BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan tergantung pada kecepatan pengaturan jaringan dalam menindak lanjuti sistem saat terjadi gangguan untuk memperkuat keamanan jaringan komputer dapat diterapkan sistem pendeteksi serangan dalam jaringan komputer. *Server* sebagai sarana vital untuk menyimpan *database*, aplikasi dan layanan penting sangat diperlukan sisi keamanannya. Baik dari segi infrastruktur sendiri maupun aplikasi pendukungnya. Diharapkan server terhindar dari hal-hal yang menggangu kinerjanya sehingga pelayanan terhadap client berfungsi secara maksimal maka perlu diterapkan aplikasi *suricata* yang dimana *suricata* ini, IDS (*Intrusion Detection System*) yang dapat mendeteksi ancaman serangan jaringan aktivitas yang dibantu dengan aturan yang adayang memiliki kelebihan ketika serangan terdeteksi maka *Suricata* akan menciptakan sebuah *log* serangan-serangan yang dilakukan, *Suricata* juga dapat melakukan deteksi otomatis pada layer 7 dan bisa juga untuk melakukan eksekusi drop bila ada aktifitas mencurigakan dengan menggunakan *netfilter* yang sudah ada pada *suricata* dan konfigurasi maka dari itu perlu diterapkan aplikasi *suricata* untuk mengamankan server dari serangan dari luar seperti *hacker* dan *tracker*. (Yousufi, 2017).

Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu merupakan salah satu instansi yang menjadikan media *wireless* dan *Wired* sebagai salah satu fasilitas dalam pelayanan masyarakat. Jaringan *wireless* dan *Wired* yang berada di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu ini tergabung menjadi satu dengan jaringan *Local Area Network* yang secara langsung tersambung ke *server* dimana server digunakan untuk mengolah data penting kantor. Sehingga Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu harus lebih memperhatikan segi keamanan jaringannya supaya terhindar dari orang-orang yang tidak bertanggung jawab yang dapat merusak sistem yang ada di instansi tersebut. (Hasil Observasi Pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu).

Berdasarkan hasil observasi pada kantor Dinas Kependudukan dan Pencatatan Sipil Kab.Luwu permasalahan yang dihadapi adalah tidak adanya

sistem keamanan yang berjalan sekarang. Kejadian seperti ini dapat menimbulkan ancaman bagi sistem keamanan *Database serve*r karena suatu serangan ke dalam *server* jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak yang ada di kantor tersebut. Hal ini menjadi landasan untuk menjadikan sistem jaringan komputer yang lebih aman, sehingga pada penelitian ini akan dilakukan analisis keamanan jaringan Database *server* menggunakan *suricata* untuk mengamankan jaringan dari serangan orang-orang yang tidak bertanggung jawab.

Berdasarkan permasalahan di atas penulis mencoba untuk mengangkat judul pada penelitian ini yaitu Analisis Keamanan Jaringan *Database serve*r menggunakan *Suricata* pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu. Sehingga memudahkan administrator jaringan dalam melihat sistem keamanan pada tersebut sudah aman atau tidak dari serangan.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang diatas, maka rumusan masalah yang akan dibahas dalam penelitian ini adalah menganalisis keamanan jaringan *Databas*e *server* menggunakan *Suricata* Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu?

1.3 Tujuan Penelitian

Tujuan yang dicapai dalam penelitian ini adalah untuk menganalisis keamanan jaringan Database *Server* menggunakan *Suricata* Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu.

1.4 Manfaat Penelitian

Adapun manfaat penelitian yang diharapkan setelah penelitian ini dilaksanakan adalah:

1. Dapat menambah pengetahuan dan pemahaman tentang menganalisa keamanan jaringan.
2. Menerapkan ilmu pengetahuan yang telah didapatkan selama menjalani studi perkuliahan
3. Penilitian diharapkan dapat membantu dan memberikan masukan kepada pihak kantor dalam mengamankan jaringannya kedepannya.

4. Dari hasil penelitian ini diharapkan dapat menjadi bahan referensi untuk mahasiswa Universitas Cokroaminoto Palopo terutama bagi peneliti sendiri untuk penelitian selanjutnya.

1.5 Batasan Penelitian

Batasan penelitian merupakan ruang lingkup atau upaya untuk membatasi permasalahan yang diteliti sehingga pembahasan tidak meluas serta penelitian yang dilakukan lebih difokuskan pada masalah yang telah ditentukan. Adapaun batasan penelitian pada penelitian ini adalah:

1. Melakukan analisis perangkat jaringan pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu.
2. Melakukan analisis terhadap keamanan jaringan *Database Server* pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Luwu.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Pustaka

Kajian teori yaitu penjelasan materi-materi yang dikaji dan digunakan untuk merancang aplikasi yang akan dibangun atau kajian materi-materi yang diambil dari buku, internet, dan media cetak lainnya.

1. Analisis

Sari (2020) analisis adalah mempelajari domain permasalahan kemudian menghasilkan spesifikasi dari tingkah laku eksternal yang diamati akan mempengaruhi dan mendukung domain permasalahan. Pernyataan yang lengkap, konsisten dan layak adalah harus dihasilkan dari sebuah analisis untuk menjabarkan karakterisitik oprasional baik fungsi maupun logikanya.

Analisis adalah suatu usaha untuk mengurai suatu masalah atau fokus kajian menjadi bagian-bagian *(decomposition)* sehingga susunan/tatanan bentuk sesuatu yang diurai itu tampak dengan jelas dan karenanya bisa secara lebih terang ditangkap maknanya atau lebih jernih dimengerti duduk perkaranya (Akbar, 2021).

Menurut Spradley (2019), Analisis adalah sebuah kegiatan untuk mencari suatu pola selain itu analisis merupakan cara berpikir yang berkaitan dengan pengujian secara sistematis terhadap sesuatu untuk menentukan bagian, hubungan antar bagian dan hubungannya dengan keseluruhan.

Jadi dapat ditarik kesimpulan bahwa analisis merupakan penguraian suatu pokok secara sistematis dalam menentukan bagian, hubungan antar bagian serta hubungannya secara menyeluruh untuk memperoleh pengertian dan pemahaman yang tepat.

2. Keamanan Jaringan

Sistem keamanan jaringan komputer merupakan suatu cara untuk mencegah atau melindungi dan mengidentifikasi pengguna yang tidak berhak (penyusup) untuk mengakses suatu jaringan guna menghindari berbagai ancaman tanpa adanya hambatan. Menurut Julianto (2021), keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang

tidak sah untuk mengakses setiap bagian dari sistem jaringan komputer. Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun *logic* baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Menurut Akbar (2021), keamanan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Segi-segi keamanan didefinisikan lima poin, yaitu *Confidentiality*, mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang, *Integrity*, mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang, *Availability*, mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan, *Authentication*, mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu, *Nonrepudiation*, Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Jadi dapat ditarik kesimpulan keamanan jaringan merupakan proses untuk mengidentifikasi dan mencegah pengguna yang ilegal dari suatu jaringan komputer.

3. Jaringan Komputer

Menurut Rachmadi (2020), jaringan komputer merupakan penggabungan beberapa teknologi komputer dan komunikasi yang merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya.

Menurut Kumala (2019), jaringan komputer adalah komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protocol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti *printer*, *hardisk*, dan sebagainya. Selain itu jaringan komputer biasa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berbeda diberbagai lokasi yang terdiri dari lebih satu komputer yang saling berhubungan.

Menurut Rachmadi (2020), Jaringan komputer (*computer network*) adalah suatu himpunan terkoneksi sejumlah komputer autonomous. Dalam bahasa yang popular dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *router, switch* dan sebagainya) yang saling terhubung satu sama lain melalui media perantara.

Jadi dari kesimpulan di atas dapat ditarik kesimpulan bahwa, Jaringan Komputer merupakan kumpulan dari perangkat keras dan lunak di dalam suatu sistem yang memiliki aturan tertentu untuk mengatur seluruh anggotanya dalam melakukan aktivitas komunikasi atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*).

4. *Web Server*

Web Server sendiri merupakan wadah untuk menopang sebuah *website* yang berisikan informasi, konten, maupun akun surel atau *email* pengguna, sekaligus sebagai penghubung antara *server* dan *client* dalam pengiriman dan perolehan informasi dan data serta mempercepat dan mengorganisasikannya secara terpusat. *Web server* sendiri menggunakan port 80 dan terdiri dari 2 komponen, yaitu perangkat komputer dan software web server yang dipakai, yang *dimana web server* inilah yang akan menopang *website* yang ditujukan kepada client atau pengguna untuk memberikan dan bertukar informasi. *Web server* juga terdapat beberapa jenis antara lain: *Nginx, Apache Tomcat, Apache Web Server*, *Microsoft Windows Server*, Light HTTP, *Internet Information Service* (IIS), *Sun Java System Web Server*, dan *Zerus Web Server*. Dan terkhusus untuk *Hosting Server*, hanya akan berfokus pada implementasi *web server* yang membahas bagaimana kinerja *web server* yang akan di implementasikan (Aziz & Tampati, 2015).

Menurut Susilo dan Nugraha (2015), *Web server* merupakan sebuah *software* yang memberikan layanan data yang berfungsi untuk menerima permintaan *HTTP* atau *HTTPS* dari klien yang dikenal dengan *Browser web* dan mengirimkan kembali hasilnya dalam bentuk halaman - halaman *web* yang umumnya berbentuk dokumen *HTML*.

Jadi, dari beberapa teori diatas dapat disimpulkan bahwa *Web Server* adalah suatu aplikasi yang memberikan layanan untuk menerima permintaan dari client kemudian dikirimkan kembali hasilnya dalam bentuk *website*.

5. *Database Server*

Database Server adalah sebuah program computer yang menyediakan layanan pengelolaan berupa basis data dan melayani computer atau program aplikasi basis data yang menggunakan model *klien\server.*Susilo dan Nugraha (2015).

6. *Suricata*

Menurut perdana, Munadi dan Irawan (2019), *Suricata* merupakan Network based intrusion detection and prevention system yaitu suatu perangkat lunak yang dapat digunakan untuk mendeteksi dan mencegah (*Detection System and Prevention System*) terhadap lalu lintas sebuah jaringan. *Suricata* adalah IDS *open source* yang dikembangkan oleh *Open Information Security Foundation* (OISF).

Jadi, dari beberapa teori diatas dapat disimpulkan *Suricata* adalah suatu aplikasi yang digunakan untuk mencegah serangan dari luar seperti *snort* yang membutuhkan *firewall*.

7. Jaringan Komputer

Menurut Rachmadi (2020), jaringan komputer merupakan penggabungan beberapa teknologi komputer dan komunikasi yang merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya.

Menurut Kumala (2019), jaringan komputer adalah komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protocol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti *printer*, *hardisk*, dan sebagainya. Selain itu jaringan komputer biasa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berbeda diberbagai lokasi yang terdiri dari lebih satu komputer yang saling berhubungan.

Menurut Rachmadi (2020), Jaringan komputer (*computer network*) adalah suatu himpunan terkoneksi sejumlah komputer autonomous. Dalam bahasa yang popular dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *router*, *switch* dan sebagainya) yang saling terhubung satu sama lain melalui media perantara.

Jadi dari kesimpulan di atas dapat ditarik kesimpulan bahwa, Jaringan Komputer merupakan kumpulan dari perangkat keras dan lunak di dalam suatu sistem yang memiliki aturan tertentu untuk mengatur seluruh anggotanya dalam melakukan aktivitas komunikasi atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*).

a. Klasifikasi Jaringan

Berdasarkan klasifikasinya, tipe jaringan yang biasa digunakan, yaitu:

1) *Local Area Network* (LAN)

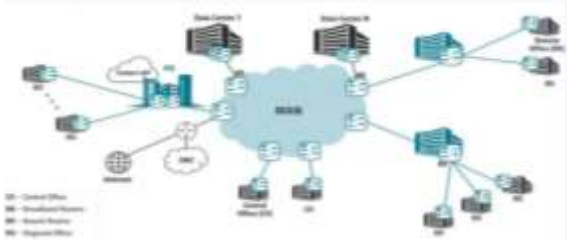
Menurut Rachmadi (2020), LAN adalah singkatan dari *Local Area Network.* LAN terdiri dari beberapa komputer yang terhubung dalam suatu jaringan. Pada jaringan ini, setiap komputer dapat mengakses data dari komputer lain. Selain itu, komputer yang terhubung dalam LAN juga dapat menjalankan *hardware* seperti *printer* dari komputer lain, *chating* dengan pemilik komputer lain, atau main *game* bersama. Jumlah komputer yang terhubung pada LAN relative kecil, misal komputer-komputer di rumah, *warnet*, tempat kos, dan beberapa dalam satu bangunan. Setiap komputer yang terhubung pada LAN mempunyai IP Address yang berbeda.



Gambar 1. Local Area Network
Sumber : Rachmadi (2020)

2) *Metropolitan Area Network* (MAN)

Menurut Rachmadi (2020), *Metropolitan Area Network* adalah jaringan yang lebih luas dari pada LAN. Beberapa LAN yang menjadi satu jaringan juga dapat disebut MAN. MAN biasanya terdapat didalam satu kampus atau dalam satu wilayah yang agak luas (dapat juga satu kota). MAN biasanya tidak dimiliki oleh satu organisasi saja. Sama seperti LAN, MAN juga memiliki *wireless* MAN dengan kekurangan dan kelebihan yang relatif sama.



Gambar 2. Metropolitan Area Network
Sumber : Rachmadi (2020)

3) *Wide Area Network* (WAN)

Menurut Rachmadi (2020), WAN (*Wide Area Network*) adalah kumpulan dari LAN atau Workgroup yang dihubungkan dengan menggunakan alat komunikasi modem dan jaringan *internet* dari kantor pusat dan kantor cabang, ataupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat, serta dengan biaya yang relative murah. Sistem jaringan ini dapat menggunakan jaringan *internet* yang sudah ada untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan PC *Stand Alone*/Notebook yang berada dilain kota ataupun Negara.



Gambar 3. Wide Area Network
Sumber: Rachmadi (2020)

b. Topologi Jaringan Komputer

Topologi jaringan merupakan sebuah desain jaringan komputer yang akan di bentuk serta menjelaskan bagaimana komputer-komputer tersebut dapat saling berhubungan antara satu sama lain. Topologi jaringan juga bias memudahkan kita untuk memahami bagaimana memahami jalur lalu lintas data yang terjadi pada sebuah sistem jaringan.dengan begini, jika kita ingin melakukan perbaikan terhadap sebuah jaringan, kita tidak perlu lagi kebingungan untuk mulai memperbaikinya dari mana, karena topologi jaringan ini sudah menggambarkan sejelas-jelasnya bagaimana *system* jaringan tersebut terbentuk. Beberapa topologi jaringan yaitu :

1) Topologi *Bus*

Topologi *Bus* dianalogikan ada komputer yang bertindak sebagai server dan nada komputer yang menerima layanan (*client*). Tampilan dari topologi *Bus* dapat dilihat pada gambar dibawah ini.Media penghantar untuk topologi ini jenis kabel koaksial.



Gambar 4. Topologi Bus
Sumber: Rachmadi (2020)

Kelebihan topologi *Bus :*

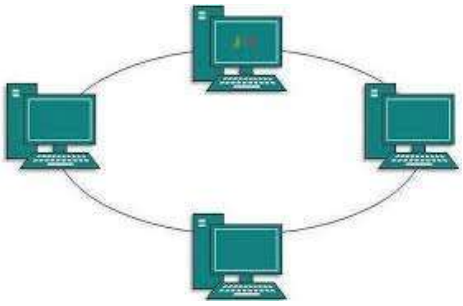
a) Hemat penggunaan kabel.
b) *Layout* pengkabel *simple*.
c) Gampang dikembangkan.

Kekurangan topologi *Bus* :

a) Kemungkinan isolasi dan deteksi kesalahan yang sangat kecil.
b) Terjadi kepadatan lalu lintas data.
c) Jaringan tidak berfungsi jika salah satu *client* rusak.

2) Topologi *Ring* (Cincin)

Bentuk dari topologi *Ring* dapat dilihat pada gambar dibawah ini. Berbeda dengan topologi Bus, setiap komputer/simpul/*host* pada topologi ini memiliki tingktan yang sama yaitu dapat bertindak sebagai *client*. Metode komunikasi data yang digunakan pada topologi ring yaitu degan cara *loop,* data dikirimkan ke setiap komputer dan setiap informasi yang diterima akan diperiksa alamatya, apakah data tersebut untuknya atau bukan.



Gambar 5. Topologi Ring
Sumber: Rachmadi (2020)

Kelebihan topologi *ring:*

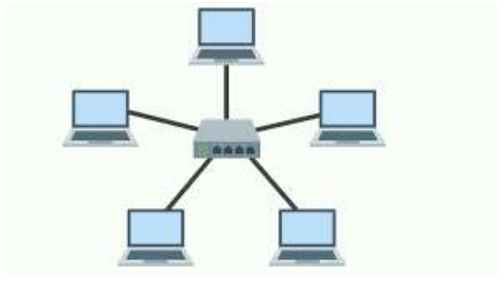
a) Hemat dalam pengkabelan.

Kekurangan topologi *ring*:

a) Sangat peka terhadap kesalahan, jika komputer satu tidak berfungsi maka komputer yang lain tidak dapat digunakan.
b) Pemgembangan jaringan sangat tidak fleksibel

3) Topologi *Star/* Bintang

Topologi star terdapat alat yang digunakan sebagai sentral. Semua link harus malalui sentral yang menyalurkan data kesemua komputer atau *client* yang dipilhnya. Komputer yang berfungsi sebgai sentral disebut *server* dan komputer yang dilayananinya dinamakan client. Untuk menghubungkan sentral dengan *client* dibutuhkan alat yang dinamakan hub. Hub inilah yang menghubungkan komputer *client* dengan media kabel atau *wireless*.



Gambar 6. Topologi Star
Sumber: Rachmadi (2020)

Kelebihan Topologi *Star*:

a) Paling felksibel dari semua topologi
b) Pengembangan sangat mudah dan tidak mengganggu bagian jaringan lain
c) Control menjadi terpusat

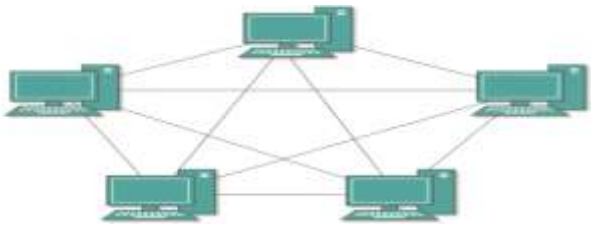
d) Kemudian dalam isolasi dan deteksi kerusakan maupun kesalahan
e) Mudah dalam melakukan administrasi jaringan

Kekurangan Topologi *Star*:

a) Membutuhkan banyak kabel
b) Perlu keterampilan khusus
c) *Control* terpusat sehingga Hub ataupun switch menjadi bagian paling kritis.

4) Topologi *Mesh* (Jala)

Menurut Rachmadi (2020), Topologi mesh adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada didalam jaringan. Akibatnya dalam topologi mesh setiap perangkat dapat berkomunikasi langsung dengan perangkat yang dituju (*dedicated links).* Dengan demikian banyaknya koneksi antar perangkat pada jaringan bertopologi mesh ini dapat dihitung yaitu sebanyak n(n-1)/2. Selain itu karena setiap perangkat dapat terhubung dengan perangkat harus memiliki sebanyak n-1 *Port Input/Output* (I/O ports).



Gambar 7. Topologi Mesh
Sumber: Rachmadi (2020)

Kelebihan Topologi Mesh:

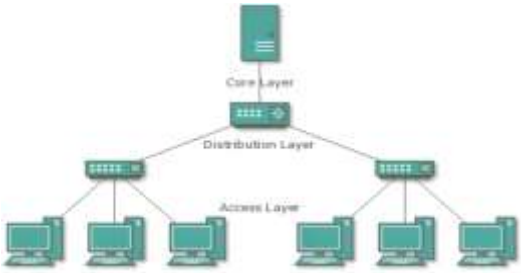
a) Hubungan *dedicted link* menjamin data langsung dikirimkan ke komputer tujuan tanpa harus melalui komputer lainnya
b) Memiliki sifat *Robuts*, yaitu apabila terjadi gangguan pada koneksi komputer A dengan komputer B karena rusaknya kabel koneksi (links) antara A dan B, maka gangguan tersebut tidak akan memegaruhi koneksi komputer A dengan komputer lainnya
c) *Privacy* dan *security* pada topologi mesh lebih terjamin
d) Memudahkan proses identifikasi permasalahan pada saat terjadi kerusakan koneksi antar komputer.

Kekurangan Topologi *Mesh*:

a) Membutuhkn banyak kabel
b) Hal tersebut sekaligus juga mengindikasikan bahwa topologi jenis ini *mesh*.
c) Banyaknya kabel yang digunakan juga mengisyaratkan perlunya *space* yang memungkinkan didalam ruangan tempat komputer-komputer tersebut berada.

5) Topologi *Tree* (Pohon)

Topologi *Tree* adalah kombinasi karakteristik antara topologi bintang dan topologi *Bus*. Topologi ini terdiri atas kumpulan topologi bintang yang dihubungkan dalam satu topologi Bus sebagai jalur tulang punggung atau *backbone*.



Gambar 8. Topologi Tree
Sumber: Rachmadi (2020)

6) Topologi Linier

Topologi linier biasa disebut dengan topologi bus beruntut, tata letak ini termasuk tata letak umum. Satu kabel utama menghubungkan tiap titik sambungan (komputer) yang dihubungkan dengan penyambungan yang disebut penamat (*terminator*). Penyambung yang digunakan berjenis BNC (*British Naval Connector*).

8. Konsep Dasar Jaringan Komputer

Menurut Joefrie (2013), *Network* atau jaringan dalam bidang computer dapat diartikan sebagai dua atau lebih perangkat cerdas yang dihubungkan sehingga dapat berkomunikasi, yang kemudian akan menimbulkan suatu efisien, sentralisasi dan optimasi kerja. Pada jaringan komputer yang dikomunikasikan adalah data sehingga bila ingin bertukar antar komputer, maka kita dapat melakukan proses unduh atau unggah berkas tanpa harus membawa media penyimpanan.

Ada beberapa jenis jaringan komputer bila dilihat dari cara pemrosesan data dan pengaksesannya:

a) *Host*-Terminal

Dimana terdapat satu atau lebih *server* yang dihubungkan dalam suatu *dumb* terminal. Karena dumb terminal hanyalah sebuah monitor yang dihubungkan dengan menggunakan kabel RS-232 maka pemrosesan data dilakukan dalam *server*. Oleh karena itu, *server* tersebut haruslah sebuah *system* komputer yang memiliki *system* komputer yang memiliki kamampuan pemrosesan data yang tinggi dan penyimpanan data yang sangat besar.

b) *Client Server*

Dimana sebuah *server* atau lebih yang dihubungkan dengan beberapaa *client.server* bertugas menyediakan berbagai macam layanan, misalnya pnegaksesan berkas, basis data. Sedangkan *client* adalah sebuah terminal yang menggunakan layanan tersebut.

c) *Peer to Peer*

Dimana terdapat beberapa terminal komputer yang dihubungkan dengan media jaringan komputer.Secara prinsip, hubungan *peer to peer* ini adalah bahwa setiap komputer dapat berfungsi sebagai *server* dan *client*, keduanya dapat difungsikan dalam waktu yang bersamaan.

9. *Port Scanning*

Pemindaian port (*Port Scanning*) merupakan aplikasi yang digunakan untuk mendeteksi dan melihat sejumlah informasi atau status dari protokol maupun port yang terbuka (*open*) dari sebuah perangkat. *Port scanner* adalah cara untuk mengakses layanan jaringan di computer (*Shaw, David, 2015).*

Penggunaan pemindaian port tidak secara keseluruhan diartikan sebagai serangan, melainkan pemeriksaan sederhana untuk menentukan layanan yang tersedia pada mesin jarak jauh..

Jadi dari kesimpulan di atas dapat ditarik kesimpulan bahwa *port scanning* merupakan kegiatan atau aktifitas untuk mencari dan melihat serta meneliti port pada suatu komputer atau peralatan lainnya yang terbuka maupun yang tertutup.

10. Router Mikrotik

Menurut Haeruddin (2021), MikroTik atau yang lebih di kenal dengan Mikrotik didirikan tahun 1995 bertujuan mengembangkan sistem ISP dengan wireless. Mikrotik saat ini telah mendukung sistem ISP (*Internet Service Protocol*) dengan wireless untuk jalur data internet di banyak negara, antara lain Iraq, Kosovo, Sri Lanka, Ghana dan banyak negara lainnya. Berbagai pengembangan telah dilakukan hingga saat ini dengan tersedianya perangkat lunak sistem operasi router versi 2 yang menjamin kestabilan, kontrol, dan fleksibilitas pada berbagai media antar muka dan sistem *routing* dengan menggunakan komputer standart sebagai hardware. Perangkat lunak ini mendukung berbagai aplikasi ISP, mulai dari RADIUS modem pool, hingga sirkuit backbone dengan DS3. Mikrotik berlokasi di Riga, ibukota Latvia, dengan 50 orang karyawan. Mikrotik juga menjalankan sebuah ISP kecil, sebagai media percobaan untuk pengembangan Router OS *software*.

Menurut Arifwidodo, dkk (2021), mikrotik didirikan pada tahun 1995 bertujuan mengembangkan sistem ISP dengan *wireless*. Mikrotik saat ini telah mendukung sistem ISP dengan *wireless* untuk jalur data internet dibanyak Negara antara lain Iraq, Sri Langka, Ghana dan Negara lainnya menggunakan mikrotik.

Mikrotik adalah sistem operasi dan perangkat lunak yang digunakan untuk memfungsikan komputer sebagai router. PC router tersebut dilengkapi dengan berbagai fasilitas dan alat, baik untuk jaringan kabel maupun nirkabel. Mikrotik sekarang ini banyak digunakan oleh ISP, penyedia hotspot. Pada standar perangkat keras berbasiskan Personal Computer (PC) Mikrotik dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah routing. Sedangkan aplikasi yang dapat diterapkan dengan Mikrotik selain routing adalah aplikasi kapasitas akses (*bandwidth*), manajemen, *firewall*, *wireless access point* (WiFi), backhaul link, sistem *hotspot*, Virtual Private Network (VPN) server dan masih banyak lainnya (Haeruddin, 2021)).



Gambar 9. *RouterBoard*
Sumber : Haeruddin (2021)

11. *NMAP (Network Mapper)*

NMAP (*Network Mapper*) digunakan untuk mengetahui *port-port* apa saja yang terbuka, aplikasi *NMAP* sangat bermanfaat untuk keamanan jaringan atau *network security*. *NMAP* merupakan sebuah alat (*software*) yang berbasis *open source* untuk melakukan eksplorasi jaringan dan audit keamanan. Menurut Rendro, Ngatono & Aji (2020) *NMAP* ("*Network Mapper*") adalah sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. *NMAP* menggunakan paket *IP raw* untuk mendeteksi *host* yang terhubung dengan jaringan dilengkapi dengan layanan (nama aplikasi dan versi) yang diberikan, sistem operasi (dan versi), apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya.

Output NMAP adalah sebuah daftar target *host* yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan. Hal kunci diantara informasi itu adalah "tabel *port* menarik" (Rendro, Ngatono & Aji, 2020). Tabel tersebut berisi daftar angka *port* dan protokol, nama layanan, dan status. Statusnya adalah terbuka (*open*), difilter (*filtered*), tertutup (*closed*), atau tidak *difilter* (*unfiltered*). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (*listening*) untuk koneksi/paket pada *port* tersebut.

Dapat ditarik kesimplan bahwa *NMAP* adalah sebuah aplikasi atau *tool* yang berfungsi untuk melakukan *port scanning* pada jaringan untuk mengetahui *port-port client* yang terbuka dan tertutup pada sebuah jaringan.

12. *Advanced Port Scanner*

Advanced Port Scanner adalah pemindai *port* gratis yang memungkinkan Anda secara cepat mencari *port* terbuka pada komputer jaringan dan mendapatkan versi program yang aktif pada *port* yang terdeteksi. Program memliki antarmuka ramah pengguna dan fungsionalitas yang kaya. (Rahmatillah, A., Firdaus, A., & Laila, 2021).

Advanced Port Scanner merupakan perangkat lunak cepat dan gratis untuk pemindaian port. Hal ini memungkinkan Anda secara cepat menemukan semua

port terbuka (TCP dan UDP) dan mendeteksi versi program yang aktif di sana. Utilitas mencakup banak fitur yang menyederhankan manajemen jaringan. (Fagroud, F. Z, dkk, 2021).

13. Penelitian Kualitatif

Penelitian kualitatif adalah penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian misalnya perilaku, persepsi, motivasi, tindakan dan lain-lain secara holisitik dan dengan cara deskripsi dalam bentuk kata-kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memanfaatkan berbagai metode alamiah. (Sugiyono, 2019).

Metode penelitian kualitatif adalah metode yang berdasarkan pada filsafat postposivisme, sedangkan untuk meneliti pada objek alamiah, dimana peneliti adalah sebagai instrumen kunci, teknik pengumpulan data dilakukan dengan cara triangulasi (Gabungan). (Sugiyono, 2019).

14. *NDLC* (*Network Development Life Cycle*)

Menurut Fatayana, (2022), menjelaskan Metode *NDLC* merupakan metode yang digunakan sebelum pembangunan dimulai seperti rencana strategi berbisnis, daur ulang dalam pembuatan aplikasi baru, dan menganalisa pendistribusian data secara berulang. Jika implementasi pada jaringan teknologi dapat dilaksanakan secara baik maka dapat diketahui beberapa informasi system yang memenuhi kriteria dalam mendesain dari dalam baik dari jaringan fisik ataupun dari jaringan logis yang digunakan. Tahapan dalam metode ini, yaitu: analisis (*analysis)*, perancangan (*design*), simulasi (*simulation prototyping*), implementasi (*implementation*), *monitoring*, dan *management*.

a) Analisis (*Analysis)*

Pada tahapan ini dalam metode *NDLC* menganalisis permasalahan yang muncul, analisa keinginan user ataupun kebutuhan hardware yang akan digunakan dan analisa topologi jaringan yang sudah ada saat ini.

b) Perancangan (*Design*)

Dari data-data observasi atau wawancara yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar *design* topologi jaringan interkoneksi yang ada dan yang akan dibangun/dikembangkan, diharapkan akan memberikan gambaran seutuhnya dari kebutuhan yang ada. *Design* bisa berupa desain struktur

topologi, desain akses data, desain tata *layout* perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun.

c) Simulasi (*Simulation Prototyping*)

Pada tahapan ini ada beberapa pengembangan pada jaringan yang akan membuat perancangan dalam bentuk semulasi dengan membutuhkan bantuan khususnya pada bidang network contohnya *Visio, Boson, Packet Tracert*, dan *Netsim*. Untuk melihat kinerja dari awal akan dibangun sebagai bahan sharing dan presentasi dengan tim-tim lainnya.

d) Implementasi (*Implementation*)

Dalam tahap iimplementasi akan dilakukan penerapan dari semua yang telah direncanakan dan di *design* sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya projek yang akan dibangun.

e) *Monitoring*

Setelah tahapan implementasi, tahapan *monitoring* merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan untuk Memantau *traffic* yang berjalan di jaringan sudah sesuai dengan semestinya.

f) *Management*

Tahapan terakhir dalam metode *NDLC* adalah tahap *management*. Pada tahap manajemen ini akan dilakukan beberapa langkah pengelolaan agar sistem yang telah dibangun dapat berjalan sesuai dengan yang diharapkan.

2.2 Hasil Penelitian yang Relevan

Peneliti melakukan penelusuran terhadap penelitian-penelitian terdahulu. Dari hasil penelusuran penelitian terdahulu:

1. Penelitian yang dilakukan Elsa Stephani, Fitri Nova dan Ervan Asri (2020). Implementasi dan Analisa Keamanan Jaringan IDS (*Intrusion Detection System*) Menggunakan Suricata Pada *Web Server*. Sistem pertahanan terhadap server umumnya masih dilakukan secara manual oleh administrator. Untuk mengatasi hal ini, maka dibutuhkan sebuah sistem yang berfungsi untuk

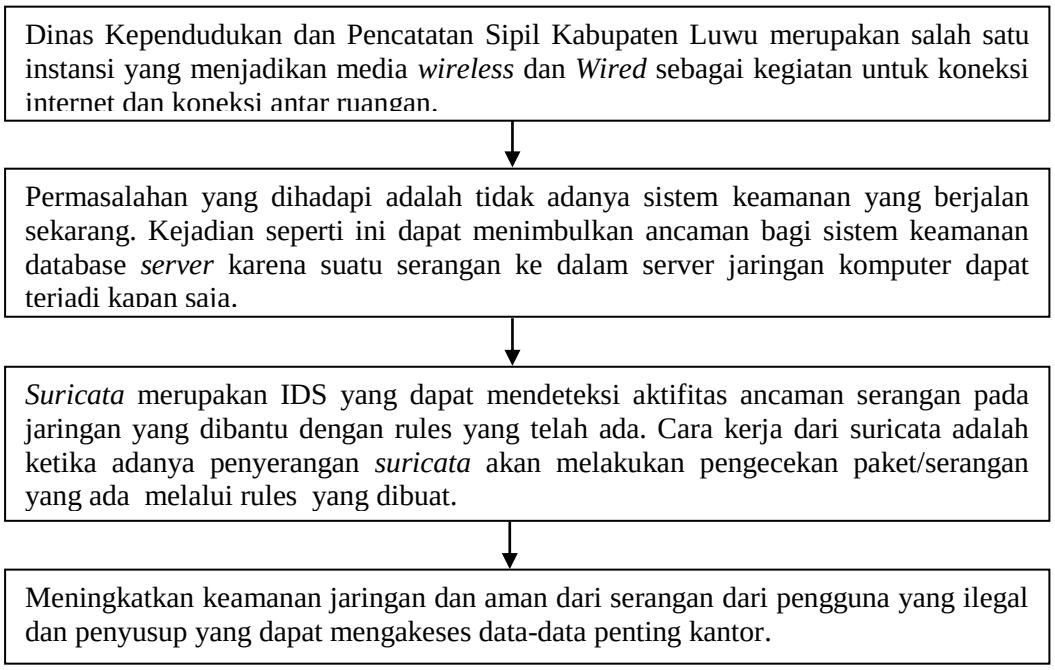
menginformasikan ancaman yang terjadi secara optimal dan diatasi dengan cepat. Maka dikembangkanlah sistem keamanan jaringan IDS menggunakan Suricata. Suricata sendiri akan dibangun menggunakan OPNsense. Dengan adanya sistem Suricata menggunakan OPNsense ini, dapat mendeteksi maupun mencegah serangan yang masuk.

2. Penelitian yang dilakukan Satria Bagus Pribadi (2019). Implementasi *Suricata* Untuk Meningkatkan Keamanan Pada *Cloud Computing*. Dari hasil ini pengujian mendapatkan hasil optimal dari hasil serangan terdeteksi oleh log sistem deteksi intrusi (IDS*) Suricata di dir /var/log/suricata/fast.log*, dan juga penulis menambahkan konfigurasi *suricata* tidak hanya untuk mendeteksi, sehingga bisa juga untuk melakukan eksekusi drop bila ada aktifitas mencurigakan dengan menggunakan netfilter yang sudah ada pada suricata dan konfigurasi oleh penulis untuk meningkatkan keamanan pada cloud computing secara optimal.
3. Penelitian yang dilakukan Nazwita, Siti Ramadhani (2017). Analisis Sistem Keamanan *Web Server* dan *Database Server* Menggunakan *Suricata*. *Suricata* dapat mendeteksi dan mencegah gangguan seperti Port Scanning atau aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status port (biasanya port TCP) pada sebuah host, dan Brute force atau metode untuk mendapatkan password dari user yang menjadi target.
4. Penelitian yang dilakukan Fahmi Bagaskara Perdana, Rendy Munadi dan Arif Indra Irawan (2019). Implementasi Sistem Keamanan Jaringan Menggunakan Suricata Dan Ntopng. hasil penelitian ini, berdasarkan rule Suricata yang penulis buat, penulis berhasil mendeteksi semua serangan yang diujicobakan. Sedangkan pada rule default pada Ntopng, penulis hanya mampu mengidentifikasi jenis serangan DoS berupa SYN *flood*. Untuk serangan DoS dengan tujuan *website server.*
5. Penelitian yang dilakukan oleh penulis (2022).Analisis keamanan jaringan *Database server* menggunakan *suricata* sistemnya berjalan dengan baik setelah menggunakan *suricata* serangan *port scanning* tidak bisa memantau

port-port yang terbuka dan dan untuk serangan *DDOS* tidak mempengaruhi kinerja *CPU.*

2.3 Kerangka Pikir

Untuk memperjelas permasalahan penelitian yang dilakukan, maka berikut akan ditunjukkan kerangka pikir seperti pada gambar berikut:



Gambar 10. Kerangka Fikir