BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Definisi Jaringan

Jaringan adalah sekumpulan sel yang memiliki bentuk serta struktur yang sama tetapi dengan fungsi yang berbeda yang mana jaringan telekomunikasi akan memberi izin untuk setiap node-node untuk saling bertukar informasi atau berbagi sumber daya *(resources)* (Fauzan & Purwanto, 2021).

Jaringan komputer adalah sekumpulan perangkat komputer yang terdiri dari *computer, hub, switch, router* serta perangkat jaringan komputer yang terhubung dengan media komunikasi lainnya yang mana nantinya akan bekerja sama dalam mencapai tujuan tertentu.

Beberapa pandangan para ahli mengenai jaringan komputer adalah sebagai berikut :

Menurut Dede sopandi yang dikutip oleh (Asnawi, 2018) jaringan komputer merupakan penggabungan dari teknologi telekomunikasi dengan teknologi komputer yang mana dari gabungan dua teknologi ini nantinya akan menghasilkan suatu pengolahan data yang meliputi pemakaian *s/w*, perangkat *h/w* yang mana database manajemen sistem akan dilakukan secara bersama sama.

Menurut Subramanian jaringan adalah pengolahan, pengaturan serta perincian yang bertujuan supaya setiap elemen pada jaringan dapat teratur dikelola

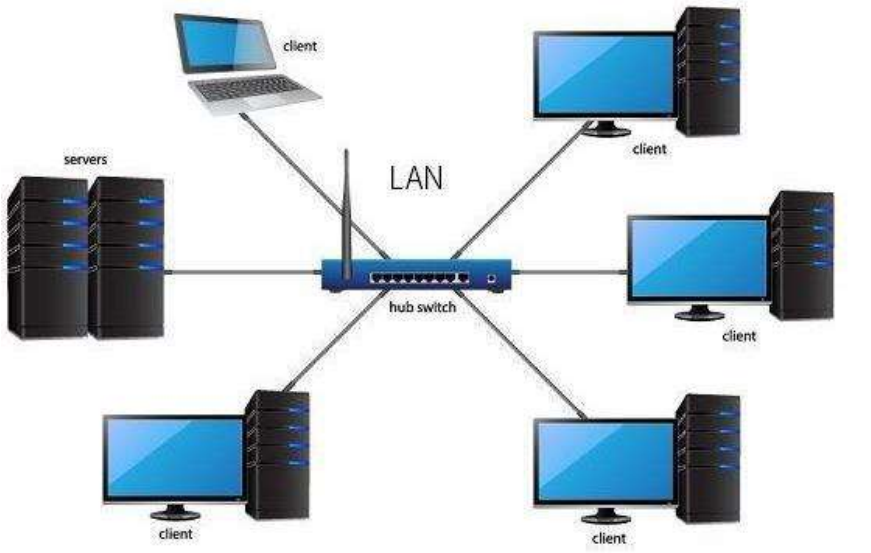
sehingga jaringan tersebut dapat digunakan sesuai dengan manajemen jaringan (Asnawi, 2018).

Berdasarkan pengertian jaringan menurut para ahli maka dapat disimpulkan jaringan adalah sistem yang melibatkan pengolahan, pengaturan dan perincian yang bertujuan untuk mengelola setiap elemen yang ada dalam jaringan secara teratur yang bertujuan untuk terbentuknya manajemen jaringan dan jaringan juga merupakan gabungan antara dua perangakat yaitu perangkat keras *(hardware)* dan perangkat lunak *(software)* serta dapat melakukan manajemen database secara bersama-sama untuk mencapai tujuan pengelolaan jaringan.

2.1.2 Jenis jenis jaringan

Jaringan komputer merupakan sebuah jaringan yang terdiri dari dua perangkat komputer yang saling terhubung sehingga dapat berbagi informasi, mengirim file dan bertukar data. Menurut (Samsumar & Hadi, 2018) dalam penelitiannya jaringan komputer dikelompokan menjadi 3 bagian berdasarkan ruang cakupannya , yaitu sebagai berikut:

1. *Local Area Network (LAN)*

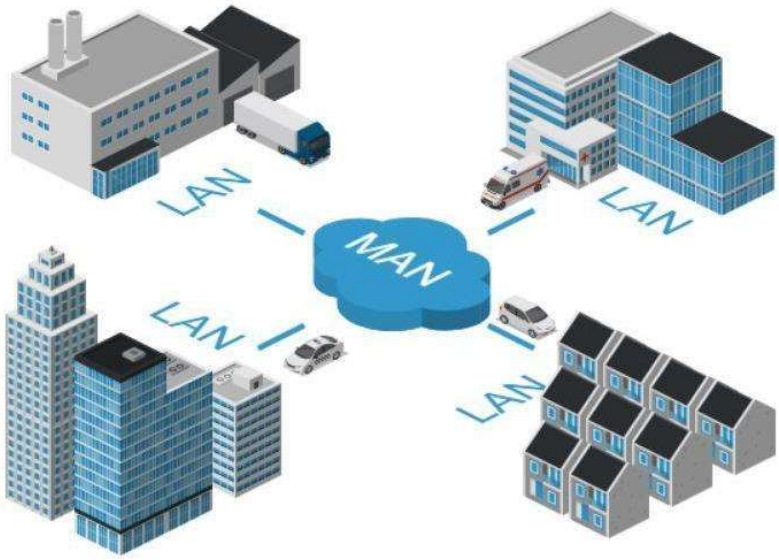


Gambar 2.1 *Local Area Network*
Sumber : (Samsumar & Hadi, 2018)

Local Area Network (LAN) adalah jenis jaringan yang berskala kecil yang mana ruang lingkupnya hanya didalam ruangan saja atau dalam gedung saja, dalam membangun jaringan LAN minimal harus mempunyai 2 buah komputer yang telah terinstall *lan card*. Biasanya jenis jaringan LAN ini sering dijumpai pada sekolah, rumah dan perkantoran, terdapat kelebihan menggunakan jaringan LAN sebagai berikut :

1. Jaringan LAN dapat dikelola pada jaringan yang lebih besar seperti WAN *(Wide Area Network)*.
2. Berbagi data atau file dapat dilakukan dengan cepat dan mudah.
3. Tingkat kerusakan pada jaringan LAN cendrung lebih rendah.

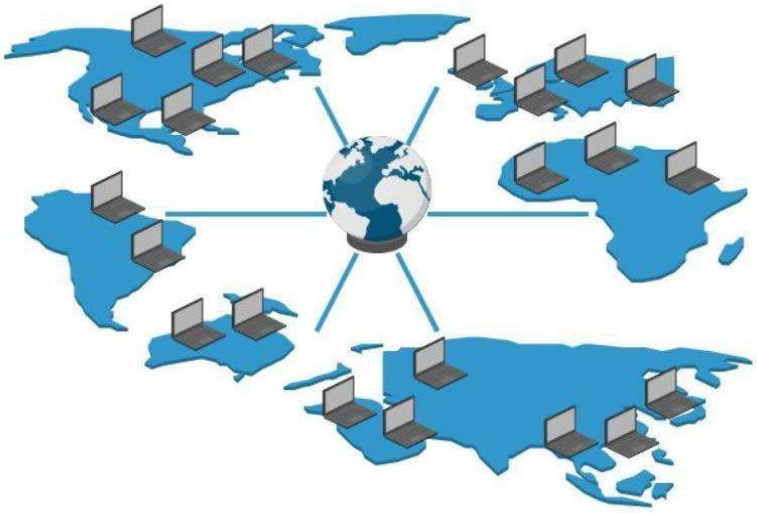
2. *Metropolitan Area Network (MAN)*



Gambar 2.2 *Metropolitan Area Network*
Sumber : (Samsumar & Hadi, 2018)

Metropolitan Area Network (MAN) merupakan pengembangan dari jaringan LAN yang mana ruang cakupanya itu sudah antar kota, jarak jaringan ini akan bergantung pada jangkauan panjang kabel yang digunakan, biasanya jaringan ini digunakan dalam satu kota dan antar kampus.

3. *Wide Area Network (WAN)*



Gambar 2.3 *Wide Area Network*
Sumber : (Samsumar & Hadi, 2018)

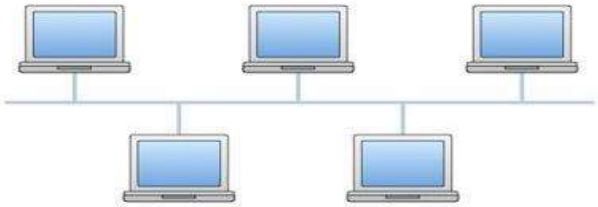
Merupakan sebuah jaringan yang cakupan jaringannya sudah luas dan jaringan wan ini juga gabungan dari jaringan LAN dan MAN. Jaringan wan ini telah memenuhi untuk kebutuhan public seperti jaringan pada perbankan, WAN menggunakan protokol internet NSP *(Network Service Provider)*. Kelebihan jaringan WAN antara lain sebagai berikut :

1. Jaringan WAN telah dapat mengirimkan sebuah file dalam jarak yang cukup jauh dengan efisien diseluruh lokasi yang terhubung.
2. Keamanan jaringan WAN telah menggunakan keamanan lanjutan seperti VPN *(Virtual Private Network)* untuk mengenkripsi data yang dikirim melalui jaringan.

2.1.3 Topologi Jaringan

Menurut (Samsumar & Hadi, 2018) Topologi secara umum dibagi menjadi 6 bagian, diantaranya sebagai berikut :

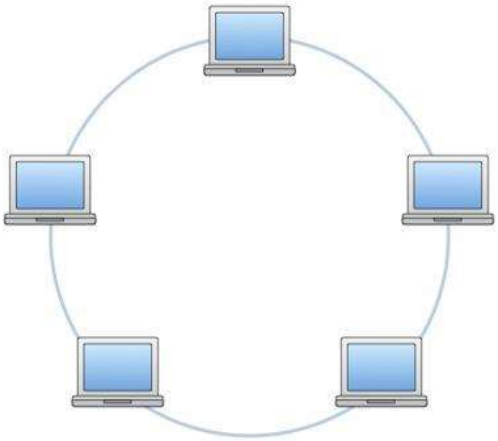
1. Topologi Bus



Gambar 2.4 *Topologi Bus*
Sumber : (Samsumar & Hadi, 2018)

Topologi bus merupakan sebuah topologi jaringan yang paling sederhana yang mana hanya menggunakan jenis kabel *coaxial* sepanjang node *client* dan konektor, topologi jenis ini hanya menggunakan sebuah jenis kabel utama sebagai tulang punggung *(backbone).* Keuntungan topologi ini adalah sebagai berikut : Karena hanya menggunakan satu jenis kabel maka topologi ini sangat mudah dikembangkan. Kerugian deteksi dan isolasi kesalahannya sangat kecil karena jalur lalu lintas yang padat yang menyebabkan apabila satu client rusak maka akan mempengaruhi jaringan yang lain.

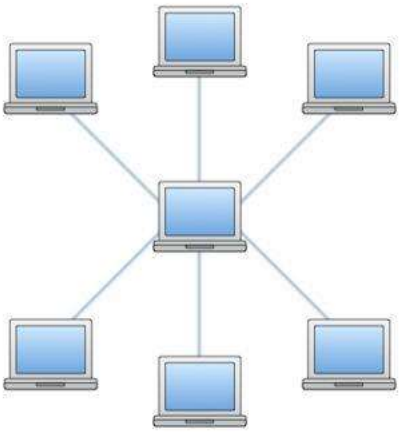
2. Topologi Ring



Gambar 2.5 *Topologi Ring*
Sumber : (Samsumar & Hadi, 2018)

Topologi Ring adalah salah satu jenis topologi jaringan komputer yang menghubungkan setiap perangkat secara langsung dengan dua perangkat lainnya sehingga membentuk sebuah cincin (lingkaran). Dimana data akan mengalir dalam satu arah melalui setiap perangkat dalam bentuk sinyal yang bergerak searah jarum jam atau berlawanan dengan arah jarum jam.

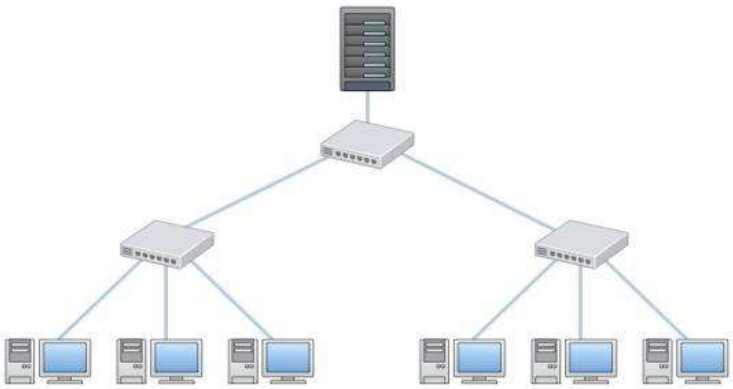
3. Topologi Star



Gambar 2.6 *Topologi Star*
Sumber : (Samsumar & Hadi, 2018)

Topologi star adalah salah satu jenis topologi jaringan komputer yang memiliki pusat distribusi atau simpul pusat *(hub/switch)* yang menghubungkan semua perangkat dalam jaringan secara langsung. Setiap perangkat dalam jaringan terhubung ke simpul pusat melalui kabel tunggal, sehingga membentuk struktur seperti bintang. Semua data yang dikirimkan dari satu perangkat akan dikirimkan terlebih dahulu ke simpul pusat sebelum diarahkan ke perangkat tujuan. Topologi jenis ini merupakan jenis topologi yang paling *fleksibel* karena setiap *client* tidak harus menunggu perintah dari *server* dan ketika ada penambahan ataupun pengurangan topologi ini tidak akan mengganggu bagian jaringan lain kerugian hanya saja akan memboros banyak kabel.

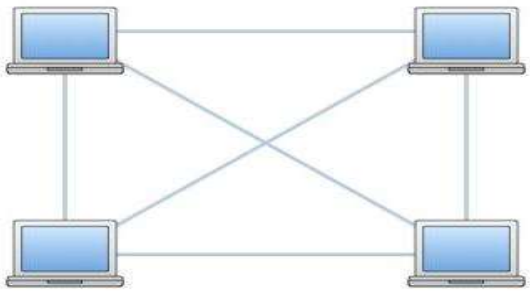
4. Topologi Tree



Gambar 2.7 *Topologi Tree*
Sumber : (Samsumar & Hadi, 2018)

Topologi Tree juga dikenal dengan topologi hierarki, yang mana topologi ini gabungan dari topologi bintang *(star)* dan topologi bus pada topologi ini setiap node akan bergantung pada node yang ada diatasnya, penerapan topologi jenis ini bisa dilakukan perusahaan yang mana dalam pengontrolan jaringan akan hanya dilakukan pada satu pusat saja.

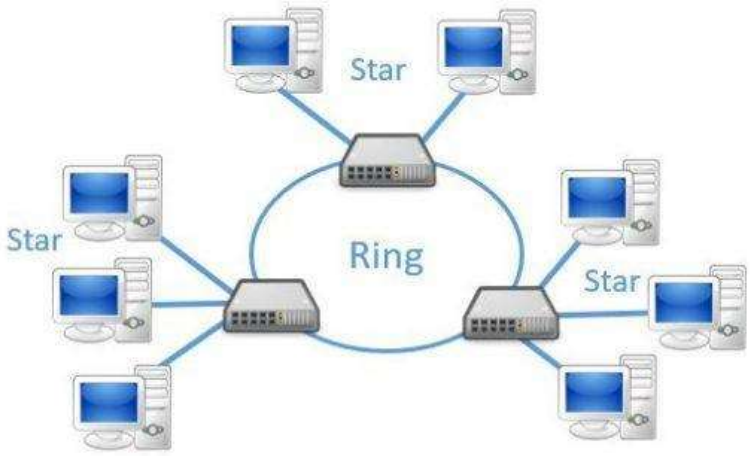
5. Topologi Mesh



Gambar 2.8 *Topologi Mesh*
Sumber : (Samsumar & Hadi, 2018)

Topologi yang setiap komputernya saling terkoneksi satu sama lain, penerapan topologi jenis ini biasanya pada jaringan WAN.

6. Topologi Hybrid



Gambar 2.9 *Topologi Hybrid*
Sumber : (Samsumar & Hadi, 2018)

Topologi Hybrid adalah kombinasi dari dua atau lebih jenis topologi jaringan yang berbeda dalam satu jaringan yang sama. Ketika digabungkan dua atau lebih topologi maka dia akan membentuk sebuah *topologi hybrid*.

2.1.4 Jenis serangan pada jaringan komputer

Di Sebuah perusahaan tentunya dalam melakukan serangkaian pekerjaan tentunya menggunakan jaringan dalam berbagi data informasi, tidak dapat dipungkiri lagi ini akan menjadi area yang sangat rentan terhadap berbagai jenis serangan. Dengan diciptakan perangkat yang dapat membatasi penggunaan jaringan serta memberikan keamanan pada jaringan yang terhubung pada perangkat tersebut

(Network Switch), akan tetapi dengan menggunakan jaringan *nirkabel* keamanan tersebut masih bisa di susupi oleh pihak secara tidak sah. Dua model jenis serangan pada jaringan komputer yakni serangan aktif dengan menggunkaan *signal jammer* untuk mengganggu transmisi data dan model *pasif* yang berfokus pada penyadapan data (Prakasa, 2020).

Menurut (Prakasa, 2020) dalam penelitian yang dilakukan semakin berkembangnya kemajuan teknologi maka juga akan diikuti juga dengan perkembangan teknik penyerangan terhadap teknologi tersebut. Dapat dilihat dari berbagai serangan yang belakangan sering terjadi diantaranya sernagan *malware* dimana seseorang memasukan sebuah virus seperti *(worm, trojan, ransomware dan spyware)* dan serangan *phising* dengan upaya untuk mendapatkan informasi sensitive seperti kata sandi dan nomor kartu kredit. Beberapa bentuk ancaman penyerangan yang sering terjadi dalam sistem keamanan jaringan mikrotik, yaitu :

2.1.4.1 Brute Force

Algoritma *brute force* adalah sebuah metode pencarian dan pemecahan masalah dengan mencoba semua kemungkinan kombinasi yang dilakukan secara berurutan untuk mencari solusi atau jawaban yang benar. Dalam konteks jaringan komputer, algoritma *brute force* digunakan oleh peretas dalam menebak atau untuk mendapatkan kata sandi atau kunci *enkripsi* yang tidak diketahui (Mulyanto et al., 2022).

Menurut (Syaifuddin et al., 2018) *Brute force* adalah sebuah upaya dalam menerka dan menebak kemungkinan kode atau *password* yang disembunyikan dan dengan tujuan tertentu, dalam melakukan *brute foce.* Dapat disimpulkan bahwa

sebuah teknik yang dilakukan dengan cara menebak password dan mengkombinasikan semua kemungkinan password dengan menggunakan beberapa kemungkinan karakter, meskipun alqoritma ini berhasil akan tetapi dalam melakukan serangan *brute force*, akan memakan waktu yang lama dikarenakan peretas akan menerka atau menebak kemungkinan kode yang di enkripsi secara berurutan. Tentunya ini tidak efektif untuk dilakukan.

2.1.4.2 Port Scanning

Port scanning merupakan sebuah teknik *hacking* yang dilakukan oleh pihak tertentu yang mana melakukan pembobolan terhadap website atau web server melalui *port* yang terbuka dan di eksekusi (Mulyanto et al., 2022). Dengan kata lain *port scanning* ini adalah sebuah teknik yang digunakan oleh pengguna untuk mencari dan mengidentifikasi port yang terbuka pada sistem komputer dan perangkat jaringan. Dalam dunia *cyber port scanning* sering digunakan oleh seorang hacker dalam mencari celah keamanan dalam sistem yang dapat dimasuki.

2.1.4.3 Secure Shell (SSH)

SSH (Secure Shell) merupakan protokol keamanan dan metode yang digunakan untuk mengamankan akses ke perangkat jaringan komputer dari jarak jauh. Pada SSH terdapat fitur yang disediakan yakni *enkripsi data, autentifikasi*, dan keamanan lainya yang digunakan dalam melindungi informasi ketika berbagi informasi pada perangkat yang terhubung yang mana ini memungkinkan pengguna untuk mengakses, mengelola dan mengendalikan perangkat atau server dari jauh dengan aman (Desmira & Wiryadinata, 2022b).

Port SSH (Secure Shell) begitu populer di kalangan perusahan besar di indonesia karena begitu banyaknya perusahaan di Indonesia menggunakannya dalam keamanan jaringan komputer mereka, perbandingan penggunaan *port SSH* dalam penelitian ini yakni menggunakan metode *port knocking.* Adapun kelebihan dapat dilakukan dengan menggunakan SSH *(Secure Shell)* diantaranya pengguna dapat mengakses sebuah perangkat jaringan atau server dari lokasi yang jauh dengan menggunakan koneksi SSH dan pengguna juga dapat membentuk sebuah *"tunnel"* atau jalur yang aman antar dua perangkat dalam berbagi informasi (Desmira & Wiryadinata, 2022a).

2.1.5 Serangan Terhadap Perangkat keras *(Hardware)*

Serangan terhadap perangkat keras adalah upaya yang dilakukan oleh penyerang untuk merusak, meyabotase atau mendapatkan akses yang tidak sah ke perangkat keras fisik yang digunakan dalam sistem komputer atau jaringan. Serangan terhadap perangkat keras merupakan ancaman yang serius karena dapat menyebabkan kerusakan fisik, kegagalan perangkat dan pelanggaran keamanan data. Dalam penelitian yang dilakukan oleh Alves & Moris yang dikutip oleh (Prakasa, 2020) Menjelaskan Serangan *malware* terhadap perangkat keras, juga dikenal sebagai "*malware* berbasis perangkat keras" atau "*malware* tingkat rendah", adalah jenis serangan yang menargetkan tingkat perangkat keras fisik dalam sistem komputer. *Malware* semacam ini dapat menyusup ke dalam komponen perangkat keras, seperti BIOS *(Basic Input/Output System), firmware*, atau bagian lain dari *hardware,* dan menyebabkan kerusakan atau merusak operasi perangkat keras tersebut. Ini adalah jenis serangan yang lebih canggih dan jarang terjadi daripada

malware yang biasa kita kenal (seperti virus atau *worm* yang beroperasi di tingkat perangkat lunak).

2.1.6 Serangan Terhadap Perangkat Lunak *(Software)*

Terdapat beberapa serangan terhadap perangkat lunak *(software)* dikelompokan sebagai berikut:

1. Serangan terhadap sistem operasi

   Menurut (Prakasa, 2020) serangan terhadap sistem informasi sebagian besar menagetkan memori atau dikenal dengan istilah *memory-corruption vulnerability*, dan serangan *rowhammer* yang menyerang DRAM sehingga dapat mengakibatkan ketidakstabilan sistem operasi *(crash*) atau bahkan mengakibatkan *privileges escalation*. Dalam dibuktikan jika melakukan akses ke alamat memori yang terlarang dapat mengakibatkan pengguna bisa menjalankan aplikasi *setar administrator (root).*

   Ancaman serangan terhadap keamanan sistem operasi dapat dikatakan sebagai *CLKScrew* dalam istilah lainya dimana seorang *hacker* bertindak dengan cara mengganggu sistem kelistrikan melalui *software*. Terdapat beberapa serangan terhadap keamanan sistem operasi yang pernah terjadi diantaranya serangan yang terjadi pada sistem operasi pada tahun 2017 yang disebut serangan *WannaCry* adalah jenis serangan *ransomware* yang menyerang ribuan organisasi diseluruh dunia yang mana serangan ini mengeksploitasi kerentanan pada sistem operasi windows yang belum diperbaharui, juga termasuk windows XP yang sudah tidak didukung dan

serangan *NotPetya* pada tahun 2017*, NotPetya* merupakan jenis serangan *malware* yang menargetkan pada perusahan-perusahan besar diseluruh dunia yang mana serangan ini menggunakan kerentanan pada perangkat lunak akuntansi ukraina untuk menyebarkan virus dan merusak sistem.

2. Serangan terhadap layanan sistem operasi *(services)*

Pada layanan sistem operasi (servis) terdapat sebuah layanan yang berfungsi untuk memberikan layanan terhadap sistem, ancaman terhadap layanan sistem layanan yakni *Distributed Denial of Services (DDoS)* (Prajapati et al., 2019).

Tujuan dari serangan ini adalah membuat kemacetan di layanan *service* (missal HTTP) sehingga tidak dapat melayani permintaan dari pengguna lainnya dan website tidak dapat diakses. Serangan lain yang pernah terjadi adalah serangan pada *secure shell (*ssh), Teknik yang dilakukan untuk menyerang SSH adalah dengan melakukan *brute-force attack.* Teknik ini merupakan teknik yang sudah cukup lama digunakan dan dinilai kurang efektif, namun dengan adanya *botnet* teknik ini jauh lebih efektif dibandingkan dengan teknik sebelumnya. *Botnet* biasanya digunakan untuk melakukan serangan *cyber* termasuk serangan DDoS *(Distributed Denial of Service), spamming* dan pencurian data.

3. Serangan terhadap aplikasi

Serangan terhadap aplikasi adalah upaya yang dilakukan oleh penyerang untuk mengeksploitasi kerentanan dalam aplikasi perangkat lunak guna mendapatkan akses tidak sah, mencuri data, menyebabkan kerusakan, atau melakukan tindakan berbahaya lainnya. Aplikasi perangkat lunak adalah sasaran yang menarik bagi penyerang karena seringkali mengandung kerentanan yang dapat dimanfaatkan untuk memasuki sistem secara tidak sah (Prakasa, 2020).

2.1.7 Serangan Terhadap Basis Data

Serangan terhadap basis data adalah upaya yang dilakukan oleh penyerang untuk mengeksploitasi kerentanan dalam sistem basis data guna mendapatkan akses tidak sah, mencuri data sensitif, merusak atau mengubah data, atau menyebabkan gangguan pada operasi basis data. Basis data merupakan kumpulan data yang disimpan dalam sistem yang terstruktur, dan serangan terhadapnya dapat menyebabkan kerugian yang signifikan bagi organisasi atau individu yang terkena dampaknya (Prakasa, 2020).

2.2 Teori Khusus

2.2.1 Keamanan Jaringan

Keamanan jaringan merupakan suatu proses yang berkaitan dengan upaya untuk melakukan pencegahan, mengidentifikasi ancaman serangan keamanan jaringan serta menghentikan segala macam upaya yang dilakukan oleh penyusup untuk dapat masuk kedalam jaringan komputer serta sistem jaringan

Keamanan jaringan *(Network Security)* merupakan segala bentuk aktivitas yang dilakukan dalam mengamankan sebuah jaringan *(Network),* terlebih untuk melindungi *usability, availability, reliability, integrity* dan *safety* dari jaringan dan data. Tujuan dari *network security* adalah bagaimana upaya dalam mencegah dan menghentikan ancaman serangan *(threats)* agar tidak masuk dan menyebar di jaringan kita, yang mana untuk keamanan jaringan mencangkup dari perangkat keras dan perangkat lunak (Fauzan & Purwanto, 2021).

Keamanan Jaringan komputer merupakan suatu proses dalam mencegah dan mengidentifikasi pengguna yang tidak berhak dalam mengakses jaringan komputer, untuk mengantisipasi dan mencegah ancaman keamanan jaringan komputer maka diperlukannya suatu langkah langkah dalam pencegahannya supaya penyusup tidak dapat masuk kedalam sistem jaringan.

Menurut (Amien, 2020) ada tiga aspek dalam keamanan jaringan antara lain sebagai berikut :

1. *Confidentiality*

   Kerahasian *(Confidentiality)* menunjukan bahwa sebuah informasi dan data hanya dapat diakses oleh pihak yang diberi izin untuk mengakses sebuah keamanan jaringan. Aspek kerahasian bertujuan untuk melindungi data dari akses yang tidak sah atau penyebaran yang tidak diizinkan.

2. *Integrity*

   Integrity yaitu bagaimana seorang pengguna dapat memastikan suatu informasi atau data didalam jaringan tetap utuh, tidak diubah atau dimanipulasi secara tidak sah selama pengiriman ataupun penyimpanan.

Aspek dari *integrity* ini bertujuan untuk melindungi sebuah data dari modifikasi yang tidak sah, penyisipan data palsu atau perubahan data yang tidak di inginkan yang akan menyebabkan kerugian atau kerusakan.

3. *Availability*

Ketersediaan *(Availability)* dalam jaringan mengacu pada kemampuan sebuah sistem atau layanan jaringan untuk dapat beroperasi, aktif, dan dapat diakses oleh pengguna secara sah dan konsisten tanpa gangguan. Aspek *availability* ini mengacu pada pentingnya menjaga ketesediaan sebuah layanan dan sumber daya jaringan agar dapat diakses dan digunakan sesuai dengan kebutuhan.

2.2.2 Mikrotik

Gambar 2.10 Mikrotik
Sumber : (Ardianto, 2020)

Mikrotik merupakan sebuah sistem aplikasi router, yang di kenalkan dengan nama *mikrotik routerOs* yang dapat kita install di setiap komputer, namun tidak seperti sistem operasi sistem router lainya yang mana hanya bisa di install pada

hardware tertentu saja, kelebihan dari router ini sendiri adalah mudah dikonfigurasikan dan harga yang diberikan juga bervariasi sesuai dengan kebutuhan penggunanya. Serta mikrotik ini berfungsi dalam membagi koneksi internet ke beberapa pengguna (Ardianto, 2020).

Mikrotik merupakan sebuah perangkat jaringan komputer yang berupa *hardware* dan *software* yang berfungsi sebagai router, sebagai alat untuk *filtering, switching,* pengaturan *bandwidth,* dan *wireless acces point* yang berguna untuk *client* maupun *server* sehingga sangat cocok untuk *routing* digunakan jaringan perusahaan bahkan juga dapat digunakan oleh ISP dan *provider hotspot* (Hidayat et al., 2022). Router mikrotik adalah satu solusi dari masalah keamanan jaringan komputer dikarenakan fitur fitur yang terdapat pada router mikrotik dapat digunakan dalam management 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 (Tasanah Assakur et al., 2020). Beberapa pandangan para ahli mengenai mikrotik

Menurut Herlambang yang dikutip oleh (Asnawi, 2018) mikrotik Router OS adalah *Operating System* (OS) yang dirancang secara khusus sebagai jaringan router *(network router),* menggunakan *personal computer* yang dijadikan sebagai *network router* dengan cara memasangkan mikrotik router OS.

Menurut (Asnawi, 2018) awalnya mikrotik di kembangkan disuatu daerah yang bernama Latvia, yang dikembangkan oleh Jhon Trully dan anies, dengan di kembangkan nya mikrotik ini akan membuat router dapat diakses serta dapat

dikembangkan serta digunakan di seluruh dunia prinsip inilah yang ditanamkan oleh *john trully* dan *anies.*

2.2.3 Keamanan Sistem Jaringan

Keamanan sistem jaringan menurut merupakan segala bentuk upaya pencegahan serta mengidentifikasi pengguna jaringan yang tidak sah (penyusup) dalam megakses jaringan. Sistem keamanan jaringan adalah kunci dalam menjaga kestabilan dan evektifitas jaringan (Wicaksono, 2022).

Dalam keamanan jaringan sistem lebih merujuk pada kumpulan perangkat keras, perangkat lunak, protokol, kebijakan dan prosedur yang digunakan dalam upaya melindungi jaringan komputer dari ancamaan keamanan serta menjaga integritas,kerahasian dan ketersediaan data, dalam keamanan jaringan terdapat beberapa elemen yang saling bekerja sama dalam melindungi jaringan dari ancaman serangan yang dapat merugikan. Terdapat beberapa pemahaman tentang sistem dalam sudut pandang para ahli yaitu sebagai berikut :

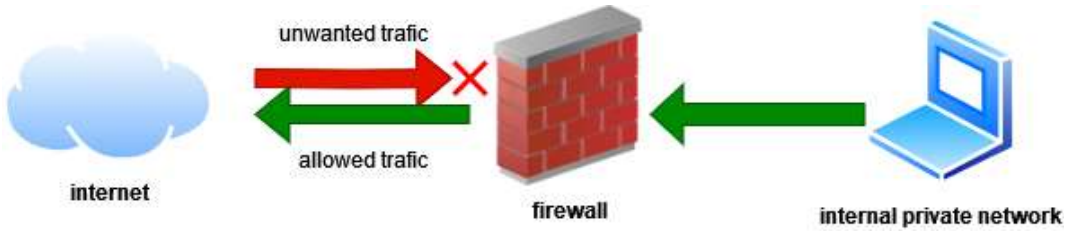
1. Menurut (Saputra et al., 2019) dalam Arifin Rahman menjelaskan sistem dalam kamus *Webster New Collegiate Dictionary* berpendapat bahwa sistem berasal dari bahasa Yunani yang mana “syn” dan “Histana” yang diartikan menempatkan bersama.
2. Menurut (Saputra et al., 2019) dalam Ludwig Von Bertallanffy sistem adalah kesatuan yang komplek yang terdiri dari elemen-elemen yang saling berinteraksi secara saling bergantungansehingga membentuk satu kesatuan yang fungsional.

3. Menurut (Basuki, 2019) dalam Fagen Dan A.HAll menjelaskan sistem merupakan suatu kumpulan objek yang meliputi hubungan antara suatu objek dengan objek lain serta hubungan dengan sifat yang mereka miliki.

2.2.4 Firewall Filtering

Firewall merupakan jenis keamanan jaringan yang berguna untuk memfilter serta mengontrol lalu lintas jaringan yang masuk dan memblokir paket data yang dianggap mencurigakan, *firewall* juga digunakan untuk melindungi, membatasi dan menolak jaringan pribadi dengan jaringan luar yang terdeteksi dapat mengancam keamanan jaringan (Wicaksono, 2022). Jika ada pihak yang mencoba untuk melakukan pengaksesan maka sistem *firewall* akan otomatis memblokir pihak yang tidak bersangkutan tersebut oleh *firewall,* sistem kerja dari firewall sendiri akan mengikuti kebijakan yang dibuat oleh administrator jaringan.

Sistem kerja dari firewall menggunakan cara *studying the deployment rule-set,* dimana *the rule-set* dibuat dengan sedemikian rupa supaya setiap data yang masuk akan diperiksa oleh *firewall* dan dilakukan analisa setiap data yang keluar dengan sistem *rule-set*. *Filter firewall* mempunyai suatu ketentuan yang dibuat *rule-set* yang mana untuk dapat mengatur lalu lintas dari paket tersebut sebelum paket tersebut di izinkan masuk, *firewall filtering* juga dapat memblokir lalu lintas data yang masuk jika terdapat data yang mencurigakan. *The Rule-set* untuk *firewall* tersebut akan dikonversikan menjadi sebuah kode tertentu yang digunakan pada *firewall* sehingga nantinya perangkat komputer dapat mengeksekusi sesuai dengan perintah yang ada (Khadafi et al., 2019).



Gambar 2.11 Cara kerja *Firewall*
Sumber : (Data Penelitian, 2023)

Firewall merupakan sebuah bentuk pengamanan yang penting, akan tetapi pertahanan keamanan jaringan yang efektif juga memerlukan kombinasi dari berbagai teknologi serta praktik keamanan yang berlapis lapisuntuk melindungi jaringan *firewall* dapat dibedakan menjadi dua *hardware* dan *software* berikut penjelasannya :

1. *Firewall* berbasis *hardware*

Firewall berbasis hardware merupakan piranti perangkat keras yang berada dalam perangkat jaringan komputer seperti router. *Firewall* berbasis perangkat keras merupakan jenis *firewall* yang diimplementasikan dengan menggunkan perangkat keras khusus yang dirancang khusus untuk menyaring dan mengamankan lalu lintas jaringan. *Firewall* berbasis *hardware* memiliki perangkat fisik yang berdiri sendiri dan berfungsi sebagai pertahanan sendiri dalam keamanan jaringan (Gregorius Hendita Artha Kusuma, 2022).

2. *Firewall* berbasis *software*

Firewall berbasis perangkat lunak adalah jenis firewall yang diimplementasikan dengan menggunakan perangkat lunak yang bejalan di atas sistem operasi komputer yang mana fungsi dari *firewall* berbasis perangkat lunak

untuk menyaring serta mengamankan lalu lintas jaringan. *Firewall* berbasis *software* biasanya melindungi *trafik inbound* dan juga *outbound*, selain itu juga dapat menghindarkan sistem dari berbagai macam virus seperti *trojan* dan *worm* (Gregorius Hendita Artha Kusuma, 2022).

2.2.5 Port Knocking

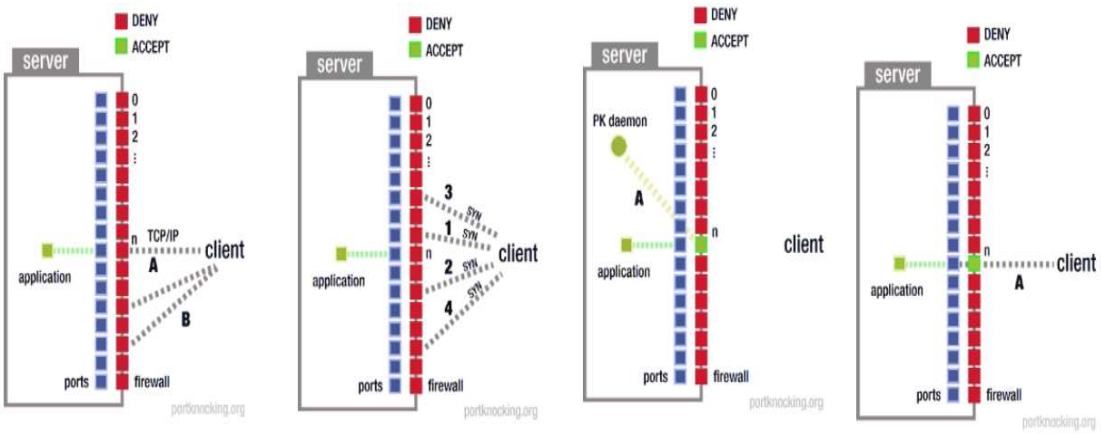
Menurut (Mulyanto et al., 2021) *Port Knocking* Merupakan suatu metode yang digunakan dalam upaya meningkatkan keamanan pada lapisan utama pada jaringan, serta memberikan perlindungan terhadap keamanan jaringan dari ancaman serangan jaringan seperti serangan *scripts kiddies* dan serangan *port scanning.* Dan memberikan hak akses terhadap pengguna untuk mengakses port yang dibuka dan menutup port kembali dan menggunakan *firewall* untuk menghapus *rule* yang pernah di eksekusi sebelumnya.

Menurut (Saputro et al., 2020) *port knocking* merupakan sebuah teknik keamanan jairngan yang digunakan untuk menyembunyikan layanan jaringan dari pemeriksaan secara rutin yang dilakukan oleh penyusup atau penyerang. Teknik tersebut bertujuan untuk mengaktifkan akses ke port tertentu setelah urutan koneksi yang tepat ke port -port dengan pola yang telah ditentukan sebelumnya sehingga ini mengharuskan pengguna untuk selalu memberikan keamanan ekstra terhadap port yang terbuka sehingga dapat mencegah terjadinya pencurian data.

Port knocking merupakan suatu metode yang digunakan dalam mengotorisasi sebuah pengguna berdasarkan *firewall* untuk dapat melakukan komunikasi melalui port, yang mana metode *port knocking* ini menggunakan sistem autentifikasi dalam pengiriman sebuah data atau file, dimana informasi yang

dikirimkan akan dikodekan bahkan di enkripsi sesuai dengan urutan nomor port, urutan ini disebut juga dengan *knock* (ketukan).

Alur kerja dari *port knocking* sendiri dapat dijelaskan berdasarkan gambar berikut, pada gambar 2.12 sebagaimana diketahui 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 klien dapat melakukan transfer data (Khadafi et al., 2019).



Gambar 2.12 Proses *Port Knocking*
Sumber : (Khadafi et al., 2019)

2.2.6 Telegram Bot

Telegram merupakan sebuah aplikasi bersifat *open source* yang dapat kita download melalui playstore dengan gratis telegram lebih berfokus pada kecepatan dan keamanan. Telegram adalah sebuah apliksi instan yang popular yang dapat menyediakan layanan pesan teks, panggilan suara, panggilan video serta berbagi file, didalam telegram kita juga dapat membuat group dengan beranggotakan sebanyak 5000 orang atau bisa juga *channel broadcasting* untuk pengguna secara terbatas (Fernando et al., 2020).

Beberapa fitur yang ditawarkan oleh telegram messenger sebagai berikut :

1. Menyediakan keamanan pesan dengan dienkripsi end-to-end dan fitur penghapusan pesan otomatis.
2. Dapat mengatur penghapusan pesan dengan waktu yang ditentukan.
3. Menyimpan file dalam *cloud.*
4. Telegram dapat digunakan diberbagai platfrom seperti android, Ios, windows, macOS dan versi web.

Menurut (Fernando et al., 2020) terdapat dua jenis API yang dapat digunakan oleh pengembang sebagai berikut :

1. Bot API memungkinkan seorang pengembang untuk dapat menghubungkan Bot ke dalam sistem telegram. Telegram *Bots* merupakan program atau skrip pada komputer yang dijalankan di platfrom telegram dan berfungsi untuk memberikan layanan dan interaksi dengan pengguna lain dalam pesan teks, gambar maupun video.
2. API Telegram memungkinkan pengembang untuk membuat klien telegram yang mereka inginkan. API telegram bersifat *open source* yang mana para pengembang dapat dengan mudah membangun aplikasi di platform telegram.

API *(Application Programming Interface*) merupakan sebuah antarmuka yang memberikan kemudahan bagi pada pengikat, mitra maupun pihak ketiga dalam membangun atau mengembangkan sebuah aplikasi seperti aplikasi Iphone dengan cepat. API Telegram dan Facebook merupakan dua contoh aplikasi yang sudah terkenal, selain itu API juga bermakna sekumpulan perintah, fungsi, protokol, dan objek yang dibuat oleh seorang *programmer* sehingga perangkat tersebut mampu berinteraksi dengan sistem *eksternal.* Adapun manfaat dan kegunaan API secara khusus akan dirasakan oleh *developer* dikarenakan API mampu meningkatkan *efisiensi* waktu, *fleksibilitas*, serta menghemat biaya (Hidayat et al., 2022). Cara kerja API (*Application Programming Interface*) dapat dilihat pada gambar berikut :

Gambar 2.13 Cara kerja API
Sumber : (Hidayat et al., 2022)

Berdasarkan gambar diatas dapat dijelaskan sebagai berikut :

1. Aplikasi akan mengakses API, kemudian API akan merespon dengan melakukan pekerjaan setelah user/pengguna membuka aplikasi
2. API akan mengirimkan permintaan ke *server*, setelah aplikasi berhasil mengakses alamat API, permintaan akan diteruskan ke server pengguna, sehingga API akan memberikan perintah untuk mengirimkan data sesuai *request* yang diminta oleh aplikasi.
3. Server akan merespon permintaan dari API jika permintaan data tersebut sesuai maka server akan mengirimkan data API berupa respon
4. Terkahir API akan memberikan informasi sesuai dengan permintaan aplikasi, seperti informasi yang diberikan ke aplikasi sehingga dapat diakses oleh pengguna

2.3 Software pendukung

1. FileZilla

Gambar 2.14 *FileZilla*
Sumber : (Rafi & Saudi, 2021)

FileZilla merupakan sebuah aplikasi pengiriman file yang bersifat *open source* dengan antar muka yang intuitif serta dengan fitur yang tersedia membuat aplikasi ini mudah digunakan. *Filezilla* juga dapat memungkinkan pengguna untuk *mentransfer file* antar komputer lokal dan server dalam jangkauan jarak jauh secara cepat dan aman.

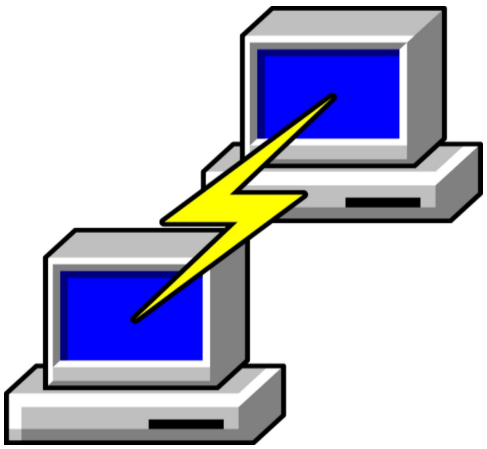
Menurut (Rafi & Saudi, 2021) dalam penelitianya menjelaskan *filezilla* adalah sebuah aplikasi jaringan yang digunakan untuk mengirim file melalui jarigan lokal dan juga internet melalui protokol FTP, yang mana aplikasi ini dikembangkan oleh tim Kosse dengan keunggulan dalam segi kenyamanan dan kecepatan dalam proses *transfer file*. Ada beberapa fitur yang ditawarkan pada aplikasi *FileZilla* diantaranya sebagai berikut:

1. Pada aplikasi *FileZilla* memungkinkan manajemen situs membuat daftar rincian situs FTP dan koneksinya seperti nomor yang dipakai pada port,

portokol yang digunakan serta menggunakan protokol anonim atau regular.

2. *Loq* pesan yang ditampilkan diatas pada atas jendela aplikasi yang berfungsi untuk menampilkan perintah yang dikirim oleh *FileZilla* serta respon yang terima oleh server.
3. Pada aplikasi *FileZilla* tampilan dari file dan folder muncul pada bagian bawah *loq* pesan
4. Antrian transfer data yang ditampilkan dibagian bawah untuk mengetahui status dari pengiriman data apakah aktif atau status pengiriman masih secara *real time.*

2. Putty



Gambar 2.15 *Putty*
Sumber : (Mulyanto et al., 2021)

Putty merupakan sebuah perangkat jaringan komputer yang dapat menghubungkan antara komputer lokal dengan komputer lain dengan jarak yang cukup jauh menggunakan sebuah protokol jaringan seperti *SSH, Telnet, rlogin*, dan

serial. Program pada *putty* lebih banyak digunakan oleh pengguna menengah keatas yang mana dapat duganakan untuk banyak hal yang berhubungan dengan jaringan seperti melakuakan simulasi keamanan jaringan dan memantau keamanan jaringan (Mulyanto et al., 2021).

Konfigurasi pada aplikasi *Putty* dengan cara melakukan pengelolaan perangkat dari jarak jauh melalui konsol yang disediakan oleh protokol SSH atau telnet. Dalam penggunaan aplikasi *putty* pengguna harus memiliki izin yang sah dari pihak yang akan diakses.

3. Zenmap

Gambar 2.16 *Zenmap*
Sumber : (Wicaksono, 2022)

Zenmap merupakan sebuah apliksi grafis yang banyak digunakan untuk memindai jaringan serta menganalisa keamanan jaringan. *Zenmap* merupakan sebuah aplikasi layanan jaringan yang bersifat terbuka dan tersedia untuk berbagai sistem operasi seperti *windows, macOS, dan Linux* (Wicaksono, 2022). Terdapat beberapa fitur pada aplikasi zenmap diantaranya sebagai berikut :

1. Pemindaian jaringan, pengguna dapat melakukan pemindaian ke host atau rentang ip tertentu dan zenmap akan memberikan informasi mengenai terhadap perangkat yang terhubung seperti alamat IP, port yang terbuka, dan layanan yang dijalankan.
2. Pemindaian port dengan aplikasi zenmap pengguna dapat melakukan pemindaian terhadap host dan jaringan tertentu sehingga ini akan membantu pengguna dalam mengidentifikasi potensi kerentanan dan dapat mengambil tindakan untuk mengamankan jaringan.
3. Pemetaan jaringan, ini akan membantu pengguna dalam memahami struktur jaringan dan mengidentifikasi titik rawan yang perlu diperhatikan.
4. Analisa keamanan , dengan aplikasi zenmap pengguna akan dengan mudah dapat menganalisa keamanan jaringan seperti mengetahui celah yang rentan terhadap keamanan dan memberikan informasi untuk untuk pengujian keamanan lebih lanjut.
5. Pelaporan dan penyimpanan hasil, aplikasi zenmap menyediakan fitur untuk menyimpan hasil pemindaian dalam bentuk file tentunya hal ini dapat dimanfaatkan untuk analisa lebih lanjut bagi seorang administrator jaringan.

Dengan adanya beberapa fitur yang terdapat pada aplikasi zenmap tentunya ini akan memberikan kemudahan kepada administrator jaringan dalam mengidentifikasi serta menganalisan dan memperbaiki kerentanan yang ada dalam jaringan.

2.4 Penelitian Terdahulu

Dalam penelitian ini terdapat beberapa artikel jurnal yang menjadi acuan dalam melakukan penelitian ini diantaranya sebagai berikut :

1. Nama pengarang (Fahana et al., 2017). Judul: Pemanfaatan Telegram Sebagai Notifikasi Serangan Untuk Keperluan Forensik Jaringan. Tahun: 2017. E-ISSN : 2579-5341. Forensik jaringan merupakan hal yang sangat penting dalam mengidentifikasi dan mengatasi serangan *cyber* pada jaringan. Penelitian ini meamanfaatkan platfrom telegram dalam memberikan pemberitahuan secara intans dan cepat dan penggunaan *snort* berguna untuk merekam serangan *Distributed Danial of Services* (DDoS) serta *traffic* data yang tersimpan di router yang tersimpan di *log* dan diteruskan ke aplikasi telegram instant *messaging* sebagai notifikasi untuk mengingatkan *administrator*.Telegram tidak hanya dapat digunakan sebagai notifikasi tetapi juga dapat digunakan sebagai tahap forensik jaringan untuk memperkuat bukti adanya penyerangan sebagai proses pengumpulan data untuk keperluan persidangan. Hasil dari penelitian ini akan memberikan keamanan ekstra pada jaringan dikarenakan telegram akan memberikan notifikasi jika terjadi serangan.

2. Nama pengarang (Hidayat et al., 2022). Judul: Bot Monitoring Jaringan Pada BMT Mentari Lampung Timur Menggunakan Mikrotik Dan API Telegram. Tahun: 2022. E-ISSN : 2620-3030, ISSN : 2620-3022. Notifikasi dalam jaringan merupakan hal yang sangat penting dalam memberikan

informasi terkini kepada *administrator* jaringan tentang kondisi server dan router. Metode penelitian yang digunakan dalam penelitian ini menggunakan metode DIO *Network Lifecycle* yang terdiri dari tahapan *design,* implementasi, dan operasi. Hasil dari penelitian menghasilkan BOT monitoring jaringan BMT Mentari Lampung Timur dengan menggunakan mikrotik dan API telegram. Sistem ini akan sangat membantu seorang administrator jaringan dalam mengelola dan memberikan notifikasi saat koneksi ke server BMT ketika mengalami masalah down atau up. Dengan demikian dengan adanya sistem notifikasi ini akan memberikan kemudahan bagi administrator jaringan dalam mengatasi permasalahan jaringan dengan cepat.

3. Nama pengarang (Fernando et al., 2020). Judul: Monitoring Jaringan dan Notifikasi dengan Telegram pada Dinas Komunikasi dan Informatika Kota Padang. Tahun: 2020. ISSN : 2722-4619, E-ISSN : 2722-4600. Monitoring keamanan jaringan pada infrastruktur T.I kota padang dilakukan dengan cara *real-time* dengan memonitoring kesehatan jaringan, status perangkat dan performa sistem. Dengan menggunakan platfrom telegram seorang administrator jaringan dapat menerima pemberitahuan instan tentang gangguan jaringan, masalah server atau ancaman serangan yang dapat terjadi sewaktu waktu. Dengan adanya sistem monitoring dan notifikasi , dinas komunikasi dan informatika kota padang dapat meningkatkan ketersediaan, keandalan, dan kinerja jaringan serta mengurangi waktu

downtime yang dapat mempengaruhi layanan pada sistem. Dengan adanya dukungan dari telegram akan memberikan kemudahan bagi dinas kota padang dalam menghadapi ancaman yang muncul.

4. Nama pengarang (Khadafi et al., 2019). Judul: Implementasi Firewall dan Port Knocking Sebagai Keamanan Data Transfer Pada FTP Server Berbasis Linux Ubuntu Server. Tahun: 2019. ISSN : 2615-6539. FTP (*File Transfer Protocol)* server yang menyediakan layanan transfer file antar mesin komputer dalam sebuah jaringan. FTP beroperasi pada lapisan layer OSI dengan menggunakan port 21 TCP (Transmission Control Protocol) sebagai port standar untuk dapat menginisialisasi koneksi transfer file antar klien dan sever. Untuk dapat meningkatkan keamanan FTP server dapat dengan menggunakan firewall untuk menutup port yang terbukan dan menggunakan port knocking dalam upaya meningkatkan kemanan yang mana ketika pengguna ingin mengakses ke layanan FTP maka di butuhkan otentifikasi. Dari hasil pengujian menunjukan bahwa *rule-set* firewall yang diimplementasikan dapat menyembunyikan informasi mengenai port yang terbuka sehingga dapat mengurangi resiko serangan.

5. Nama pengarang (Iqbal et al., 2020). Judul : Analisa Dan Simulasi Keamanan Jaringan Ubuntu Server Dengan Port Knocking, Honeypot, IpTables, Icmp. Tahun: 2020. E-ISSN : 2615-8442. Keamanan jaringan komputer sangat penting dalam upaya melindungi kerahasian data dan

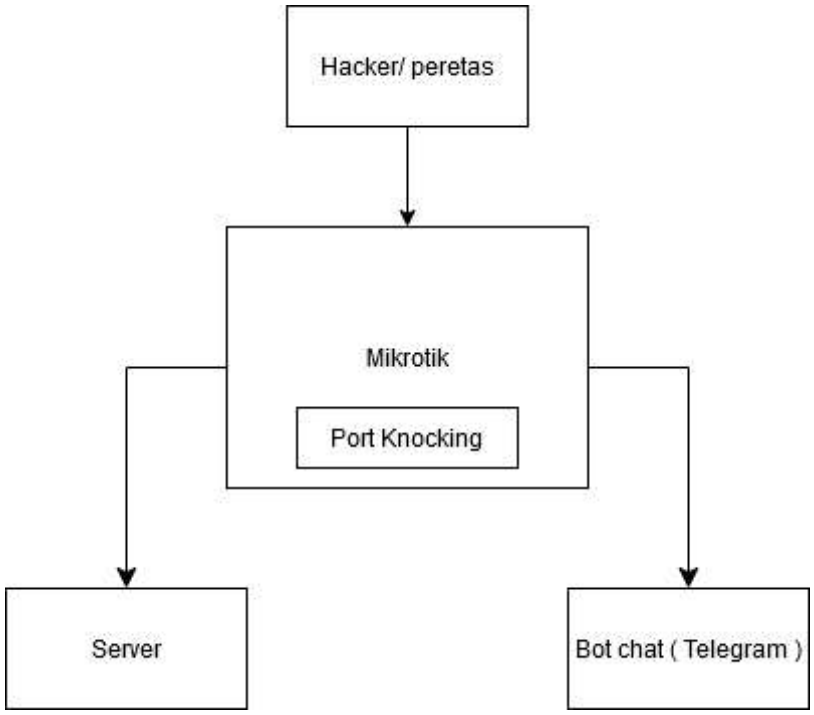
informasi pada server , serangan yang sering terjadi terhadap server seperti *brute force* dan *scan port,* dengan maraknya penyerangan maka server memerlukan perlindungan dengan menggunakan *firewall filtering* tapi ini kurang efektif dikarenakan *firewall* ini akan memblok siapa saja yang mencoba masuk tanpa terkecuali termasuk administrator. Dalam penelitian ini peneliti mengimplementasikan metode *port knocking* yang digabungkan dengan *Honeypot, Iptables* dan *ICMP* untuk meningkatkan keamanan server. IPtables digunakan untuk memfilter aturan port yang akan diizinkan sehingga paket port yang di tentukan saja yang dapat masuk ke server. *Port knocking* untuk memberikan *otentifikasi* dengan memberikan kode rahasia untuk dapat mengakses layanaan ke *server* dan *honeypot* untuk mengalihkan *port service* ke port tiruan yang terbuka untuk mengetahui upaya ancaman serangan yang dilakukan pada *server* serta ICMP digunakan sebagai ping *request* untuk mengakses *server.*

6. Nama pengarang (Saputro et al., 2020). Judul : Demilitarized Zone And Port Knocking Methods For Computer Network Security. Tahun : 2020. E-ISSN 2615-8442. Dengan perkembangan dalam bidang komunikasi tentunya akan merubah seluruh aspek yang bergantung pada jaringan komputer dikarenakan perkembangan yang ada saat ini. Semakin *public* bergantung pada jaringan internet maka akan semakin besar pula potensi serangan terjadi. Teknik keamanan jaringan DMZ *(Demilitarized Zone)* dan *Port knocking* adalah dua pendekatan yang dapat diimplementasikan dalam

jaringan lokal maupun interlokal untuk meningkatkan keamanan server dan router dari serangan potensial. DMZ adalah jaringan yang berada diantara jaringan *internal (inside)* dan jaringan *eksternal (outside)* dan *port knocking* merupakan teknik yang memerlukan pengguna melakukan rangkaian koneksi ke port-port tertentu dengan urutan dan pola tertentu sebelum akses ke server atau router diberikan. Kedua teknik ini dapat memberikan keamanan tambahan pada server utama dan router, terutama dari serangan *DDoS* dan *port scanning.* Dengan menggunakan teknik keamanan ini hal yang harus diperhatikan dan dipertimbangkan yakni pada sisi seperti ruang penyimpanan fisik dan sistem enkripsi password pada server. Keamanan di area *inside* (dalam) juga harus menjadi perhatian utama karena teknik keamanan di DMZ dan *Port knocking* hanya melindungi area *outside* (luar).

2.5 Kerangka pemikiran

Penelitian tentang rancang bangun keamanan jaringan mikrotik menggunakan *firewall filtering* dan *port knocking* dengan notifikasi telegram yang mana menempatkan mikrotik router sebagai *server*, diperlukan suatu kerangka pemikiran mengenai rancang bangun keamanan jaringan supaya suatu perencanaan dapat berjalan dengan baik.



Gambar 2.17 Kerangka pemikiran
Sumber : (Data Penelitian, 2023)

Beberapa tahapan dalam kerangka pemikiran dalam rancang bangun sistem keamanan sebagai berikut :

1. *Hacker /* peretas

   Ketika *hacker* mencoba untuk melakukan *port scanning, brute force* terhadap sistem keamanan jaringan mikrotik maka sistem keamanan jaringan mikrotik akan langsung merespon serangan tersebut dengan mengirimkan notifikasi ke aplikasi telegram

2. Mikrotik

   Pada mikrotik administrator jaringan akan membatasi akses jaringan pada host yang diizinkan saja serta melakukan konfigurasi terhadap port knocking dengan mengubah aturan *firewall* secara dinamis yang mana pengaturan *firewall* ini berguna untuk memblokir akses yang tidak valid

3. Port knocking

   Merupakan tahapan yang penting karena kita harus menentukan port yang dapat digunakan dalam *port knocking* dan *firewall* hanya akan aktif jika pola *port knocking* yang valid terdeteksi. Menggabungkan komponen komponen yang ada dalam merancang keamanan sistem jaringan mikrotik. Membangun keamanan pada jaringan mikrotik dengan menggunakan *firewall filtering* dan *port knocking*, serta menentukan batasan terhadap izin pengaksesan *port knocking* untuk membatasi kemungkinan percobaan mengakses secara illegal atau tidak sah.

4. Server

   Server akan mengidentifikasi host yang dapat diakses melalui port knocking serta membuat skema *port knocking* yang tepat. Memilih dan mengkonfigurasikan perangkat mikrotik sebagai *firewall*

5. Bot chat (Telegram)

   Mengkonfigurasi mikrotik untuk mengirimkan notifikasi melalui telegram menggunakan API bot serta membuat *skrip* yang akan mengirimkan notifikasi ke telegram ketika terjadi akses yang tidak valid terdeteksi. Melakukan pengujian terhadap sistem keamanan untuk memastikan keberhasilan *port knocking* dan notifikasi telegram dan memantau log keamanan mikrotik untuk mendeteksi serangan atau percobaan akses yang mencurigakan.