BAB II
TINJAUAN PUSTAKA

2.1 Landasan Terori

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (*printer*, *CPU*, Dll), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Jaringan komunikasi data yang terintegrasi saat ini sudah menjadi kebutuhan utama bagi sebuah institusi atau perusahaan bisnis, terutama perusahaan yang mempunyai banyak kantor cabang di lokasi geografis yang berbeda dan juga untuk perusahaan yang kegiatan perkantorannya menurut seorang karyawan tidak hanya behind the desk saja (Sidik et al., 2021).

Begitu juga dengan keamanan jaringan atau sistem informasi terdiri dari seperangkat kebijakan dan pelaksanaan yang diterapkan untuk mencegah dan memantau akses tidak sah, modifikasi dalam sistem, penyalahgunaan, atau penolakan jaringan komputer dan sumber daya yang dapat diakses jaringan. Implementasi teknologi keamanan sebagai tindakan perlindungan menjadi pilihan dalam upaya melindungi aset informasi dari ancaman atau serangan teknologi keamanan hadir sebagai perlindungan keamanan atas ancaman atau serangan pada jaringan atau sistem informasi antara lain *firewall, cryptographic system, IDS, SSL, antivirus system, IPSec, authentication* dan lain sebagainya (Lesmana et al., 2024).

2.1.1 Jenis-jenis Jaringan Komputer

1. Berdasarkan Jangkauan Jaringan

Komputer yang saling terhubung ini pun harus mempunyai setidaknya satu kartu jaringan masing-masing yang kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data dan terdapat perangkat lunak sistem operasi jaringan yang akan membentuk sebuah jaringan komputer sederhana. Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya maka diperlukan peralatan tambahan untuk mendukung seperti *Hub, Switch, Router*, dll. (Suhendi &

Gusdevi, 2023). Ada beberapa jenis jaringan komputer yang sering kita lihat dan di klasifikasikan menurut cangkupan areanya yaitu:

A. LAN (Local Area Network)

   LAN atau *Local Area Network* adalah konsep yang menghubungkan perangkat jaringan dalam jarak yang relatif pendek. Biasanya digunakan untuk gedung sekolah, kantor, rumah, dll. Konsep jaringan LAN ini cenderung menggunakan *konektivitas* tertentu, terutama *Ethernet* dan Token Ring. Dan ada juga LAN yang menggunakan gelombang elektromagnetik airwaves untuk melakukan pertukaran data atau informasi yang dibutuhkan yang menggunakan teknologi jaringan *Wireless* atau nirkabel dengan WI- FI disebut dengan *Wireless Local Area Network* (WLAN) (Nurdadyansyah & Hasibuan, 2021).

B. MAN (Metropolitan Area Network)

   MAN *(Metropolitan Area Network)* adalah suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN juga dapat disebut sebagai gabungan dari beberapa LAN (Rismawati & Mulya, 2020). MAN merupakan suatu jaringan komputer gabungan beberapa LAN atau gabungan beberapa gedung yang terletak pada suatu kota contohnya saja jaringan internet antar Gedung pada Kantor Pemerintahan, dan di Kampus antar Gedung-gedung Fakultas. Di bawah ini merupakan gambar dari rangkaian jaringan MAN *(Metropolitan Area Network)*.

C. WAN (Wide area network)

   WAN atau *Wide Area Network* adalah konsep yang menghubungkan perangkat jaringan komputer yang mencangkup wilayah super luas dan menggunalan peralatan yang super canggih. *Wide Area Network* (WAN) adalah jaringan *computer* dengan jangkauan area *geografi* yang paling luas, antar negara, antar benua bahkan keluar angkasa (sebagai contoh jaringan internet yang menggunakan sistem koneksi satelit (Suhendi & Gusdevi, 2023).

2. Berdasarkan Fungsi Jaringan

Berdasarkan fungsi jaringan ,ada dua bagian besar yaitu: jaringan *Client-Servers* dan *Peer To Peer* (N. A. Putra et al., 2021).

a. Jaringan Client-Server

Jaringan yang terdiri dari client, yaitu mikro komputer yang meminta data dan *server*, yaitu komputer yang menyuplai data.

b. Peer To Peer

Pada jaringan ini, semua *mikrokomputer* dalam sebuah jaringan berkomunikasi secara langsung satu sama lain tanpa harus bersandar pada *server*. Komputer bisa berbagi *file* dan *peripheral* dengan seluruh komputer lainnya pada jaringan, jika semua komputer tersebut diberi hak akses.

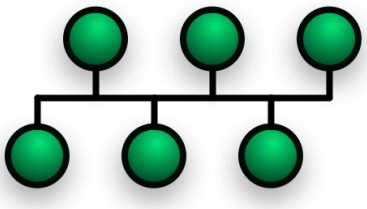
2.1.2 Topologi Jaringan

Topologi jaringan merupakan bagaimana sebuah komputer dan perangkat teknologi lainnya saling terhubung. Konsep dasar topologi jaringan *point to point*, kemudian berkembang menjadi *multi point* dimana nama topologi didasarkan pada bentuk jaringan yang terhubung.

Topologi jaringan merupakan elemen fundamental dalam perancangan sistem komunikasi data. Struktur fisik dan logis dari jaringan, seperti topologi bus, ring, star, mesh, dan hybrid, memiliki pengaruh signifikan terhadap kinerja jaringan, khususnya dalam hal kecepatan transmisi data dan efisiensi penggunaan sumber daya (Engineering, 2024).

1. Topologi Bus

Topologi bus merupakan topologi yang digunakan pertama kali, topologi bus atau juga disebut dengan linier bus yaitu topologi yang menghubungkan komputer dengan komputer yang lain dengan satu kabel (linier).



Gambar 2. 1 Topologi Bus

(Sumber: https://id.wikipedia.org/wiki/Topologi_bus)

Kelebihan Topologi Bus:

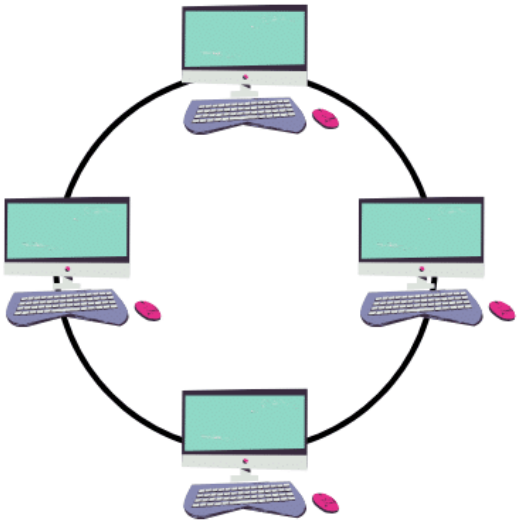
b. Pengembangan jaringan atau penambahan *workstation* baru dapat dilakukan dengan mudah tanpa mengganggu workstation lain.
c. Kecepatan pengiriman data lebih cepat karena data berjalan searah.
d. Lebih mudah dan murah jika ingin menambah atau mengurangi jumlah node karena yang dibutuhkan hanya kabel dan konektor.

Kekurangan Topologi Bus :

a. Apabila terdapat gangguan disepanjang kabel pusat maka keseluruhan jaringan akan mengalami gangguan.

2. Topologi Ring

Topologi ring atau cincin merupakan kumpulan komputer yang terhubung, dan membentuk suatu ring atau cincin. Topologi ini mempunyai kekurangan seperti topologi bus karena desain topologi ring menyerupai topologi bus, hanya saja ujung-ujungnya terhubung. Dalam topologi ring, data dikirimkan dalam bentuk sinyal bergerak searah sepanjang cincin dari satu perangkat keperangkat berikutnya.



Gambar 2. 2 Topologi Ring

Kelebihan Topologi Ring:

a. Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan *server*.
b. Dapat melayani aliran lalu lintas data yang padat, karena data dapat bergerak ke kiri atau ke kanan.

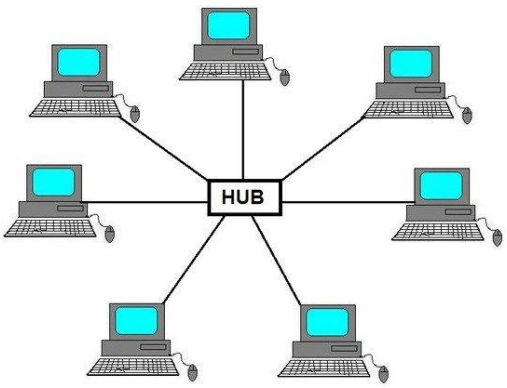
c. Waktu untuk mengakses data lebih optimal.

Kekurangan Topologin Ring:

a. Penambahan terminal atau *node* akan menjadi lebih sulit bila *port* sudah habis.
b. Jika pada salah satu terminal mengalami kerusakan, maka semua terminal pada jaringan tidak dapat digunakan.

3. Topologi Star

Topologi ini berbentuk seperti star atau bintang, setiap komputer terhubung ke konsentrator atau hub melalui sebuah kabel, jadi kalau terjadi kerusakan pada perangkat jaringan di salah satu *computer* maka tidak akan mempengaruhi jaringan pada komputer yang lain. Karakteristik dari topologi jaringan ini adalah *node* berkomunikasi langsung dengan station lain melalui *central node* (*hub/switch*), *traffic* data mengalir dari *node* ke *central node* dan diteruskan ke *node* tujuan. Jika satu segmen kabel putus, maka jaringan yang lain tidak akan terputus. Apabula terjadi kerusakan pada *node* maka semua perangkata akan terganggu dengan beberapa jaringan yang lain (Susanto, 2020).



Gambar 2. 3 Topologi Star

(Sumber : exabytes.co.id, 2023)

Kelebihan Topologi Star:

a. Jika terjadi penambahan atau pengurangan terminal tidak mengganggu operasi yang sedang berlangsung.

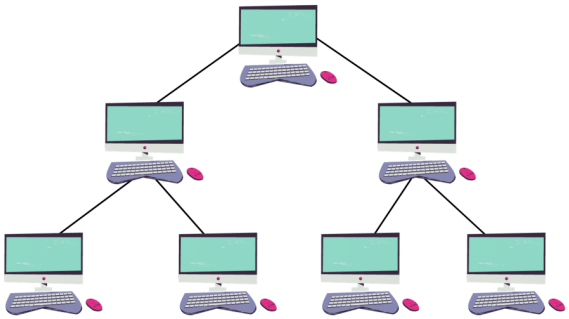
b. Jika salah satu terminal rusak, maka terminal lainnya tidak mengalami gangguan arus lalu lintas informasi data lebih optimal.

Kekurangan Topologi Star:

a. jumlah terminal terbatas, tergantung *port* yang ada pada *hub*.
b. Lalu lintas data yang padat dapat menyebabkan jaringan bekerja lebih lambat

4. Topologi *Tree*

Topologi *tree* pada jaringan komputer memiliki pengertian dimana sebuah perangkat komputer (*hub* atau *switch*) atau disebut *root* pada level teratas yang bertindak sebagai pusat utama bagi seluruh komputer lainnya, dan terdapat sebuah komputer sentral yang menjadi pusat komunikasi bagi komputer di bawahnya.



Gambar 2. 4 Topologi Tree

(Sumber : itbox.id, 2023)

Topologi *Tree* sebenarnya kombinasi dari Topologi Star dan Topologi Bus namun yang membedakannya adalah topologi *tree* ini terdapat banyak *Hub* atau *Switch* dalam jaringan dan *system* hierarkinya.

Kelebihan Topologi *tree*:

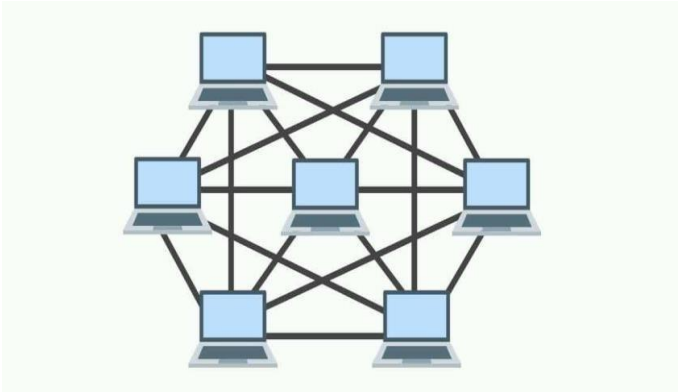
a. Seperti topologi star perangkat terhubung pada pusat pengendali/*hub*.
b. Tetapi hub dibagi menjadi dua, *central hub*, dan *secondary hub*.
c. Topologo *tree* memiliki keunggulan lebih mampu menjangkau jarak yang lebih jauh dengan mengaktifkan fungsi *Repeater* yang dimiliki oleh *hub*.

Kekurangan topologi *tree*:

a. Kabel yang digunakan menjadi lebih banyak sehinnga diperlukan Perencanaan yang matang dalam pengaturannya, termasuk didalamnya adalah tata letak ruangan.
b. Sulitnya pada saat melakukan instalasi dan melakukan konfigurasi ulang saat jumlah komputer dan peralatan-peralatan yang terhubung semakin meningkat jumlahnya.
c. Biaya yang besar untuk memelihara hubungan yang berlebih. Menyebabkan jarang juga yang menggunakan topologi *tree* ini karena di butuhkan biaya pemeliharaan yang cukup besar.

5. Topologi Mesh

   Topologi jaringan ini menerapkan hubungan ke semua *computer* sehingga membutuhkan lebih dari satu Lan *card*, topologi ini jarang digunakan karena rumit dan tidak praktis sebab membutuhkan kabel yang banyak.



Gambar 2. 5 Topologi Mesh

(Sumber : (N. A. Putra et al., 2021)

Kelebihan Topologi Mesh:

a. Terjaminnya kapasitas *channel* komunikasi, karena memiliki hubungan yang berlebih.
b. Relatif lebih murah untuk dilakukan *troubleshoot*.

2.1.3 Perangkat Jaringan

Sesuai dengan fungsinya perangkat *computer* dalam sebuah jaringan dibedakan menjadi 2 (dua) yaitu : Komputer *server* dan *computer client* . Dan segala sesuatu yang berhubungan dengan koneksi jaringan seperti: *Printer, CDROM, Scanner, Bridges, Router* dan lainnya yang dibutuhkan untuk *procces transformasi* data didalam jaringan (Bali, 2021).

1. Server

   Server merupakan pusat *control* dari jaringan *computer*. Biasanya berupa komputer berkecepatan tinggi dengan kapasitas RAM yang besar dan memiliki space hard disk yang cukup besar. Sistem operasi yang digunakan merupakan sistem operasi khusus yang dapat memberikan berbagai layanan bagi *workstation*. *Server* jaringan yang terpusat dan bias dengan cepat memperbaiki masalah yang ada pada *hardware* (Nurdadyansyah & Hasibuan, 2021).

2. Workstation

   Workstation adalah salah satu dari jenis komputer yang biasanya dipakai untuk keperluan tertentu yang berhubungan dengan pekerjaan berat, bahkan tugas yang diberikan dapat lebih ke spesifik dalam satu bidang saja. Semua komputer yang terhubung dengan jaringan dapat dikatan sebagai workstation. Komputer ini yang melakukan akses ke server untuk mendapat layanan yang telah disediakan oleh server (Farhan Fatoni et al., 2022)

3. *Hub* (Penghubung)

   Hub bias disebut dengan perangkat yang digunakan untuk menghubungkan antar komputer dalam pertukaran data. *Hub* ini juga dapat dikatakan sebagai *central node* yang mana merupakan perangkat yang sangat penting. Sebab aliran data akan melewati perangkat ini sebelum data tersebut sampai pada tujuannya (Susanto, 2020).

4. Bridge

   Bridge adalah perangkat yang meneruskan lalu lintas antara segmen jaringan berdasar informasi pada lapisan *data link*. *Bridge* membagi satu buah jaringan besar kedalam beberapa jaringan kecil. *Bridge* juga dapat di

gunakan untuk mengkoneksi *network* yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula (Bali, 2021).

5. Router

   Router adalah perangkat yang berfungsi menghubungkan suatu LAN ke suatu *internetworking*/WAN dan mengelola penyaluran lalu-lintas data di dalamnya. Router akan menentukan jalur terbaik untuk komunikasi data. Sistem kerja ini berbeda dengan bridge yang bersifat *protocol* independent, dimana *protocol independent* adalah keluarga *protocol multicast* untuk jaringan protokol internet yang menyediakan distribusi data satu-ke-banyak dan banyak-ke-banyak melalui LAN, WAN, atau Internet (Bali, 2021).

6. Switch

   Switch merupakan perangkat jaringan komputer yang berfungsi untuk menghubungkan beberapa komputer. Secara fisik, bentuk dari *switch* sama dengan *hub*, namun jika dilihat dari sisi logika *switch* sama dengan *bridge*. *Switch* memiliki dua tipe, yaitu *unmanaged switch* yang merupakan tipe termurah dan *managed switch* yang merupakan tipe termahal (Bali, 2021).

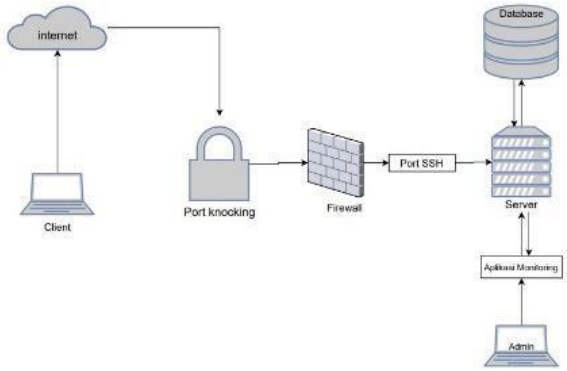
2.2 Keamanan Jaringan

Pengertian keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Bisa juga dikatakan keamanan jaringan komputer adalah praktik dan prosedur yang dilakukan untuk melindungi jaringan komputer dari ancaman dan serangan yang merusak, seperti virus, *malware, hacker*, dan peretasan data. Tujuan utama dari keamanan jaringan komputer adalah untuk melindungi data sensitif dan informasi rahasia dari kebocoran atau akses yang tidak sah. Keamanan jaringan komputer mencakup sejumlah langkah dan teknologi untuk mencegah, mengidentifikasi, dan merespon ancaman keamanan jaringan komputer (Yulianto & Aprilyani, 2020).

2.3 Port Knocking

Sebuah *port* dalam protokol jaringan *TCP/IP* merupakan suatu mekanisme yang memberikan atau mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. *Port* dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam

jaringan *TCP/IP*. Sehingga, *port* juga mengidentifikasikan sebuah proses tertentu di mana sebuah *server* dapat memberikan sebuah layanan kepada *client* atau bagaimana sebuah *client* dapat mengakses sebuah layanan yang ada dalam *server* (Yudi mulyanto et al., 2021).



Gambar 2. 6 Penutupan Port

(Sumber : Ernawati et al., 2022)

Port Knocking merupakan metode sistem autentikasi yang secara khusus dibuat untuk jaringan. Ide dasar dari sistem autentikasi ini telah lama digunakan namun baru pada tahun 2013. Pada dasarnya *Port Knocking* dapat didefinisikan sebagai suatu metode komunikasi antara dua komputer, dimana informasi yang dikirimkan di-*encode* dalam bentuk usaha koneksi ke *port-port* dalam urutan tertentu. Usaha membangun koneksi ini bisa disebut juga ketukan. Mekanisme *Port Knocking* akan menggunakan *file log* yang dibuat oleh *Firewall* untuk mengetahui apakah suatu usaha koneksi telah dibuat oleh suatu *host* atau tidak (Yudi mulyanto et al., 2021).

Port Knocking adalah suatu metode untuk membangun komunikasi antar komputer dari mana pun selama masing-masing komputer tersebut terhubung dalam suatu jaringan komputer, dengan perangkat komputer yang tidak membuka port komunikasi apapun secara bebas, tetapi perangkat tersebut masih tetap dapat diakses dari luar, dengan menggunakan suatu format konfigurasi *port* ketukan yang berupa percobaan untuk mengirimkan koneksi pada *port* ketukan (Yudi mulyanto et al., 2021). *Port Knocking* merupakan suatu sistem keamanan yang dibuat secara

khusus untuk sebuah jaringan. Pada dasarnya cara kerja dari *Port Knocking* adalah menutup *port* yang ada seperti *Winbox*, SSH dan HTTP (Rahman et al., 2023).

2.3.1 Cara Kerja Port Knocking

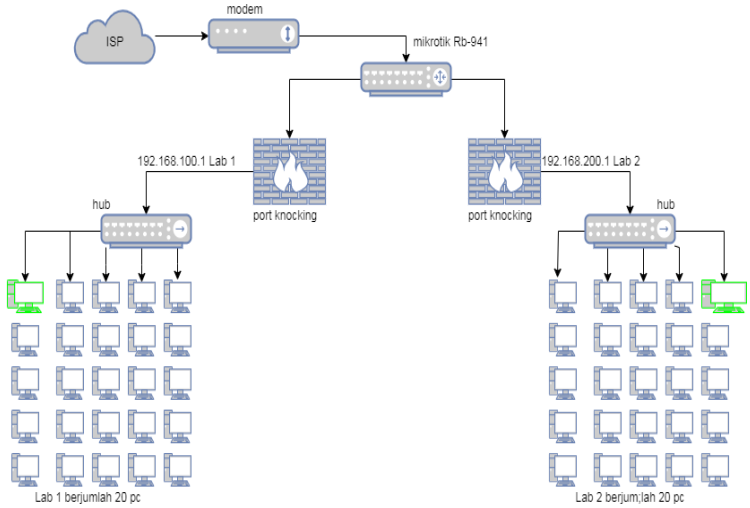
Fungsi dan cara kerja dari sistem ini tidak jauh berbeda dengan arti harafiahnya. *Port Knocking* merupakan sebuah metode untuk membangun komunikasi dari mana saja, dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas. Dengan kata lain, perangkat Komputer ini tidak memiliki *port* komunikasi yang terbuka bebas untuk dimasuki, tetapi perangkat ini masih tetap dapat diakses dari luar. Ini dapat terjadi jika Anda menggunakan metode *Port Knocking*. (Farhan Fatoni et al., 2022)

Koneksi dapat terjadi dengan menggunakan metode pengetikan *port-port*

komunikasi yang ada. Pengetukan *port-port* ini dilakukan dengan kombinasi tertentu secara berurutan dalam satu rentan waktu tertentu. Jika kombinasi dari pengetukan tersebut sesuai dengan yang telah ditentukan, maka sebuah *port* komunikasi yang diinginkan akan terbuka untuk Anda.

Setelah terbuka, Anda bebas mengakses apa yang ada dalam jaringan tersebut melalui *port* komunikasi yang baru terbuka tadi. Setelah selesai melakukan pekerjaan dan kepentingan Anda, *port* komunikasi yang tadi terbuka dapat ditutup kembali dengan melakukan pengetukan sekuensialnya sekali lagi.

Maka, perangkat komputer dan jaringan Anda akan kembali aman Salah satu metode keamanan jaringan yaitu dengan metode *Port Knocking*. (Farhan Fatoni et al., 2022)



Gambar 2. 7 Perancangan desain jaringan Simple Port Knocking

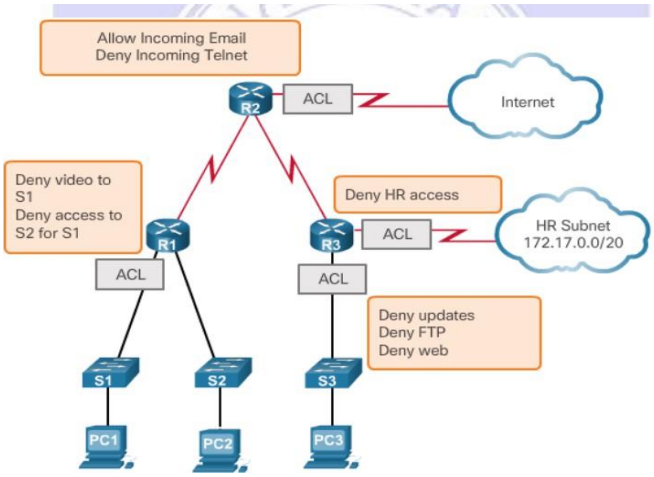
(Sumber: Farhan Fatoni et al., 2022)

Port Knocking merupakan sebuah konsep menyembunyikan layanan jarak jauh di dalam sebuah *Firewall* yang memungkinkan akses ke *port* tersebut hanya untuk mengetahui service setelah klien berhasil diautentikasi ke *Firewall*. Kinerja dari *Port Knocking* itu sendiri adalah menutup semua port yang ada, dan hanya user tertentu saja yang dapat mengakses *port* yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu. Berbeda dengan *Firewal*l, cara kerja dari *Firewall* adalah menutup semua port tanpa memperdulikan apapun meskipun user tersebut memiliki hak untuk mengakses *port* tersebut. Sehingga user yang memiliki hak akses tersebut juga tidak bisa untuk mengaksesnya. Dengan cara ini perangkat jaringan akan lebih aman seperti *router*, sebab admin jaringan dapat melakukan *filtering* terhadap *port-port* yang lemah.. (Farhan Fatoni et al., 2022)

2.4 Access Control List (ACL)

Access Control Lists (ACL) adalah *tools* yang penting dan cukup berguna di dalam jaringan komputer. *Access Control List* (ACL) memungkinkan *administrator* jaringan untuk menyaring lalu lintas *traffic* yang masuk ataupun keluar dari perangkat jaringan. Sistem keamanan jaringan menjadi faktor yang sangat penting untuk dipertimbangkan bagi seorang *administrator* jaringan dan berbagai upaya dilakukan dalam mengamankan jaringan dari ancaman dan

serangan baik oleh *hacker* maupun penyebaran virus. *Access Control List* (ACL) yang dibuat dengan baik dapat dijadikan dasar sistem keamanan jaringan komputer.



Gambar 2. 8Struktur Access Control List (ACL)

(Sumber: Kelompok, 2022)

Fungsi dari *Access Control List* (ACL) :

1. Membatasi *traffik* jaringan dan meningkatkan unjuk kerja jaringan.
2. Mampu memberikan dasar keamanan untuk akses ke jaringan.
3. Memberi keputusan terhadap jenis *trafik* mana yang akan dilewatkan atau di *interface router*.
4. Mengontrol daerah-daerah *(cells)* dimana client dapat mengakses jaringan. Memilih *host-host* yang diijinkan atau di akses ke segmen jaringan.

2.4.1 Jenis-Jenis Access Control List (ACL)

Access Control List adalah mekanisme untuk mengatur "siapa yang boleh melakukan apa "dan "dari mana dan boleh kemana". Penerapannya membutuhkan klasifikasi data *(public, private,confident, secret)* dan berbasiskan *role* (kelompok atau grup hak akses). Menururut penulis ACL *(Access Control List)* merupakan metode selektivitas terhadap *packet* data yang akan dikirimkan pada alamat yang dituju. Secara sederhana ACL dapat kita ilustrasikan seperti sebuah *standard* keamanan. Hanya paket yang memiliki kriteria yang sesuai dengan aturan yang diperbolehkan melewati gerbang keamanan, dan bagi paket yang tidak memiliki kriteria yang sesuai dengan aturan yang diterapkan, maka paket tersebut akan

ditolak. ACL dapat berisi daftar IP *address*, MAC *address*, *subnet*, atau *port* yang diperbolehkan maupun ditolak untuk melewati jaringan.

Berikut adalah Jenis-Jenis *Access Control List* (ACL) (Sihotang et al., 2020):

1. Standard ACL (Access Control List)

   Standard ACL (Access Control List) merupakan jenis ACL yang paling sederhana. ACL ini diterapkan pada router tujuan. mengizinkan atau menolak paket hanya berdasarkan alamat sumber. Alamat sumber yang dimaksud dapat berupa alamat sumber dari jaringan *(Network Address)* atau alamat sumber dari *host. Standard ACL (Access Control List)* dapat diimplementasikan pada proses *filtering protocol* TCP, UDP atau pada nomor *port* yang digunakan. Meskipun demikian, *Standard* ACL hanya mampu mengijinkan atau menolak paket berdasarkan alamat sumbernya saja (Sihotang et al., 2020).

2. Extended Access Control List (ACL)

   Extended Access Control List (ACL) merupakan jenis *Access Control List* (ACL) yang mampu memberikan tingkat keamanan yang lebih baik ketimbang Standard *Access Control List* (ACL). *Extended Access Control List* (ACL) ini diterapkan pada router sumber. mengizinkan atau menolak paket berdasarkan sumber dan juga alamat tujuan. Selain itu *Extended Access Control List* (ACL) memberikan keleluasaan kepada admin jaringan dalam melakukan proses *filtering* dengan tujuan yang lebih spesifik (Sihotang et al., 2020).

3. Lalu Lintas Access Control List (ACL)

   Access Control List (ACL) merupakan daftar *access control* yang berisi perizinan serta data kemana *user* akan diberikan izin. Jika data telah memiliki izin, maka hanya dapat diakses oleh beberapa *user* yang telah diberikan akses saja dan tentunya sudah dikontrol oleh *access control* tersebut. Dalam hal ini, diperlukan administrator untuk mengamankan informasi dan mengatur hak atas informasi apa saja yang boleh diakses dan kapan informasi tersebut dapat diakses. Secara sederhana *Access Control List* (ACL) merupakan sebuah standar keamanan (Yel et al., 2023).

Cara kerja *Access Control List* (ACL) sendiri adalah selalu membaca setiap list dengan cara sequential atau berurut dari atas ke bawah. Ketika ada paket data ACL kan membaca dan membandingkan setiap *list* yang sudah dibuat. Jika menemukan kondisi yang sesuai, paket akan mengikuti aturan yang sudah ada dalam *Access List*. Namun jika paket tidak menemukan kondisi yang sesuai maka paket tidak bisa mendapatkan akses (Yel et al., 2023)

Penggunaan paling umum dan paling mudah untuk dimengerti adalah melakukan penyaringan paket yang tidak diinginkan saat Anda melakukan implementasi kebijakan keamanan, seperti mengatur *Access Control List* (ACL) untuk membuat keputusan yang sangat spesifik mengenai pola lalu lintas sehingga hanya *host* tertentu saja yang dapat mengakses sumber daya tersebut, sedangkan yang lainnya ditolak (Yel et al., 2023).

Access list juga dapat digunakan pada situasi lain, dimana tidak harus meliputi penolakan paket, seperti mengontrol *network* yang akan atau tidak dinyatakan sebagai *protocol dynamic routing* dengan mengkonfigurasikan *access list* dengan cara yang sama seperti sebelumnya dimana penerapannya dilakukan ke *protocol routing* bukan ke *interface*.

Selain itu, kita juga dapat menggunakan *Access Control List* (ACL) ini untuk mengkategorikan paket atau antrian atau layanan QOS serta mengontrol tipe lalu lintas data nama yang akan mengaktifkan link ISDN. *Access Control List* dapat digunakan untuk mengaudit berbagai percobaan akses yang terekam dalam sistem. Sehingga, pemilik *resource* dapat dengan mudah melacak siapa saja yang mengakses sistem, kapan waktu aksesnya, dan apa jenis akses yang dilakukan (Yel et al., 2023)

2.5 *Cisco Paket Tracer*

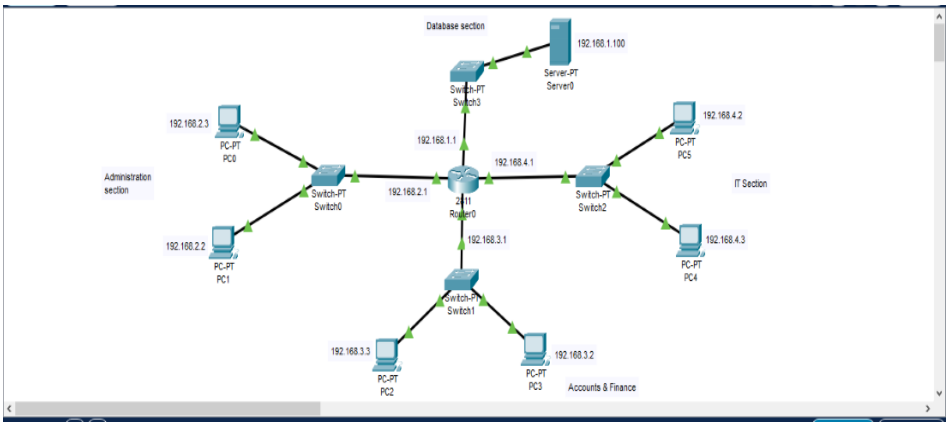
Cisco Packet Tracer adalah sebuah perangkat lunak simulasi jaringan interaktif yang dikembangkan oleh *Cisco Systems* dan dirancang untuk membantu dalam pembelajaran, pelatihan, perancangan, serta simulasi jaringan komputer tanpa memerlukan perangkat keras *(hardware)* secara langsung. *Cisco Packet Tracer* sangat populer di kalangan pelajar, mahasiswa, guru, teknisi jaringan, dan

profesional IT karena memberikan lingkungan virtual yang kaya fitur untuk membangun dan menguji topologi jaringan secara fleksibel dan efisien.

Cisco Packet Tracer bekerja dengan menyediakan antarmuka *grafis (GUI)* yang memungkinkan pengguna melakukan drag and drop berbagai perangkat jaringan seperti *router, switch, PC, server, firewall, access point,* sensor *IoT*, dan perangkat lainnya, lalu menghubungkannya menggunakan berbagai jenis kabel. Dalam lingkungan simulasi ini, pengguna dapat melakukan konfigurasi jaringan layaknya di dunia nyata, termasuk mengatur IP *address, subnetting, VLAN, DHCP, DNS, routing statis* maupun dinamis (seperti RIP, OSPF, dan EIGRP), serta menerapkan aturan keamanan seperti *Access Control List (ACL*).

Salah satu keunggulan utama *Cisco Packet Tracer* adalah kemampuannya untuk bekerja dalam dua mode: *Realtime Mode* dan *Simulation Mode* :

1. Pada *Realtime Mode,* jaringan akan berjalan seperti di dunia nyata, memungkinkan pengguna menguji seberapa baik konfigurasi yang telah dilakukan.
2. Sementara itu, *Simulation Mode* memberikan pengguna kendali penuh untuk memantau alur data *(packet flow)* secara mendetail — misalnya melihat bagaimana paket ICMP dikirim dan diterima, atau bagaimana sebuah paket diblokir oleh *firewall* atau ACL.



Gambar 2. 9 *Cisco Paket Tracer*

(Sumber : Ernawati et al., 2022)

Selain untuk pembelajaran dasar hingga lanjutan tentang jaringan komputer, *Cisco Packet Tracer* juga digunakan untuk mempersiapkan sertifikasi jaringan internasional, terutama *Cisco Certified Network Associate (CCNA).* Banyak

skenario dan latihan praktikum dari program *Cisco Networking Academy* yang dirancang langsung menggunakan platform ini.

2.6 Mikrotik

Mikrotik adalah adalah sistem operasi komputer dan perangkat lunak *computer* yang digunakan untuk menjadikan komputer biasa menjadi router, mikrotik dibedakan menjadi dua yaitu operation sistem mikrotik bisa dikenakan mikrotik os dan mikrotik *routerboard*, untuk mikrotik *routerboard* tidak memerlukan komputer dalam menjalankannya cukup menggunakan board yang sudah include dengan mikrotik os. Mikrotik os mencakup fitur yang dibuat khsus untuk *ip network* dan jaringan *wireless*.

Mikrotik OS merupakan sistem operasi khusus yang digunakan untuk memanajemen *network*. Kata Mikrotik merujuk pada bahasa Latvia tempat OS ini berasal, yang berarti *network* kecil. Mikrotik hadir dalam dua jenis, yaitu Mikrotik Router OS (ROS) dan Mikrotik *RouterBoard*. Mikrotik *Routerboard* merupakan *hardware* spesifik yang telah ditanamkan sistem operasi mikrotik untuk dijadikan router. Sedangkan Mikrotik *RouterOS* merupakan sistem operasi mikrotik yang dapat diinstall pada PC sehingga dapat berfungsi sebagai *router.*

2.6.1 Jenis-Jenis Mikrotik

Mikrotik hadir dalam dua jenis, yaitu Mikrotik *Router* OS (ROS) dan Mikrotik *RouterBoard*.

a. Mikrotik *Router* OS (ROS)

   Mikrotik *Router* OS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan *computer* menjadi *router network* yang mempunyai berbagai fitur dalam teknologi jaringan.

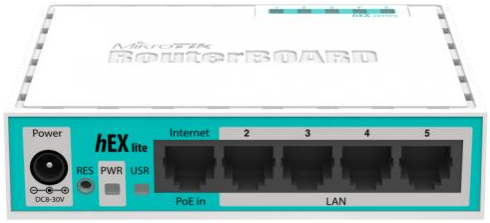
Gambar 2. 10 Mikrotik OS

Sumber: (Danang & Setiawan, 2022)

MikroTik *Router* OS adalah sistem operasi yang digunakan pada perangkat *Routerboard*. Selain itu, *Router* OS juga dapat diinstal pada komputer (PC) dan mengubahnya menjadi *router* dengan berbagai fitur yang diperlukan, termasuk *Routing* Mengelola pengiriman data antara jaringan *Firewall* Melindungi jaringan dari ancaman dan mengatur lalu lintas data. *Firewall* adalah teknologi yang digunakan untuk memonitor dan memfilter lalu lintas jaringan. *Firewall* dapat memblokir akses yang tidak sah ke jaringan, mencegah serangan *malware* dan *virus*, serta mengidentifikasi aktivitas mencurigakan. Jadi, MikroTik *Router*OS adalah sistem operasi yang kuat dan serbaguna yang digunakan untuk mengelola perangkat jaringan dan *router* (Rahman et al., 2023)

b. Mikrotik *RouterBoard*

Mikrotik *routerboard* adalah suatu *hardware* yang dapat menjalankan *router network* tanpa perlu di *install* ke sebuah komputer, karena *router* mikrotik ini telah didesain untuk menjalankan *router* OS sehingga dapat menjadi *router* yang handal untuk pengguna.



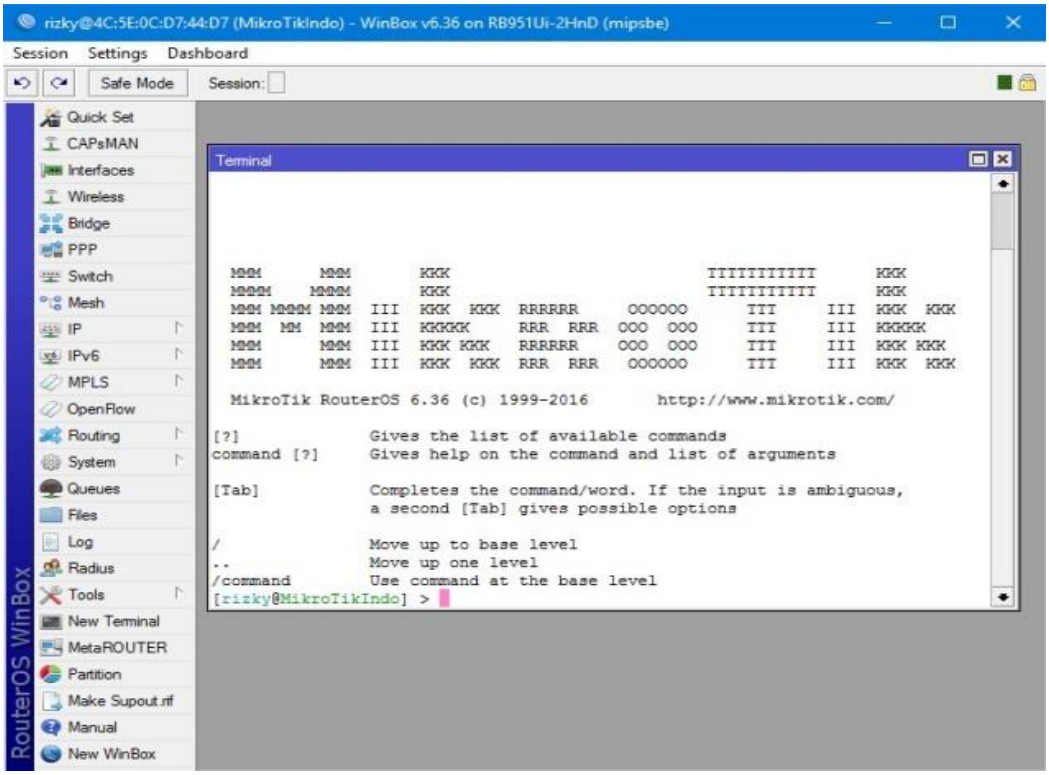
Gambar 2. 11 Mikrotik *RouterBoard*

(Sumber: Hendrawan & Saputra, 2021)

2.7 Winbox

Winbox adalah sebuah *software* jaringan yang digunakan untuk me-*remote* sebuah *server* mikrotik kedalam mode *GUI (Graphical User Interface)* melalui *operating* sistem *windows. Winbox* adalah *utility* yang digunakan untuk konektivitas dan konfigurasi Mikrotik menggunakan *MAC Address* atau Protokol IP, dengan *winbox* kita dapat melakukan konfigurasi mikrotik *Router* OS dan *Router Board* menggunakan metode *GUI (Graphical User Interface)* dengan cepat dan mudah.

Winbox dibuat menggunakan Win32 *binary* tapi dapat dijalankan pada *Linux*, dan *MAC* OS dengan menggukanan wine, semua fungsi *winbox* didesain dan dibuat semirip mungkin dengan fungsi *console, Winbox* memiliki beberapa fungsi yaitu *setting* mikrotik *router* dalam mode *GUI, Setting bandwith* atau membatasi kecepatan jaringan, memblokir sebuah situs, mengetahui dan mengatur alamat Ip dan akses ke situs tertentu.



Gambar 2. 12 *Winbox*

(Sumber : P. G. O. W. Putra & Adi Jaya, 2022)

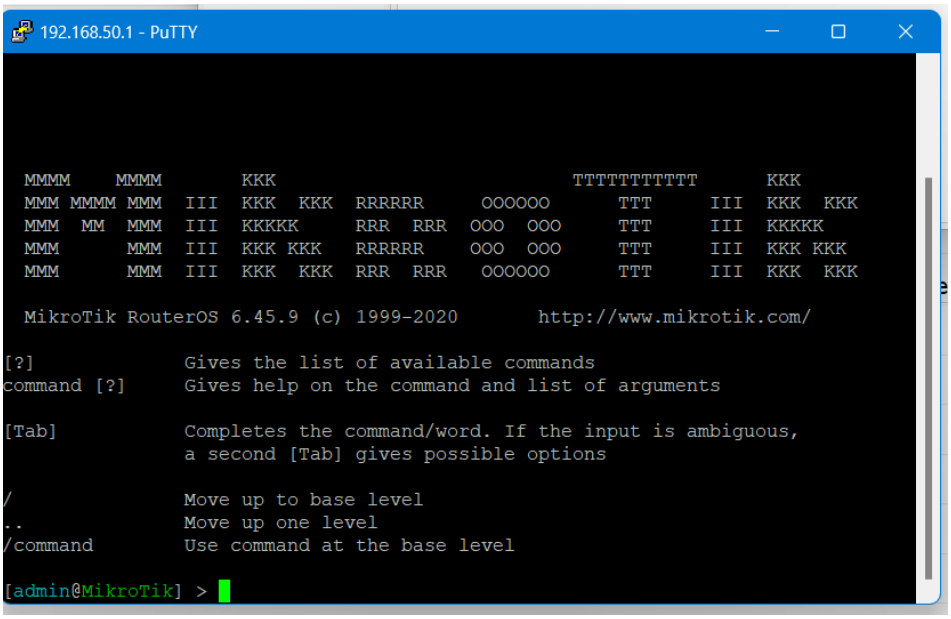
Kebanyakan teknisi banyak mengkonfigurasi mikrotik OS atau mikrotik *routerboard* menggunakan *winbox* dibanding dengan mengkonfigurasi langsung lewat mode *CLI (Command LineInterface)*. Hal ini karena menggunakan *winbox* dirasa lebih mudah dibanding melalui *browser*. Dan hasilnya pun juga lebih cepat (Yel et al., 2023).

2.8 *PuTTY*

PuTTY merupakan perangkat lunak terminal emulator yang berfungsi untuk melakukan akses serta pengendalian perangkat jaringan secara jarak jauh *(remote access)* melalui berbagai protokol, antara lain *Secure Shell* (SSH), Telnet, dan *rlogin*. Aplikasi ini banyak dimanfaatkan oleh administrator jaringan maupun pengguna yang membutuhkan interaksi langsung dengan perangkat jaringan dari lokasi yang berbeda (Setyawan, 2023).

PuTTY memiliki antarmuka yang sederhana namun informatif, sehingga memudahkan pengguna dalam melakukan konfigurasi maupun pengelolaan

koneksi. Fitur yang disediakan meliputi dukungan koneksi melalui SSH, Telnet, dan *rlogin*, opsi konfigurasi yang fleksibel, penggunaan kunci publik maupun kunci privat untuk autentikasi, serta kemampuan menyimpan data sesi koneksi secara aman.



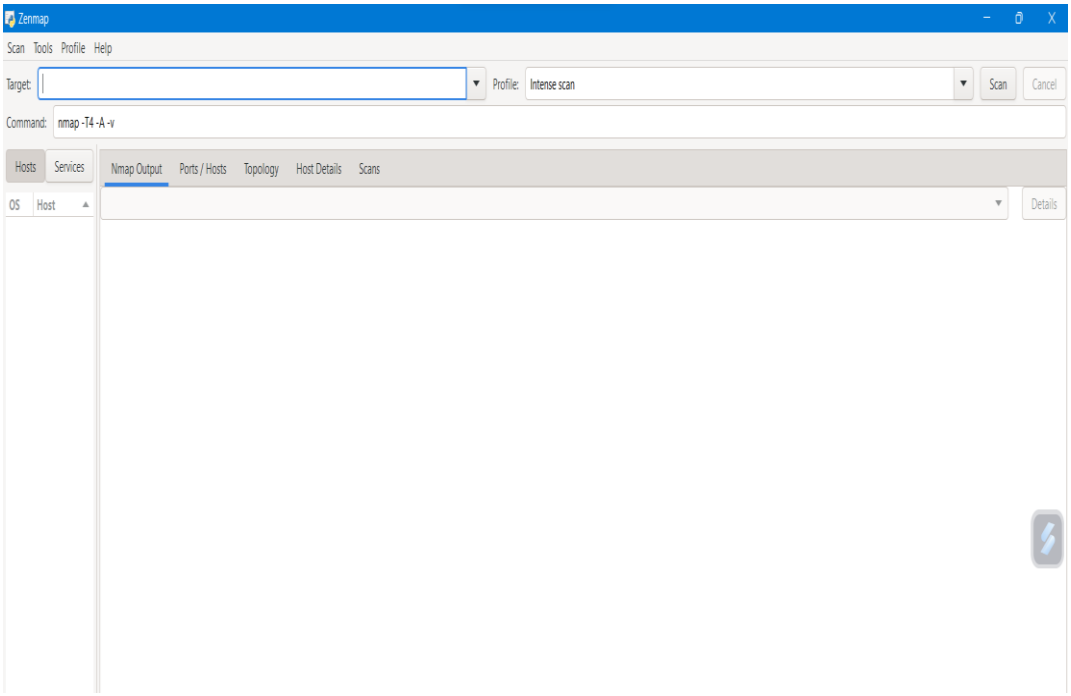
Gambar 2. 13 Aplikasi *Putty*

(Sumber : Setyawan, 2023)

Sebagai aplikasi *open-source, PuTTY* menawarkan kombinasi antara kemudahan penggunaan *(user-friendly interface)* dan kelengkapan fungsi, sehingga menjadi salah satu perangkat lunak yang andal dalam pengelolaan serta pengendalian perangkat jaringan secara *remote*, baik dalam lingkup administrasi sistem maupun manajemen jaringan komputer (Setyawan, 2023).

2.9 Zenmap

Zenmap adalah antarmuka grafis *(Graphical User Interface/GUI)* resmi dari Nmap *(Network Mapper),* yang merupakan salah satu perangkat lunak pemindai jaringan *(network scanning)* paling populer dan banyak digunakan di bidang keamanan jaringan. Zenmap dirancang untuk memudahkan pengguna, baik yang masih pemula maupun yang sudah berpengalaman, dalam melakukan pemindaian dan pemetaan jaringan komputer (Nur et al., 2024).



Gambar 2. 14 Aplikasi Zenmap

(Sumber : (Nur et al., 2024)

Dengan Zenmap, pengguna dapat menjalankan berbagai perintah Nmap tanpa harus mengetikkan sintaks di terminal, karena semua fungsi tersedia melalui tampilan grafis yang intuitif. Aplikasi ini mampu menampilkan hasil pemindaian dalam bentuk tabel, teks, maupun peta topologi jaringan, sehingga mempermudah analisis terhadap *host,* layanan, dan *port* yang terbuka di dalam jaringan (Nur et al., 2024).

2.9 Penelitian Terdahulu

Tabel 2. 1 Penelitian Terdahulu

No	Nama Penelitian (tahun)	Metode	Data	Hasil
1.	(Santoso et al., 2022)	Port Knocking	Perkembangan teknologi semakin meningkat. Keamanan sistem dipengaruhi oleh perkembangan ini. Oleh karena itu, pengguna aplikasi yang terhubung dengan jaringan internet	didapatkan hasil bahwa Peneliti dapat membantu administrator mengamankan *Routerboard* Mikrotik pada sistem jaringan komputer SMK N 1

			perlu lebih berhati-hati terhadap penyusupan oleh pihak yang tidak berwenang.	Sumbawa Besar dengan menggunakan pendekatan *Port Knoking* yang dapat membantu meningkatkan keamanan jaringan.
2.	(Farhan Fatoni et al., 2022)	Port Knocking	Keamanan data antara internal instansi, maka pemecahan masalah dapat dilakukan dengan *Port Knocking* pada mikrotik yang sudah tersedia di masing-masing gedung.	Data dan informasi yang digunakan dalam penelitian ini merupakan hasil riset yang dilakukan pada LKP Surya Komputer. Riset dilakukan selama 30 hari yaitu tanggal 1-30 januari 2021. Tujuan dari penelitian ini adalah merancang sistem keamanan jaringan pada Lab LKP Surya Komputer.
3.	(Laksono & Nasution, 2020)	Acees Control List	Di sebuah Perusahaan X penggunaan internet merupakan sebuah tuntutan bagi para pekerja.	Hasil reset penulis membuktikan bahwa Vlan *Access Control List* dengan metode *filtering* dan pembagian pengguna koneksi internet dapat menyaring dan mengidentifikasi pengguna yang telah di batasi aksesnya untuk mengakses pengguna yang lain atau ke *server* di Perusahaan X untuk meningkatkan Keamanan data.
4	(Jayanto et al., 2021)	Port Knocking	Sebagian besarjaringan komputer yang mengalami permasalahanyang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer.	Berdasarkan hasil penelitian yang telah dilakukan Pada tahap ini dilakukan evaluasi tentang sistem jaringan yang berjalan. Berdasarkan tahapan-tahapan yang telah dilakukan maka perlu penelitisarankan untuk

				selalu mengupdate *port-port* yang digunakan oleh aplikasi. Bukan hanya itu saja sistem ini akan berjalan jika operator terus mengupdatenama alamat aplikasi yang terkadang berubah-ubah
5.	Nurbahri &Cahyono , (2023	Control List	Mayoritas cracker menggunakan sistem *port* terbuka untuk menyerang sistem jaringan. sebagai ilustrasi, Serangan Dos atau ddos yang menargetkan *host* atau komputer target dengan sejumlah besar paket yang datang dari beragam *host*.	Hal ini dapat bertindak sebagai pencegah serangan *zero-day* dan membantu mencegah pemindai menemukan *service* yang tersedia dan dapat diakses pada *host*. Dalam hal ini *blocking port* dapat melindungi *Firewall* dari pemindai.
6	(Jamalul'ain & Nurdiawan, 2022)	Port Knocking	Di zaman modern sekarang ini perkembangan Teknologi Informasi (TI) sangat pesat, dibuktikan dengan semakin canggihnya dunia Teknologi Informasi dari waktu ke waktu yang Memberikan kemudahan bagi manusia dalam berkomunikasi. Jaringan komputer digunakan hampir oleh semua orang tanpa terkecuali termasuk para *craker*.	Hasil pengujian hipotesis penelitian tesawal dan tes akhir di peroleh nilai thitung =4.714 dan nilai tabel =0,3550. Maka hitung > table. Dengan demikian dapat disimpulkan bahwa diterima dan ditolak. Metode *knocking port* berbasis mikrotik dapat mengoptimalkan keamanan jaringan komputer.

7.	(Yudi mulyanto et al., 2021)	Port Knocking	Penelitian dilakukan untuk menganalisa dan mengimplementasikan metode *Port Knocking* dalam keamanan jaringan agar dapat mencegah serangan pada *port-port* jaringan komputer SMKN 1 Sumbawa Besar.	Dari hasil analisis dan perancangan kemanan jaringan yang telah dilakukan dengan menggunakan metode *Network DevelopmentLife Cycle* (NDLC) maka penulis dapat mengambil kesimpulan bahwa implementasi *Port Knocking* untuk keamanan jaringan SMKN 1 Sumbawa Besar telah selesai dilakukan menggunakan perangkat *Routerboard* Mikrotik RB750r2 dan aplikasi pendukung lainnya.
8.	Heriyanto et al, (2020)	Port Knocking	Dengan berkembang nya zaman akses internet yang disediakan oleh tempat kerja memunculkan masalah terkait penggunaan internet untuk kepentingan pribadi, seperti bermain game online	Untuk menangani permasalahan ini peneliti memblokir *trafic –trafic* dari situs yang tidak ada hubungan nya dengan kinerja perusahaan itu dengan menggunakan fitur yang ada pada *router* Mikrotik yaitu *filter rule* dan *filter layer* 7 protokol.
9	Karlinda et al, (2021)	Access Control List (ACL)	Penelitian yang telah dilakukan di PT MNC Televisi *Network* ini akan memaanfatkan fitur fitur yang ada pada *router* Mikrotik untuk mengatasi keamanan jaringan di PT MNC Televisi *Network.*	Dengan di manfaatkannya beberapa fitur yang ada di *router* Mikrotik bisa membuat jam kerja di PT MNC Televisi *Network* lebihteratur dan membuat para karyawan tidak lagi bermain *game online* dan sosial media di jam kerja.

2.10 Tinjangan Umum Pengadilan Agama Rantauprapat

Pengadilan Agama Rantauprapat Kelas I B merupakan lembaga peradilan di bawah Mahkamah Agung Republik Indonesia yang memiliki kewenangan dalam memeriksa, mengadili, dan memutus perkara di bidang hukum Islam bagi masyarakat beragama Islam. Lembaga ini berkedudukan di wilayah hukum Kabupaten Labuhanbatu dan sekitarnya, dengan lingkup perkara meliputi perkawinan, waris, wasiat, hibah, wakaf, zakat, infaq, shadaqah, serta ekonomi syariah.

Sebagai peradilan tingkat pertama, Pengadilan Agama Rantauprapat Kelas I B bertujuan memberikan pelayanan hukum yang profesional, cepat, sederhana, dan berbiaya ringan. Pencapaian tujuan tersebut didukung oleh peningkatan kompetensi aparatur, optimalisasi pelayanan publik, serta pemanfaatan teknologi informasi untuk mewujudkan peradilan yang transparan dan akuntabel.

2.10.1 Sejarah Singkat Pengadilan Agama Rantauprapat Kelas I B

Dasar Hukum dan Sejarah Pembentukan Pengadilan Agama Rantauprapat

Pengadilan Agama Rantauprapat secara resmi berdiri pada tanggal 1 Mei 1953 berdasarkan Peraturan Menteri Agama Republik Indonesia Nomor 2 Tahun 1953. Pada awal pembentukannya, lembaga ini dikenal dengan nama Majelis Pengadilan Agama Islam (M.P.A.I.) Kabupaten Labuhanbatu.

Sebelum pembentukan secara kelembagaan, fungsi peradilan agama di wilayah Labuhanbatu telah dijalankan sejak masa kesultanan pada era penjajahan Belanda. Saat itu, terdapat empat kesultanan, yaitu Kesultanan Panai, Kesultanan Kualuh, Kesultanan Kota Pinang, dan Kesultanan Billah. Masing-masing Sultan mengangkat Qadi sebagai pejabat yang berwenang memeriksa dan memutus sengketa keagamaan serta perkara keluarga umat Islam, dengan keputusan yang disahkan oleh Sultan.

Pada masa pendudukan Jepang, sistem peradilan agama tetap berada di bawah kewenangan para Sultan. Qadi tetap memeriksa perkara-perkara keagamaan seperti nikah, cerai, rujuk, hadanah, wakaf, waris, dan baitul mal, meskipun kondisi sosial-ekonomi masyarakat mengalami kemerosotan akibat situasi perang.

Pasca kemerdekaan Indonesia pada tanggal 17 Agustus 1945 hingga tahun 1953, peradilan agama di Labuhanbatu belum berdiri sebagai lembaga mandiri dan masih berada di bawah pengelolaan Kepala Departemen Agama setempat. Kepala Departemen Agama pertama yang menangani fungsi ini adalah M. Arifin Isa. Baru pada tahun 1953, melalui landasan hukum yang jelas, Pengadilan Agama Rantauprapat berdiri sebagai lembaga peradilan tingkat pertama yang memiliki kewenangan penuh dalam penyelesaian perkara di bidang hukum Islam.

2.10.2 Visi dan Misi

Adapun visi dan misi Pengadilan Agama Rantauprapat Kelas I B sebagai berikut :

a. Visi

"Terwujudnya Pengadilan Agama Rantauprapat Yang Agung"

b. Misi

1. Menjaga kemandirian badan peradilan;
2. Memberikan pelayanan hukum yang berkeadilan kepada para pencari keadilan;
3. Meningkatkan kualitas kepeminmpinan badan peradilan;
4. Meningkatkan kredibilitas dan transparansi badan peradilan.

2.10.3 Struktur Organisasi

Gambar 2. 15 Struktur Organisasi