BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan berkembangnya teknologi informasi yang sangat cepat terutama internet, Memberikan dampak yang sangat besar pada aktifitas sebuah perusahaan atau instansi dalam melakukan interaksi dengan karyawan atau pegawai melalui jaringan komputer. akan tetapi aktivitas-aktivitas tersebut akan sangat terganggu dan berisiko jika informasi yang sangat penting diakses oleh orang yang tidak berkepentingan. Terlebih dahulu harus diketahui bahwa ada jenis media transmisi jaringan komputer, yaitu kabel dan nirkabel *(wifi)*.

Teknologi nirkabel (*wireless)* menggunakan transmisi frekuensi radio sebagai alat untuk mengirim data, sedangkan teknologi kabel menggunakan kabel. Penggunaan penyedia jasa *wireless* antara lain ISP, Warnet, *hostpot* komersil, kampus-kampus maupun perkantoran sudah banyak yang memanfaatkan *wifi* pada jaringan masing-masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut. Oleh karena itu banyak *hacker* yang tertarik untuk mengksplore kemampuannya dalam melakukan berbagai aktifitas yang biasanya ilegal menggunakan *wifi* (Gondohanindijo,2012)

Salah satu bentuk kejahatan di dunia digital yang banyak terjadi adalah kejahatan terhadap data pribadi. Berdasarkan laporan dari UNICEF pada tahun 2017, tercatat lebih dari 5 (lima) juta profil dan akun sosial media di dunia digital telah dicuri menggunakan pencurian berbasis internet, selanjutnya, pada tahun 2017 *javelin strategy* & *research* juga menemukan bahwa lebih dari satu juta anak anak di amerika serikat telah menjadi korban dari pencurian indetitas yang menyebabkan kerugian sebesar $2.6 miliar (dua miliar enam ratus juta dolar). Kerugian akibat kejahatan data pribadi juga dialami oleh negara-negara Eropa pada tahun 2017 yang mencapai angka 1.37 miliar data yang hilang atau dicuri menggunakan internet. (Bismo,2019)

Salah satu masalah penting dalam keamanan jaringan pada saat ini adalah internet yang menghubungkan beberapa jaringan seperti pada saat ini adalah internet yang menghubungkan beberapa jaringan seperti jaringan *wireless LAN* yang dapat digunakan untuk mengirim data dan kadang tidak aman sehingga akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk memanfaatkan data tersebut sewenang-wenangnya. Perlu dipahami bahwa dalam merancang sistem

keamanan jaringan yang baik diperlukan sebuah perencanaan yang matang agar sumber daya yang berada di dalam jaringan tersebut dapat terhindar dari penjahat dunia maya (*cracker)*. *Cracker* adalah seseorang yang mencari kelemahan suatu sistem dan hasil temuannya akan diberitahukan kepada pemilik sistem atau dipublikasikan secara umum bahwa sistem tersebut memiliki kelemahan. *Hacker* juga akan memberikan pendapat yang mungkin bisa memperbaiki kelemahan sistem tersebut dengan cara yang legal.

Salah satu ancaman keamanan jaringan yang sangat umum dilakukan oleh para penjahat dunia maya adalah serangan *packet sniffing. packet sniffing* adalah salah satu bentuk serangan yang menangkap data dari paket yang lewat di jaringan. Data tersebut bisa berupa *username,password,* dan informasi-informasi penting lainnya yang lewat dijaringan dalam bentuk *text*. Paket yang dapat ditangkap tidak hanya satu tapi bisa berjumlah ratusan bahkan ribuan. Hal tersebut dapat membahayakan para pengguna jaringan komputer.

Kantor Dinas Perhubungan Luwu adalah salah satu kantor yang mempunyai fasilitas jaringan *internet*. Masalah yang terjadi pada Kantor Dinas Perhubungan Luwu terdekteksinya keberadaan dan keamanan jaringan WIFI yang terbuka tanpa pengamanan sehingga, menyebabkan jaringan menjadi lambat dan susah di akses dikarenakan banyaknya pihak pengguna jaringan. Jaringan ini belum mempuyai keamanan jaringan yang kurang baik serta kurangnya pengetahuan tentang jaringan komputer, mengingat pegawai yang bekerja pada bidang IT hanya memiliki basic pengetahuan pada bidang multimedia dan pemrograman, hal ini yang melatar belakangi kurangnya upaya pihak instansi dalam mengatasi masalah yang penulis kemukakan. karena tidak dilengkapi, dengan adanya *firewall* Untuk mengamankan sebuah jaringan serta pembagian *bandwithnya* belum merata. Maka perlunya peningkatan keamanan yang lebih baik untuk dapat menangani serangan kejahatan *sniffing* salah satu bentuk serangan yang menangkap data dari paket yang lewat di jaringan. Data tersebut bisa berupa *username, password*, dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk *text.*

Dimana permasalahan tersebut diantara jaringan WIFI yang kurang mendukung pada pengguna jaringan komputer sejauh ini belum terdapat sistem keamanan karena tidak menerapkan sebuah keamanan jaringan, dari permasalahan diatas maka sangat penting untuk menggunakan *hardware (mikrotik)* untuk meminimalisir permasalahan yang ada.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah yang akan dibahas dalam penelitian ini adalah bagaimana menganalisis keamanan jaringan Nirkabel dari Serangan *Packet Sniffing* pada Kantor Dinas Perhubungan Luwu?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk menganalisis keamanan jaringan Nirkabel dari Serangan *Packet Sniffing* pada Kantor Dinas Perhubungan Luwu.

1.4 Manfaat Penelitian

Adapun manfaat penelitian yang diharapkan setelah penelitian ini dilaksanakan adalah:

1. Manfaat terhadap Instansi

Manfaat yang di dapatkan instansi terkait dari hasil penelitian ini yaitu orang-orang dari instansi terkait dapat mengetahui kinerja jaringan atau topologi yang digunakan pada lokasi penelitian berdasarkan dari hasil analisis yang peneliti lakukan.

2. Manfaat terhadap Dunia Akademik

Penelitian ini dapat dijadikan bahan atau referensi dalam penelitian selanjutnya tentang perancangan sebuah sistem keamanan jaringan komputer.

1. Manfaat terhadap Penulis

Dengan hasil penelitian ini tentunya diharapkan dapat digunakan sebagai sumber informasi dan sebagai bahan referensi penelitian selanjutnya untuk mahasiswa yang mengangkat judul yang sama.

BAB II

TINJAUAN PUSTAKA

2.1. Kajian Teori

Penyajian materi yang di kemukakan dalam kajian teori merupakan teori yang menjadi dasar bidang yang di teliti. Teori-teori dasar atau umum dan juga khusus yang merupakan pengertian dan definisi yang diambil dari media cetak dan media elektronik.

1. Analisis

Dalam melakukan analisis, diperlukan suatu sistem informasi yang utuh agar kita dapat mengidentifikasi atau mengevaluasi berbagai macam masalah yang akan timbul pada sistem, sehingga masalah tersebut dapat di perbaiki dan dilakukan pengembangan terhadap komponen untuk dikaji lebih lanjut.

Menurut setiawan (2004), Analisis adalah metode yang digunakan untuk memahami deskripsi data, hubungan antar data, semantik data, dan bagaimana batasan data ada dalam sistem informasi. Ada banyak cara untuk menganalisis dan memodelkan data, beberapa di antaranya menggunakan diagram hubungan entitas.

Lebih lanjut Mait (2013) mengatakan analisis adalah penguraian suatu persoalan atau permasalahan serta menjelaskan mengenai hubungan antara bagian- bagian yang ada di dalamnya untuk selanjutnya diperoleh suatu pengertian secara keseluruhan.

Analisis adalah kegiatan yang terdiri dari urutan operasi yang juga dapat dipahami sebagai fitur yang memecah atau memecah informasi menjadi komponen yang lebih kecil untuk lebih mudah dipahami.

2. Analisis Keamanan Jaringan

Keamanan jaringan diterapkan untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan atau penolakan jaringan komputer dan sumber daya yang dapat diakses jaringan.

Menurut Yuliandoko (2018:206), keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya terhadap upaya perubahan dan perusakan oleh seseorang yang tidak diizinkan.

Mustaqin (2016) mengatakan bahwa analisis keamanan jarignan merupakan salah satu proses mencegah dan memonitoring penggunaan jaringan yang tidak sah, tujuanya yaitu mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun *logic* baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang

berlangsung.

Sedangkan Amarudin (2018) mengatakan bahwa analisis kemanan jaringan merupakan salah satu hal terpenting dalam proses sebelum implementasi jaringan komputer. Banyak jaringan komputer akan mengalami masalah karena kelalaian tersebut. Oleh karena itu, dapat membuka peluang bagi peretas untuk menyerang dan merusak jaringan

Analisis keamanan jaringan merupakan suatu cara mengamankan informasi agar dapat mencegah atau mendeteksi adanya gangguan dalam jaringan, adapun pendapat dari beberapa ahli.

3. Jaringan

Jaringan saat ini sudah menjadi kebutuhan dasar masyarakat. Untuk berkomunikasi dan kebutuhan lainnya melalui jaringan komputer, dua atau lebih perangkat perlu terhubung ke jaringan itu sendiri untuk menghasilkan media transmisi atau media komunikasi.

Tenggario dan Lukas (2011) mengatakan bahwa Jaringan komputer adalah sekelompok komputer yang menggunakan media komunikasi dan protokol komunikasi untuk saling terhubung sehingga komputer dapat saling berbagi dan bertukar informasi. Pada saat ini, manfaat jaringan komputer sering memainkan peran penting dalam penyebaran informasi yang cepat.

Sedangkan Haryanto dan Riadi mengatakan bahwa Jaringan (komputer) adalah jaringan yang terdiri dari dua atau lebih komputer yang terhubung satu sama lain. Mereka berbagi sumber daya seperti CD ROM, *printer*, dan pertukaran file atau memungkinkan komunikasi elektronik satu sama lain. Komputer yang terhubung dapat dihubungkan dengan kabel, saluran telepon, gelombang radio, satelit, atau media inframerah.

Menurut Madcoms (2010:2-3), adapun jenis-jenis jaringan antara lain:

1. *Local Area Network* (LAN) adalah jenis jaringan yang menghubungkan beberapa komputer di satu lokasi ke area terbatas, seperti ruangan atau gedung. LAN dapat menggunakan media komunikasi seperti kabel dan *nirkabel.*
2. *Wide Area Network* (WAN) adalah jaringan antara LAN dengan LAN lain yang dipisahkan oleh jarak yang cukup jauh. Contoh penggunaan WAN adalah hubungan antara kantor pusat dan cabang *regional.*

3. *Metropolitan Area Network* (MAN) jaringan yang lebih besar dari LAN tetapi lebih besar dari WAN. Baik jaringan area metropolitan maupun jaringan area luas terhubung ke berbagai jaringan area lokal, satu-satunya perbedaan adalah areanya berbeda

Jaringan merupakan alat penghubung antar komputer, sehingga dapat saling memberikan informasi dan dapat bekerja sama untuk mencapai tujuan yang sama, guna mencapai pengelolaan sumber daya yang lebih efektif.

4. Topologi Jaringan

Topologi jaringan merupakan bagaimana komputer secara fisik terhubung satu sama lain.

Menurut Hardani (2011) sebuah topologi yang sama dapat didefinisikan oleh beberapa protokol jaringan yang berbeda dapat digunakan untuk mendefinisikan topologi yang sama. Misalnya, FDDI dan *Token Ring* beroperasi dalam topologi *ring*.

Terdapat 5 jenis topologi jaringan yaitu:

a. Topologi *Bus* merupakan topologi yang menggunakan kabel *relay*, dan semua *host* terhubung langsung dengan kabel tersebut. Topologi ini paling banyak digunakan selama proliferasi kabel koaksial
b. Topologi *Ring* adalah topologi dimana *host* dan *host* lainnya terhubung dalam suatu *loop* atau *loop* tertutup. Jaringan topologi *ring* ini mirip dengan topologi *bus*, hanya saja kedua ujungnya saling terhubung oleh segmen kabel membentuk lingkaran.
c. Topologi *Star* adalah topologi yang menghubungkan semua komputer ke sebuah pusat atau konsentrator. Hub biasanya merupakan hub atau perangkat *switch*. Kabel yang sering digunakan pada topologi ini adalah UTP Kategori 5
d. Topologi *Star*-Bus menggabungkan beberapa topologi bintang dalam satu unit. Alat yang digunakan untuk menghubungkan setiap topologi star adalah hub atau *switch.* Topologi ini merupakan topologi yang paling banyak digunakan. Komputer terhubung ke hub, dan satu hub terhubung ke hub lain sebagai *trunk* mirip dengan topologi *bus.*
e. Topologi *Mesh* menghubungkan setiap titik komputer ke titik lainya. Artinya semua komputer akan terhubung satu per satu, sehingga tidak akan ditemukan *broken link.* Topologi *mesh* adalah topologi yang digunakan oleh internet, dimana setiap *link*

menghubungkan satu *router* dengan *router* lainnya.

Topologi jaringan adalah topologi yang secara fisik untuk menghubungkan komputer satu sama lain.

5. Jaringan Pada Lokasi Penelitian

Jaringan pada Kantor Dinas Perhubungan Luwu merupakan jaringan yang menerapkan penggunaan jaringan berbasis *wireless.* Jaringan pada kantor merupakan jaringan internet yang berasal dari provider yang dapat terhubung dengan komputer yang satu dengan komputer yang lainnya. Jaringan pada kantor dapat diakses melalui ruang kelautan yang menyediakan 4 unit Pc, dan 4 unit laptop, 2 unit Hp yang digunakan saat peneliti melakukan observasi langsung. Jaringan yang telah diterapkan pada kantor merupakan jaringan yang menerapkan sistem keamanan yang standar tanpa pengamanan dan dapat diakses oleh siapapun yang berada dalam lingkungan kantor.

6. *Packet sniffing*

a. Pengertian *packet sniffing*

Menurut Mathew (2004), sebuah program *sniffing* ini bagian dari perangkat lunak yang mengambil semua lalu lintas data yang melalui komputer yang terhubung jaringan. *Sniffing* merupakan tindak kejahatan penyadapan yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mengambil data dan informasi yang bersifat privasi secara ilegal. Cara kerja *sniffing* adalah ketika anda terhubung ke jaringan yang bersifat *public*, saat anda melakukan proses transfer data dari *client server* dan sebaliknya. Karena data yang mengalir pada *client* dan *server* yang bersifat bolak balik, *sniffing* ini akan menangkap paket-paket yang dikirimkan dengan cara ilegal.

b. Jenis-Jenis *Sniffing*

1) *Passive Sniffing*

Passive sniffing adalah tindakan kejahatan dengan tidak merubah isi dari paket data yang dikirimkan antara *server* dan *client.* Jadi anda tidak merasa curiga karna ada tanda-tanda kalau menjadi korban *sniffing*. *Passive sniffing* biasanya terjadi pada *Hub*, karna tugas utama *Hub* membagikan signal ke semua komputer *clien*t, berbeda dengan fungsi *switch* yang memiliki fitur untuk menghindari terjadinya *collision* atau bentrokan dengan membaca alamat *MAC Address computer client*. Beberapa *tools* yang sering digunakan untuk *passive sniffing* seperti *Wireshark, Tcpdump, Kismet, Ettercap, Dsniff*

dan lain sebagainnya.

2). *Active Sniffing*

Kebalikan dari *passive sniffing*, *active sniffing* adalah tindak kejahatan dengan cara mengubah isi paket data dalam jaringan. Tindakan *active sniffing* yang paling sering dilakukan adalah *ARP Poisoning*, *Man in the middle attack*, *active sniffing* ini biasanya dilakukan pada *switch* jaringan, bukan lagi pada *hub*.

a. Cara Kerja *Packet Sniffing*

Sniffing cara kerjanya memiliki beberapa tahap sampai paket data yang diambil bisa terbaca, Berikut pembahasannya:

1) *Collection*

Cara kerja paket pertama adalah merubah *interface* dan mulai mengumpulkan semua paket data yang melalui jaringan yang sedang diawasi.

2) *Conversion*

Cara kerja setelah *collection* adalah *conversion* dengan cara merubah data yang sudah di *collect binary* kedalam data yang lebih muda dipahami.

3) *Analisys*

Cara kerja ketiga adalah menganalisis data yang sudah dikonversi kedalam blok-blok *protocol* berdasarkan sumber transmisi data.

4) Pengambilan Data

Cara kerja *packet sniffing* yang terakhir setelah semua dilakukan, *hacker* akan mengambil data.

b. Protocol yang digunakan untuk *Sniffing*

Berikut beberapa protokol jaringan komputer yang sering digunakan *sniffing* digunakan untuk melakukan aksinya

1) *HTTP*

HTTP atau *Hypertext Transfer Protocol* digunakan untuk mengirimkan paket data tanpa adanya enkripsi, sehingga tindakan *sniffing* bisa dilakukan dengan mudah.

2) *SMPT*

SMPT atau Simple Mail Transfer Protocol fungsi utamanya untuk transfer *email*, tetapi masih belum aman dari tindak kejahatan *sniffing*

3) *NNTP*

NNTP atau Network New Transfer Protocol bisa digunakan untuk semua jenis komunikasi, namun kekurangannya setiap paket data yang dikirimkan berbentuk teks yang jelas mudah dibaca sehingga sangat rawan sekali.

4) *POP*

POP atau Post Office Protocol memiliki fungsi untuk menerima *email* dari server, *protocol* ini tidak bisa dijamin aman karena *email* yang masuk masih memungkinkan untuk disisipi *spoofing email.*

5) *FTP*

FTP atau *File Transfer Protocol* memiliki fungsi untuk mengirim dan menerima file, namun tidak memiliki fitur keamanan sedikitpun. Semua data yang dikirimkan berbentuk teks yang mudah sekali diambil oleh s*niffer*.

6) *IMAP*

IMAP atau *Internet Massage Access Protocol* yaitu fungsinya hampir mirip dengan SMTP yaitu berhubungan *email* transfer.

7. *Ettercap*

Ettercap adalah sebuah *tools packet sniffing* yang digunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. Dan memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri *password*, dan melakukan penyadapan aktif terhadap protokol-protokol umum. *Ettercap* merupakan *tools* yang ditujukan untuk penganalisisan paket data jaringan. *Ettercap* juga melakukan pengawasan paket secara *real time* dan kemudian menangkap data dan menampilkannya selengkap mungkin .(Fauzi dan Suartana, 2017).

8. Mikrotik

Menurut Madcoms (2015:212) menyatakan bahwa mikrotik merupakan sebuah perusahaan yang bergerak dibidang produksi perangkat keras (*hardware)* dan perangkat lunak *(software)* yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, berseblahan dengan rusia. *Mikrotik* didirikan pada tahun 1995 untuk mengembangkan *router* dan sistem ISP (*internet service provider)*.

Mikrotik didefinisikan oleh Hardana dan Inovanto (2012:1), menyatakan bahwa mikrotik adalah *router* canggih berbasis sistem operasi *linux*. Alat ini dapat digunakan untuk berbagai keperluan jaringan komputer , mulai dari *ruting, statis,*

dinamis, *hostpot,firewall, VPN, DHCP, DNS, web proxy* dan beberapa fungsi lainnya. Sedangkan menurut Amaruddin danUlun (2018:73), *mikrotik* adalah perangkat jaringan komputer yang beberapa *hardware* dan *software* yang dapat difungsikan sebagai *router* ,sebagai alat *filtering, switching* maupun yang lainnya.

Berdasarkan uraian diatas penulis menyimpulkan bahwa *mikrotik* merupakan sistem operasi dan perangkat lunak yang memiliki berbagai fitur yang dapat digunakan untuk menjadikan komputer sebagai pengatur lalu lintas antar jaringan.

9. *Winbox*

Salah satu keunggulan *routerboard mikrotik* adalah konfigurasi yang berbasis GUI. Salah satu cara untuk mengakses *mikrotik routerboard* adalah *winbox. Winbox* adalah utilitas untuk menghubungkan dari jarak jauh ke *server proxy* dalam mode antarmuka pengguna grafis GUI. Saat menggunakan *winbox,* pengguna dapat mengkonfigurasi dengan satu klik tanpa *scripting* (Hariadi, Bagye, dan Zaen, 2019). *Winbox* adalah perangkat lunak jaringan yang dapat digunakan sebagai *proxy* untuk koneksi dan konfigurasi menggunakan alamat *MAC* dan *protocol* IP. *Winbox* banyak digunakan di sistem operasi windows, tetapi *winbox* juga dapat digunakan di *linux* dengan bantuan *software wine. Winbox* lebih populer karena memiliki tampilan grafis yang sederhana dibandingkan dengan telnet atau *web browser.* Saat menggunakan *winbox* untuk konfigurasi, ia menyediakan banyak fungsi, terutama dalam hal keamanan.

Ada beberapa fungsi *winbox,*yaitu :

a. Setting *mikrotik router* dalam mode GUI
b. Setting *bandwith* atau membatasi kecepatan jaringan
c. Memblokir sebuah *website/situs*
d. Mempercepat pekerjaan
e. Dapat meremote *mikrotik* dari jarak jauh
f. Dapat mengetahui dan mengatur alamat IP dan akses ke situs tertentu

Winbox adalah perangkat lunak yang digunakan untuk terhubung ke *server proxy* jarak jauh dalam mode antarmuka pengguna grafis GUI. Dengan menggunakan *winbox* untuk memenuhi kebutuhan konfigurasi jaringan *router mikrotik* pasti akan lebih mudah digunakan tanpa keluar dari sistem keamanan.

10. *Firewall*

Menurut Haryadi, Bagye dan Zaen, (2019) *firewall* adalah sebuah sistem keamanan jaringan komputer yang bertanggung jawab melindungi komputer dari berbagai macam serangan dari komputer dari luar. Secara umum, *firewall* komputer merupakan sebuah program perangkat lunak untuk mencegah jalan masuk yang tidak sah ke jaringan pribadi, dimana sebuah *firewall* mampu momonitor serta mengontrol seluruh lalu lintas jaringan yang masuk dan keluar yang berlandaskan suatu aturan keamanan yang sudah ditetapkan. Dimana bahaya *walmare* berbasis data yang ada internet yang mempunyai beberapa manfaat yaitu :

a. Salah satu hal yang paling buruk yang biasanya terjadi pada komputer yaitu, seseorang berusaha untuk membobol dari jarak yang jauh namun dengan adanya *firewall* kemudian telah selesai dikonfigurasi dengan benar maka kita bisa menonaktifkan akses komputer dari jarak jauh, sehingga kita dapat mencegah *hacker* yang mengambil ahli komputer tersebut.
b. *Internet* mempunyai banyak kode yang buruk untuk mengatasi PC yang tidak terlindungi untuk bisa memblokir pesan yang menyatakan ke konten yang tak diinginkan.
c. Cara *hacker* memanfaatkan *walmare* yaitu mereka bisa masuk ke sistem untuk memblokir kemudian bisa membangun sistem menjadi aman.

Cara kerja *firewall* yaitu :

Firewall memandu semua lalu lintas untuk sebuah informasi yang memungkinkan data yang bagus serta masuk untuk memblokir data yang buruk yang masuk ke komputer. Dimana ketika komputer mempunyai suatu pengamanan *firewall,* maka semua yang masuk dan keluar akan dimonitor dan dipantau.

Adapun metode yang digunakan untuk mengontrol lalu lintas yang akan mengalir masuk dan keluar ke jaringan yaitu :

a. Penyaringan paket

Filter yang akan dikirim ke suatu sistem yang diminta, untuk sementara itu paket lainnya dibuang,kemudian dapat dianalisis terhadap satu set *filter.*

b. Layanan *proxy*

Sebuah informasi dari internet bisa di ambil dengan *firewall* lalu sudah itu dikirim kemudian di ambil oleh *firewall* dan kemudian dikirim pada sistem maka sistem

pula yang akan diminta ataupun sebaliknya.

c. *Inspeksi stateful*

Informasi dari sebuah *firewall* masuk keluar monitor untuk memilih kriteria atau karakteristik ataupun spesifik lalu kemudian informasi yang akan masuk belum bisa di kembangkan dengan karateristik tersebut. Apabila perbandingan bisa menimbulkan kecocokan yang masuk akal, serta informasi tersebut bisa di izinkan untuk masuk ke metode yang baru ini akan tetapi bukan untuk memeriksa konten setiap paket akan dibandingkan oleh bagian-bagian kunci untuk paket beserta database informasi yang terpercaya.

Dimana keefektifan menggunakan *firewall* yaitu sangat efektif dalam mengkonfigurasikan keamanan jaringan WIFI dimana *firewall* disini berfungsi memblok pengguna yang tidak memiliki izin masuk ke jaringan kantor Dinas Perhubungan Luwu sehingga lebih aman dari keamanan sebelumnya yang tidak memiliki keamanan *firewall*.

11. Teori Kategori Validasi

Widoyoko (2016) menyatakan bahwa tahap Verifikasi adalah tahap mengevaluasi apakah produk yang dirancang masuk akal. Verifikasi ini dilakukan melalui penggunaan tabel verifikasi. Kemudian menginterpretasikan nilai koefisien efektivitas untuk menentukan kategori atau tingkat efektivitas. Kriteria koefisien validitasnya dapat dilihat pada tabel 1.

Tabel 1. Kategori validasi

Interval Rata-Rata Skor	Kategori
> 3,25 s/d 4,0	Sangat valid
> 2,5 s/d 3,25	Valid
> 1,75 s/d 2,5	Kurang valid
> 1,0 s/d 1,75	Tidak valid

Sumber: Widoyoko (2016)

2.2. Hasil Penelitian yang Relevan

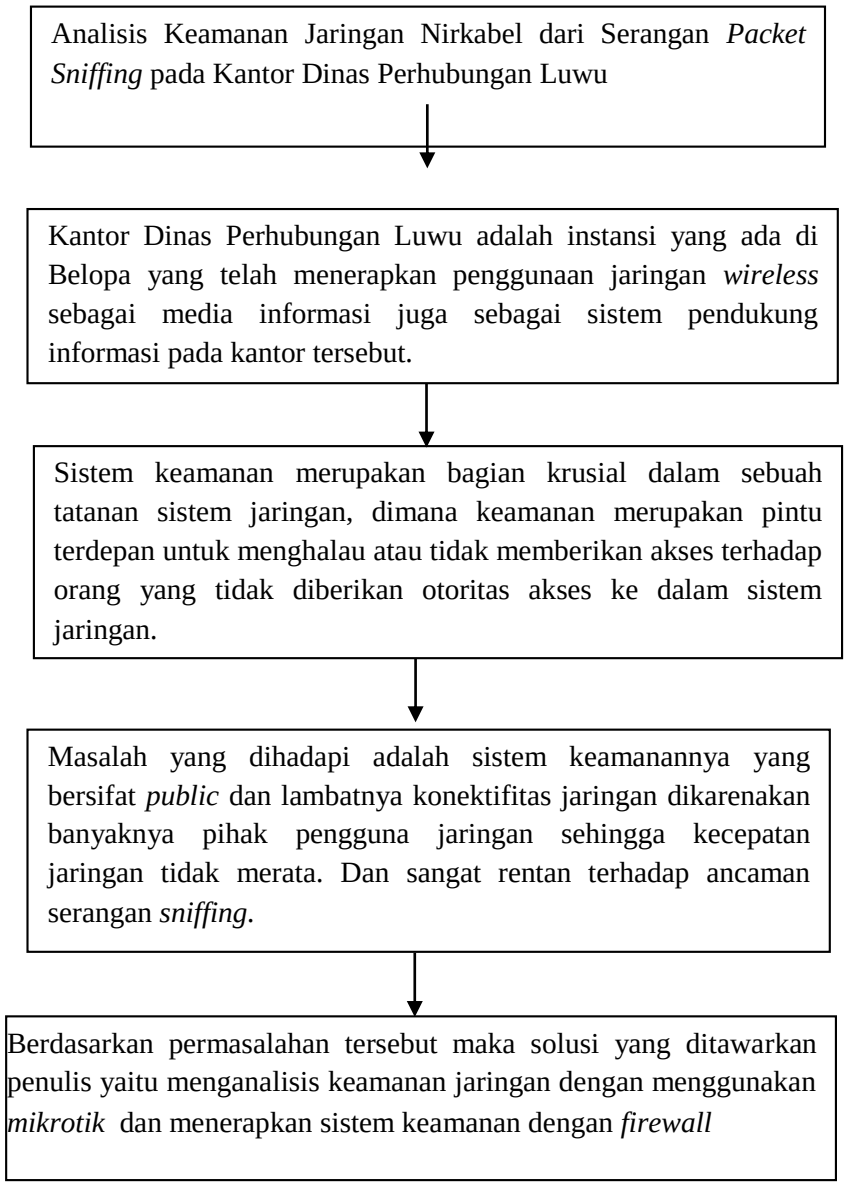
Kajian pustaka relevan adalah sumber pustaka berbentuk penelitian sebelumnya yang relevan dengan permasalahannya. Fungsi dari kajian pustaka relevan ini adalah mengemukakan secara sistematis hasil penelitian sebelumnya yang berkaitan dengan penelitian yang di lakukan. Hasil kajian pustaka menujukkan penelitian tentang

"Analisis Keamanan Jaringan Nirkabel Dari Serangan *Packet Sniffing* Pada Kantor Dinas Perhubungan Luwu". Belum pernah dilakukan namun, ada beberapa penelitian yang relevan untuk mendukung penelitian tersebut antara lain :

1. Arianto (2018) dalam jurnalnya yang berjudul "Deteksi *Packet Sniffing* pada *Wireless* Menggunakan *Arp Watch*" Tujuan dari pengujian disini adalah untuk mengetahui ancaman keamanan jaringan untuk mendeteksi serangan *packet sniffing* dengan indikasi *ARP spoofing* pada jaringan menggunakan aplikasi *Arp watch* yang digunakan untuk mendeteksi adanya serangan pada jaringan *public*. *Arp watch* ini akan memonitor aktifitas *ethemer* dan menyimpan informasi yang didapat dalam bentuk pasangan IP dan alamat *MAC*. Selain itu peneliti menggunakan mikrotik sebagai *access point*. Dalam penelitian ini dilakukan teknik untuk mendeteksi adanya paket yang tidak dikenal, setelah itu *Arp watch* akan langsung mendeteksi dan segera melakukan pemblokiran terhadap aktivitas tersebut.
2. Rhadita, Sopian Soim, dan Muhammad Fadhil (2020) dalam jurnalnya yang berjudul "Analisis Keamanan Data Seluler terhadap Serangan *Sniffing* menggunakan RTL-SDR "tujuan dari pengujian ini adalah pencarian referensi yang terkait dengan pembahasan mengenai sistem keamanan data, proses pengiriman data,ancaman keamanan data sistem *wireless* dan teknologi jaringan seluler. pengambilan data dilakukan dengan metode *penetration testing*, yaitu metode pengujian penyadapan (*sniffing*) terhadap target yang menerima data berupa SMS dan *email* yang telah dirancang.
3. Angga Novento Ihsana, dan Andi Maslan (2020) dalam jurnalnya yang berjudul "Analisis Keamanan Jaringan Dari Serangan *Packet Data Sniffing* Di PT Raden Syaid Kantor pos piayu Kota Batam ". saat mengirim data atau dari *client* ke *server* atau sebaliknya. kemungkinan terjadi tindakan *sniffing*. karena itu, ketika anda mengirim data atau menerima data melalui koneksi internet.apakah ada *sniffer* yang mencoba mencuri data *sniffing* mengendus-endus atau menyadap paket data yang melintas dalam sebuah jaringan.

2.3 Kerangka Pikir

Kerangka pikir adalah penjelasan sementara terhadap suatu gejala yang menjadi objek permasalahan peneliti. Kerangka pikir ini disusun dengan berdasarkan pada tinjauan pustaka dan hasil penelitian yang relevan. Berikut adalah kerangka pikir pada penelitian ini adalah sebagai berikut :



Gambar 1. Kerangka pikir