HTTP) pada pengujian komputer *client* tidak bisa di akses, dan pada gambar 5.27 menampilkan *port* 8291 (Winbox) pada komputer *client* tidak bisa *login* kedalam menu winbox mikrotik.



Gambar 5. 25 Pengujian *port* 22 (SSH) setelah diblok



Gambar 5. 26 Pengujian *port* 80 (HTTP) setelah diblok



Gambar 5. 27 Pengujian *port* 8291 (Winbox) setelah diblok

Tabel 5. 3 Hasil Pengujian Metode *Port Blocking*

Port	IP Target	Keterangan	Sebelum diblok	Sesudah diblok
22	192.168.10.1	SSH	Terbuka	Tertutup
80	192.168.10.1	HTTP	Terbuka	Tertutup
8291	192.168.10.1	Winbox	Terbuka	Tertutup

Hasil setelah diterapkan dan digunakannya metode *port blocking* adalah komputer *client* tidak dapat memasuki atau mengakses *port* yang terbuka sebelumnya, seperti pada *port* yang sudah di *blocking* agar tingkat keamanan lebih efisien dalam mengamankan data dan jaringan.

BAB VI

PENUTUP

6.1 Kesimpulan

Bab ini menyajikan beberapa kesimpulan dari uraian masalah dan pembahasan yang dilakukan di bab-bab sebelumnya. Tujuan dari kesimpulan ini adalah untuk memberikan solusi dan jawaban atas masalah yang sedang dibahas. Berikut adalah kesimpulan yang dicapai :

1. Penerapan metode *port knocking* akan membantu pengendalian orang-orang yang terhubung ke jaringan Kantor Dinas Kesehatan Kabupaten Tanah Datar dan tindakan pengendalian yang dilakukan akan memungkinkan deteksi serta pemantauan orang-orang yang terhubung ke jaringan.
2. Metode *port blocking* mencegah serangan dari luar dan menjaga integritas dan kerahasiaan data kesehatan yang sensitif. Ini karena metode ini membatasi akses ke beberapa port tertentu.

6.2 Saran

Sistem keamanan jaringan yang di rancang dengan batasan yang di tentukan, mungkin masih banyak kekurangan dan perlu banyak perkembangan, adapun beberapa saran untuk menjadikan sistem menjadi lebih baik sebagai berikut:

1. Untuk mengurangi jumlah *port* yang terbuka untuk akses ilegal, penelitian selanjutnya diharapkan akan menerapkannya pada *port* lain.
2. Metode keamanan *port knocking* dan *port blocking* memerlukan pengujian tambahan. Misalnya, pengujian simulasi serangan *port* harus dilakukan.

Meskipun sistem sudah dirancang dengan baik, masih diperlukan pengembangan sistem yang lebih baik untuk memberikan keamanan yang lebih terjamin.