BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi saat ini mengalami perkembangan yang cepat, terutama dalam penggunaan jaringan komputer nirkabel. *Internet* semakin luas digunakan dan jumlah pengguna internet di seluruh dunia terus meningkat, hal ini disebabkan karena dengan pengetahuan tentang internet menyebar di berbagai kalangan masyarakat. Namun, kemajuan teknologi informasi juga membawa dampak negatif, terutama dalam bidang keamanan. Saat ini, serangan *cyber* mengancam pengguna individu, bisnis, organisasi pemerintah, dan lainnya. Tujuan dari serangan ini adalah untuk mengganggu integritas sistem-sistem ini, mencuri data, dan menimbulkan kerusakan pada infrastruktur (Rivaldi & Marpaung, 2023). Wifi adalah singkatan dari *Wireless Fidelity*, yang merupakan teknologi untuk pertukaran data menggunakan gelombang radio (nirkabel) di antara berbagai perangkat elektronik seperti komputer, smartphone, tablet, dan lainnya (Abdillah, dkk., 2020).

Sistem keamanan jaringan adalah cara untuk mencegah dan mengidentifikasi pengguna jaringan yang tidak sah (penyusup) di dalam suatu lingkungan jaringan. Tindakan pencegahan ini bertujuan untuk menghalangi akses pengguna yang tidak sah tersebut ke berbagai bagian dalam jaringan yang disusupinya (Rivaldi & Marpaung, 2023). Tujuan keamanan jaringan komputer adalah untuk mengantisipasi risiko yang mungkin timbul dalam bentuk ancaman fisik maupun logis yang dapat mengganggu aktivitas jaringan komputer, baik secara langsung maupun tidak langsung. Selain itu, keamanan jaringan juga bertujuan untuk melindungi data yang tersimpan dalam sistem komputer. supaya aman dari berbagai ancaman. Adanya sebuah keamanan jaringan maka pengguna berharap bahwa informasi yang dikirim sampai pada tujuan dengan baik dan aman (Permana, dkk., 2019).

Praktisi sering membahas dan mempertimbangkan kerentanan jaringan nirkabel terhadap keamanan data, informasi, dan ketersediaan layanan. Sebuah

teori menyatakan bahwa keamanan dan kehandalan suatu jaringan komputer dapat dinilai dari sejumlah unsur berikut:

1. *Privacy* dan *Confidentiality*

   Aspek untuk menjaga informasi dari akses pengguna jaringan yang tidak sah, sementara confidentiality lebih mengarah kepada tujuan dari informasi yang diberikan dan hanya boleh untuk tujuan tersebut saja.

2. *Integrity*

   Aspek yang menekankan akses informasi yang diberikan hanya kepada pengguna tertentu, dengan memastikan bahwa integritas informasi tetap terjaga.

3. *Authentication*

   Aspek ini menekankan pentingnya validasi dari pengguna yang mengakses data, informasi, atau layanan dari suatu institusi.

4. *Availability*

   Aspek yang berkaitan dengan ketersediaan data, informasi, atau layanan, ketika data, informasi atau layanan tersebut diperlukan.

5. *Accec Control*

   Aspek yang berkaitan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.

6. *Non Repudiation*

   Aspek yang terkait dengan pencatatan penggunaan untuk memastikan bahwa pengguna data, informasi, atau layanan tidak dapat mengingkari atau membantah bahwa pengguna telah mengakses data, informasi, atau layanan yang tersedia (Samsumar & Gunawan, 2017).

Dalam suatu jaringan komputer aspek atau indikator diatas adalah hal penting yang harus dipahami dan diperhatikan dengan baik. Banyak terjadi tindakan pencurian informasi pengguna seperti *username, password* dari akun, atau data penting karena itu tidak adanya perlindungan terhadap aspek tersebut dalam suatu jaringan komputer maka jaringan tersebut dapat dikatakan tidak aman.

Kantor Desa Taripa adalah salah satu Kantor Desa yang berada di wilayah Desa Taripa, Kecamatan Angkona, Kabupaten Luwu Timur. Seperti kebanyakan kantor desa lainnya, Kantor Desa Taripa bertanggung jawab atas administrasi

kependudukan, termasuk data-data yang sangat penting untuk kegiatan pemerintahan desa. Oleh karena itu, untuk meningkatkan efisiensi pertukaran informasi antar komputer, kantor desa telah menerapkan jaringan nirkabel. Namun, penggunaan jaringan nirkabel ini juga meningkatkan potensi kerusakan sumber daya dan pencurian informasi sensitif, terutama setelah mengalami kejadian *down* yang mempengaruhi produktivitas, kelemahan keamanan jaringan dan kurangnya perlindungan menjadi faktor utama yang menyebabkan hal tersebut terjadi.

Berdasarkan penjelasan diatas, peneliti mengangkat sebuah judul yaitu Analisis dan Evaluasi Keamanan Jaringan Nirkabel di Kantor Desa Taripa. Dengan demikian peneliti akan melakukan analisis dan evaluasi terhadap sistem keamanan jaringan nirkabe untuk mengetahui tingkat kerentanan dan memberikan penilaian terhadap keamanan jaringan nirkabel yang ada di kantor desa taripa. Evaluasi jaringan akan dilakukan dengan menerapkan metode pengujian penetrasi, dimana serangkaian serangan akan disimulasikan. hasil dari analisis dan evaluasi ini kemudian dapat dijadikan pertimbangan oleh pihak yang terkait.

Dengan adanya penelitian ini, diharapkan jaringan yang digunakan di Kantor Desa Taripa mendapat perhatian lebih dalam hal keamanan, dengan ditingkatkan keamanannya sehingga dapat menjamin kerahasiaan data penduduk, mengurangi risiko pencurian informasi sensitif, dapat memberikan panduan bagi administrator jaringan Kantor Desa Taripa untuk mengidentifikasi kerentanan dalam sistem keamanan yang berpotensi mengancam.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka didapatkan sebuah rumusan masalah dari analisis dan evaluasi keamanan jaringan nirkabel di kantor desa taripa yaitu “Bagaimana menganalisis dan mengevaluasi keamanan jaringan nirkabel di kantor desa taripa?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisis dan mengevaluasi tingkat keamanan jaringan nirkabel di kantor desa Taripa.

1.4 Manfaat Penelitian

Manfaat yang didapatkan dari dilakukannya penelitian di kantor desa taripa ini dibagi dalam tiga hal yaitu sebagai berikut :

1. Bagi Penulis

   Menambah pemahaman dan pengetahuan bagi mahasiswa untuk menganalisis dan mengevaluasi sebuah keamanan jaringan nirkabel.

2. Bagi Instansi

   Membantu administrator jaringan dalam mengetahui resiko ancaman yang ada dan dapat diantisipasi.

3. Bagi Akademik

   Dapat menjadi bahan referensi untuk mahasiswa Universitas Cokroaminoto Palopo dalam mengamankan jaringan dari serangan dan mengenal jenis serangan.

1.5 Batasan Penelitian

Dibatasan penelitian ini ada beberapa point yang menjadi batasan penelitian diantaranya sebagai beriku:

1. Penelitian ini hanya untuk menganalisis dan mengevaluasi keamanan jaringan nirkabel di Kantor Desa Taripa.
2. Analisis dan evaluasi jaringan nirkabel ini hanya ditujukan pada Kantor Desa Taripa.
3. Analisis dan evaluasi keamanan jaringan nirkabel ini dilakukan dengan menerapkan metode *penetration testing*.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Menurut Surahman, dkk., (2020), bahwa kajian teori merupakan merupakan tahap penting dalam proses penelitian yang wajib dilakukan oleh seorang peneliti. Penyusunan kajian teori menjadi landasan dalam penentuan langkah-langkah penelitian. Seorang peneliti harus memahami betul pentingnya perihal penyusunan kajian teori yang baik dan benar.

Menurut Gischa (2023), kajian teori merupakan bagian dari proses penelitian yang mencakup kegiatan mencari teori penelitan, mengidentifikasi literatur, menganalisis dokumen, dan penerapan hasil analisis tersebut sebagai landasan teori untuk penyelesaian masalah dalam penelitian yang dilakukan.

Dari berbagai definisi tersebut, baik dalam lingkup umum maupun menurut ahli, disimpulkan bahwa kajian teori konsep yang sistematis dan terhubung secara logis untuk menguji fakta dan juga variabel dari satu fenomena, sebagai contoh, studi kasus yang penulis angkat yaitu *Analisis dan Evaluasi Keamanan Jaringan Nirkabel di Kantor Desa Taripa.*

1. Analisis

Menurut Kamus Besar Bahasa Indonesia (KBBI), Pengertian Analisis adalah proses penyelidikan terhadap suatu peristiwa dengan tujuan untuk memahami kondisi yang sebenarnya. Analisis sangat dibutuhkan untuk menganalisa dan mengamati sesuatu yang tentunya bertujuan untuk mendapatkan hasil akhir dari pengamatan yang sudah dilakukan.

Menurut Abdi (2021), pengertian analisis adalah usaha dalam mengamati sesuatu secara mendetail dengan cara menguraikan komponen-komponen pembentuknya atau menyusun komponen tersebut untuk dikaji lebih lanjut. Menurut Septiani (2020), bahwa analisis adalah sustu kegiatan berpikir untuk menguraikan atau suatu permasalahan dari unit menjadi unit yang lebih kecil.

Berdasarkan penjelasan diatas dapat disimpulkan bahwa analisis merupakan suatau penyelidikan atau pengamatan yang dilakukan untuk mengetahi dan

memahami keadaan atau fenomena yang terjadi kemudian didapatkan sebuah kesimpulan.

2. Evaluasi

Evaluasi berasal dari kata bahasa Inggris "*evaluation*" yang mengandung konsep nilai. Konsep nilai dalam evaluasi terkait dengan penilaian mengenai kebaikan atau keburukan, kebenaran atau kesalahan, kekuatan atau kelemahan, dan sebagainya. Evaluasi dapat didefinisikan sebagai proses untuk mengevaluasi sesuatu dengan menggunakan standar atau kriteria tertentu.

Menurut Suchman, evaluasi dipandang sebagai sebuah proses menantukan hasil yang telah dicapai beberapa kegiatan yang direncanakan untuk mendukung tercapainya tujuan. Sementara itu, Worthen dan Sanders menggambarkan bahwa evaluasi adalah kegiatan mencari sesuatu: dalam pencarian ini termasuk pengumpulan informasi yang bermanfaat untuk menilai efektivitas suatu program, produksi, prosedur, serta strategi alternatif yang bertujuan untuk mencapai tujuan yang telah ditemukan.

Stufflebeam dan Rukajat (2018), menjelaskan bahwa evalusai merupakan proses penggambaran, pencarian dan pemberian informasi yang sangat bermanfaat bagi pengambil keputusan dalam menentukan alternatif putusan.

Berdasarkan beberapa penjelasan yang dikemukakan para ahli diatas dapat disimpulkan bahwa evaluasi merupakan suatu proses atau langkah untuk menentukan keputusan tentang kualitas sebuah objek yang melibatkan pertimbangan nilai berdasarkan data serta informasi yang telah dikumpulkan dan dianalisis secara sistematis.

3. Keamanan Jaringan

Network Security merupakan sebuah topik dengan cakupan yang sangat luas dan sangat kompleks. *Network security* berkaitan dengan segala aktifitas yang dilakukan untuk mengamankan network, khususnya untuk melindungi *usability*, *availability*, *reliability*, *intergrity* dan *safety* dari *network* dan data. Keamanan jaringan meliputi perangkat keras dan perangkat lunak.

Keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi pengguna atau penggunaan yang tidak sah dalam jaringan komputer. Ini melibatkan langkah-langkah pencegahan dan deteksi untuk

menghentikan penyusup atau pengguna tidak sah dari mengakses sistem jaringan komputer dan komponennya (Fauzan & Purwanto, 2021).

Menurut Mulyadi (2023), *Network security* adalah upaya untuk melindungi jaringan komputer dari serangan yang tidak diinginkan atau akses yang tidak sah. Ini meliputi berbagai teknik yang digunakan untuk mengamankan jaringan, seperti *firewall, enkripsi, autentikasi*, dan pemantauan.

Dari penyataan di atas dapat disimpulkan bahwa keamanan jaringan begitu penting untuk mejaga hal-hal penting yang ada dikomputer dari orang-orang yang tidak bertanggung jawab dan orang-orang yang tidak memiliki haknakses untuk masuk kedalam jaringgan maka dari itu kemanan jaringan harus ada dalam sebuah sistem jaringan komputer.

4. *Wireless*

Wireless merupakan teknologi yang menghubungkan dua perangkat untuk bertukar data tanpa menggunakan media kabel. WiFi, atau *Wireless Fidelity*, adalah standar perangkat yang digunakan untuk komunikasi jaringan lokal tanpa kabel (WLAN), yang mengikuti spesifikasi IEEE 802.11. Beberapa istilah yang umum digunakan dalam jaringan wireless meliputi:

a. *Wireless Local Area Network* (LAN), yaitu jaringan tanpa kabel yang memanfaatkan gelombang radio sebagai media komunikasi antara perangkat. Gelombang radio ini dapat beroperasi pada frekuensi 2,4 GHz (seperti 802.11b, 802.11g, 802.11n) atau 5 GHz (802.11a). Standarisasi Wireless LAN dibagi menjadi beberapa jenis, yaitu 802.11a, 802.11b, 802.11g, dan 802.11n.
b. *Wireless Fidelity* (WiFi) adalah produk/ perangkat yang mematuhi standar 802.11. Pengguna lebih mengenal kartu atau adaptor nirkabel daripada kartu atau adaptor 802.11. Awalnya WiFi ditujukan untuk penggunaan perangkat nirkabel dan jaringan area lokal (LAN), namun saat ini lebih banyak digunakan untuk mengakses *Internet.*
c. *Access Point*, adalah perangkat titik akses nirkabel (Wireless Access Point) yang memungkinkan perangkat nirkabel untuk terhubung ke jaringan menggunakan WiFi, Bluetooth, atau standar nirkabel lainnya.

d. *Captive Portal*, adalah halaman *web* yang digunakan untuk memasukkan nama pengguna dan kata sandi pengguna hotspot. Ketika pengguna mencoba menjelajah internet, akan diarahkan (*redirect*) ke *captive portal* terlebih dahulu untuk mengisi *username* dan *password*. Jika informasi yang dimasukkan sesuai dengan yang ada di database pada radius server, sistem akan membuka koneksi untuk pengguna sehingga mereka dapat terhubung ke jaringan *internet.*

e. *Service Set Identifier* (SSID), merupakan identifikasi/ nama jaringan nirkabel Setiap jaringan nirkabel harus menggunakan SSID tertentu. Peralatan nirkabel dianggap satu jaringan jika tergabung pada SSID (Samsumar, & Hadi, 2018).

5. Kantor Desa Taripa

Kantor Desa Taripa adalah sebuah ksntor pemerintahan yang ada di Desa Taripa. Desa Taripa adalah salah satu desa yang berada diwilayah Kecamatan Angkona, Kabupaten Luwu Timur, Provinsi Sulawesi Selatan. Desa Taripa adalah area pedesaan yang didominasi oleh kegiatan pertanian dan perkebunan sebagai mata pencaharian utama sebagian besar penduduknya. Selain itu, terdapat juga sektor industri kecil yang berfokus pada perdagangan dan pengolahan hasil pertanian dan perkebunan (Desa Taripa, 2023).

Berdasarkan penjelasan diatas, dapat disimpulkan bahwa kantor desa taripa adalah pusat pemerintahan desa taripa yang berada dikawasan pedesaan yang bersifat agraris dan penduduknya banyak bergelut disektor pertanian.

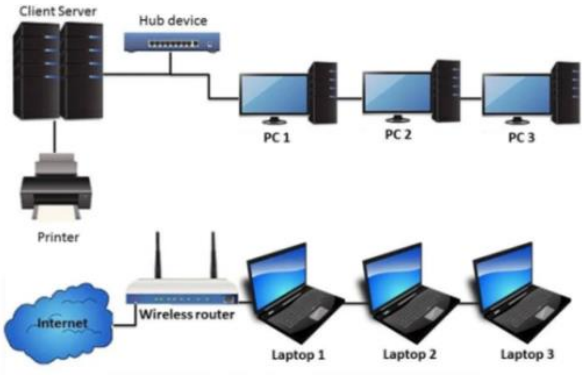
6. Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri dari sejumlah komputer yang dirancang untuk dapat berbagi sumber daya (*printer* dan *CPU*), berkomunikasi melalui (*surel, pesan instan*), serta dapat mengakses informasi browser web. Jaringan komputer merupakan sejumlah komputer yang terpisah akan namun saling berhubungan untuk menjalankanya. Dua buah komputer misalnya dikatakan terkoneksi bila keduanya dapat saling bertukar informasi. Bentuk koneksi dapat melalui kawat tembaga, serat optik, gelombang mikro, satelit.

Menurut Papaceda, dkk., (2023), Jaringan komputer adalah sekumpulan dua atau lebih komputer yang saling terhubung untuk bertukar data. Hubungan antara

komputer-komputer tersebut dapat dilakukan menggunakan media kabel atau nirkabel.

Dari beberapa paparan pengertian jaringan komputer diatas dapat disimpilkan bahwa jaringan komputer adalah kumpulan dua atau lebih komputer yang saling terhubung antar komputer untuk melakukan komunikasi, berbagi informasi, dan pengiriman data melalui kabel maupun nirkabel.



Gambar 1. Skema Jaringan Komputer
Sumber: *Computory.com*, diakses 23 November 2023, pukul 21.20 wita

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

a. LAN atau *Local Area Network* adalah konsep yang menghubungkan perangkat jaringan dalam jarak yang relatif pendek. Biasanya di gunakan untuk gedung sekolah, kantor, rumah, dll. Konsep jaringan LAN ini cenderung menggunakan konektivitas tertentu, terutapa *Ethernet* dan Token Ring. Ada juga LAN yang menggunakan teknologi jaringan *Wireless* atau nirkabel dengan WI-FI dan dikenal dengan nama *Wireless Local Area Network* (WLAN).
b. MAN (*Metropolitan Area Network*) MAN atau *Metropolitan Area Network* adalah konsep yang menghubungkan perangkat jaringan dari satu Kota ke Kota lainnya. Jika penggunaan LAN sudah tidak memungkinkan untuk membangun jaringan maka jaringan MAN akan di gunakan, karena cangkupannya lebih besar dari LAN maka MAN menggunakan perangkat khusus dan memerluka operator telekomunikasi yang bertugas sebagai penguhubung antar jaringan komputer.

c. WAN (*Wide Area Network*) WAN atau *Wide Area Network* adalah konsep yang menghubungkan perangkat jaringan komputer yang mencangkup wilayah super luas dan menggunalan peralatan yang super canggih apabila di bandingkan dengan MAN dan LAN (Astuti, 2020).

7. Topologi Jaringan

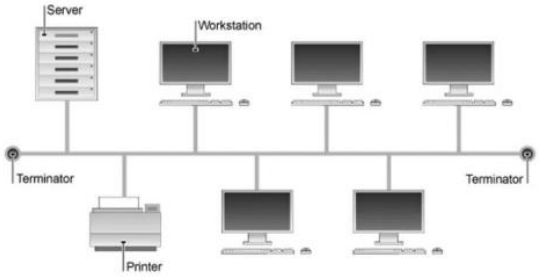
Topologi jaringan adalah metode untuk menghubungkan komputer satu dengan yang lain dalam sebuah jaringan, di mana pilihan topologi ini dipengaruhi oleh pertimbangan biaya, kecepatan akses data, skala jaringan, dan tingkat konektivitas, yang semuanya berdampak pada kualitas dan efisiensi jaringan (Ofrianky, 2022).

Topologi merupakan struktur fisik dalam menghubungkan setiap node pada sebuah jaringan. Pada jaringan sedehana *local area network* (LAN) dikenal 3 topologi yang paling sering digunakan yaitu Topologi Bus, Star (Bintang) dan Ring (Cincin). Seiring perkembangan zaman topologi dikenal dengan topologi Tree (Pohon), *Extended Star* dan *Mesh* (Tak Beraturan) (Setiawan, Dkk, 2022).

Berdasarkan penjelasan beberpa teori diatas penulis menyimpulkan bahwa topologi jaringan adalah bentuk teknik untuk menghubungkan server kepada komputer lainnya.

a. Topologi Bus

Topologi jaringan komputer bus disusun secara linier menggunakan satu kabel coaxial, di mana setiap komputer terhubung melalui konektor BNC ke kabel tersebut. Kabel coaxial harus diakhiri dengan terminasi pada kedua ujungnya untuk menjaga integritas sinyal.



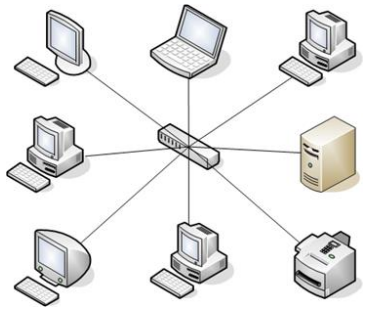
Gambar 2. Topologi Bus
Sumber: Kompas.com, diakses 23 November 2023, pukul 21.31 wita

Kelebihan dari topologi jaringan ini mirip dengan topologi ring, yaitu menggunakan sedikit kabel dan mengurangi biaya pemasangan.

Kekurangan dari topologi jaringan ini adalah gangguan pada satu komputer dapat mempengaruhi jaringan komputer lainnya, sulit mendeteksi gangguan, sering terjadi antrian data, dan memerlukan repeater jika jaraknya terlalu jauh.

b. Topologi Star

Topologi jaringan ini membentuk seperti bintang karena setiap komputer terhubung ke sebuah hub atau switch menggunakan kabel UTP. Dalam topologi ini, hub atau switch berperan sebagai pusat dari jaringan yang mengontrol aliran data. Jika komputer 1 ingin mengirim data ke komputer 4, data akan dikirimkan ke switch dan langsung diteruskan ke komputer tujuan tanpa harus melalui komputer lain. Topologi jaringan komputer ini sangat umum digunakan saat ini karena memiliki banyak kelebihan.kelebihannya lebih banyak.



Gambar 3. Topologi Star
Sumber: *Pinhome.id* diakses 23 November 2023, pukul 21.34 wita

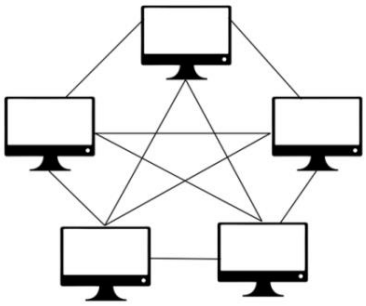
Kelebihan dari topologi jaringan ini adalah kemudahan dalam mendeteksi komputer yang mengalami gangguan, serta kemudahan dalam menambah atau mengurangi komputer tanpa mengganggu yang lain. Selain itu, tingkat keamanan data juga lebih tinggi.

Kekurangan dari topologi jaringan ini adalah biaya pemasangan yang tinggi karena membutuhkan banyak kabel dan perangkat *switch/hub*. Selain itu, stabilitas jaringan sangat bergantung pada keandalan *switch/hub* pusat; jika *switch/hub* mengalami gangguan, seluruh jaringan dapat terganggu.

c. Topologi Mesh

Dalam topologi ini, setiap komputer terhubung langsung satu sama lain menggunakan kabel tunggal dalam jaringannya. Dengan demikian, pengiriman

data dapat mencapai komputer tujuan secara langsung tanpa harus melalui komputer lain atau *switch/hub*.



Gambar 4. Topologi *Mesh*
Sumber: Tekno.kompas.com, diakses 23 November 2023, pukul 21.37 wita

Kelebihan dari topologi jaringan ini adalah data dapat dikirim lebih cepat secara langsung ke tujuan tanpa melalui komputer lain, serta gangguan pada satu komputer tidak akan mempengaruhi kinerja komputer lain.

Kekurangan dari topologi jaringan ini adalah biaya pemasangan yang tinggi karena membutuhkan jumlah kabel yang besar serta setiap komputer harus dilengkapi dengan banyak port I/O.

8. *Brute Force Attack*

Serangan *brute force* adalah teknik di mana penyerang menggunakan percobaan berulang-ulang untuk menebak informasi login, kunci enkripsi, atau menemukan halaman *web* yang tersembunyi. Para peretas mencoba semua kemungkinan kombinasi dengan harapan dapat berhasil menebak dengan benar. Teknik ini dilakukan secara kasar dan intensif, dengan upaya untuk memaksa masuk ke akun pribadi. Meskipun merupakan metode serangan lama, *brute force* tetap efektif dan populer di kalangan peretas karena tergantung pada kompleksitas dan panjang kata sandi yang menjadi sasaran, waktu yang dibutuhkan untuk memecahkannya bisa bervariasi mulai dari beberapa detik hingga bertahun-tahun (Yudi mulyanto, 2022)

Berdasakan penjelasan diatas, *brute force* adalah jenis serangan yang menggunakan dapat menebak informasi login dengan melakukan kombinasi-kombinasi huruf dan angka.

9. *Distributed Denial of Service* (DDOS)

Beberapa serangan paling umum namun mengerikan pada SDN adalah serangan DoS dan DdoS. Serangan tersebut mempengaruhi kinerja dan perilaku jaringan. Dengan menghabiskan sumber daya, mereka menonaktifkan atau menurunkan versi layanan jaringan , dan *host* yang sah tidak dapat berkomunikasi dengan pengontrol SDN atau mengirim paket di jaringan. Serangan DoS atau DDoS dicapai di SDN dengan menciptakan beberapa aliran baru yang membanjiri *bandwidth* bidang kontrol, sakelar *OpenFlow*, dan pengontrol SDN, yang mengakibatkan kegagalan jaringan pada *host* yang sah.

Lebih khusus lagi, penyerang menghasilkan beberapa aliran baru yang memiliki alamat *IP* palsu tetapi dikirim dari satu sumber (DoS) atau beberapa sumber (DDoS). Alamat palsu ini tidak cocok dengan aturan aliran apa pun yang ada di tabel aliran *switch OpenFlow*, yang mengakibatkan situasi tabel hilang. Situasi seperti ini menghasilkan pesan paket dalam jumlah besar yang dikirim ke pengontrol *SDN* dari saklar *OpenFlow* korban, yang menghabiskan *bandwidth* komunikasi, memori, dan *CPU* baik di bidang kontrol maupun data SDN (Eliyan. 2021).

10. *Man In The Middle Attack* (MITM)

Serangan *Man In The Middle* (MITM) memanfaatkan fakta bahwa server *HTTPS* mengirimkan sertifikat dengan kunci publiknya ke *browser web*. Jika sertifikat ini tidak dipercayai, semua komunikasi dapat menjadi rentan terhadap pencurian data. Serangan semacam itu menggantikan sertifikat asli yang mengautentikasi server *HTTPS* dengan sertifikat yang telah dimodifikasi. Serangan berhasil jika pengguna tidak memeriksa sertifikat saat *browser* mengirimkan peringatan. Hal ini terjadi terlalu sering terutama di antara pengguna yang sering menghadapi sertifikat yang ditandatangani sendiri saat mengakses situs intranet.

Serangan *MITM* umumnya ditargetkan pada individu, dan seringkali tidak terdeteksi atau tercatat dalam statistik. Ketika operator ekonomis menjadi target serangan, seringkali serangan tersebut disembunyikan dari publik untuk menjaga reputasi perusahaan. Hanya pada serangan skala besar, dampak kerusakan yang diakibatkannya dapat terungkap sepenuhnya (Wahanani, 2020).

11. Perangkat Keras Jaringan (*Hardware*)

Perangkat keras jaringan komputer merupakan perangkat yang digunakan untuk mencapai tujuan dari fungsi jaringan komputer itu sendiri, seperti berbagi sumber daya, berkomunikasi dan lain sebagainya. Ada banyak perangkat jaringan komputer yang berperan penting dalam terciptanya suatu jaringan, diantaranya sebagai berikut:

a. *Server*

Server adalah perangkat atau komputer khusus yang menyediakan berbagai layanan atau servis kepada client yang terhubung kepadanya. Biasanya, server dilengkapi dengan spesifikasi hardware yang tinggi, terutama dalam hal *prosesor* (sering kali menggunakan *Intel Xeon*) dan kapasitas RAM (umumnya lebih dari 16GB). Karena server harus menjalankan tugas-tugas multitasking yang berat, tidak mengherankan jika biaya untuk membangun komputer server cukup tinggi. Selain itu, sistem operasi yang digunakan juga khusus, seperti *windows server* atau *linux debian.*

b. *Router*

Router adalah perangkat jaringan yang menghubungkan dua jaringan atau lebih untuk memungkinkan pengiriman data antar jaringan-jaringan tersebut. Dengan *router*, kita dapat menghubungkan jaringan yang berbeda, seperti menghubungkan jaringan 192.168.2.0/24 dengan jaringan 200.200.200.0/24. Secara prinsip, cara kerja *router* mirip dengan *bridge* dalam hal meneruskan paket data serta membagi atau menggabungkan segmen-segmen jaringan, namun perbedaannya terletak pada lokasi *router* yang berada pada lapisan ketiga dalam model *OSI*.



Gambar 5. *Router*
Sumber: nesabamedia.com, diakses 23 November 2023, pukul 21.55 wita

c. *Modulator*

Demodulator atau yang sering disingkat dengan modem adalah perangkat jaringan yang berfungsi mengubah sinyal digital menjadi sinyal analog atau sebaliknya. Data yang diberikan kepada komputer ke modem umumnya berbentuk sinyal digital. Maka dari itu, ketika modem mendapatkan data berbentuk sinyal analog, modem harus merubahnya terlebih dahulu menjadi sinyal digital agar dapat diproses lebih lanjut oleh komputer. Terdapat berbagai jenis modem yang bisa kita jumpai, semisal modem *ADSL*, modem *USB*, modem Mifi dan lain sebagainya.



Gambar 6. Modem
Sumber: Medium.com, diakses 23 November 2023, pukul 22.05 wita

d. *Bridge*

Bridge adalah perangkat jaringan yang berfungsi untuk memperluas suatu jaringan dan mengelompokkan segmen-segmen jaringan. *Bridge* melakukan pemetaan alamat *Ethernet* dari setiap perangkat pada segmen-segmen jaringan yang berbeda. Selanjutnya, bridge melakukan seleksi dan mengizinkan hanya data tertentu untuk dilewati. Cara kerja bridge adalah dengan mengenali alamat *MAC* yang mengirimkan data ke jaringan, kemudian bridge secara otomatis membangun tabel internal yang digunakan untuk menentukan pengalihan atau penyaringan data antar segmen-segmen jaringan.



Gambar 7. *Bridge*
Sumber: nesabamedia.com, diakses 24 November 2023, pukul 19.45 wita

e. *Hub*

Hub adalah salah satu perangkat jaringan yang berperan mengubah sinyal transmisi jaringan, memungkinkan beberapa komputer untuk saling terhubung. Namun, *hub* tidak dapat mengatur alur jalannya suatu data, sehingga setiap paket data yang melewati *hub* akan *dibroadcast* ke semua *port* sampai paket data yang dimaksud sampai ke tujuan karena inilah membuat paket data yang dikirim mengalami collision atau tabrakan data. Untuk saat ini, penggunaan *hub* sangat jarang karena kebanyakan orang lebih memilih *Switch* karena fitur-fiturnya yang lebih canggih dibandingkan *hub*.



Gambar 8. *Hub*
Sumber: nesabamedia.com, diakses 24 November 2023, pukul 19.49 wita

f. *Swicth*

Switch adalah perangkat jaringan yang berfungsi serupa dengan *hub*, tetapi lebih canggih karena mampu mengelola masalah tabrakan data. Selain itu, *switch* memiliki keunggulan dalam hal kecepatan transfer data dan kapasitas jaringan yang lebih baik dibandingkan *hub*. Perangkat ini tidak hanya membagi sinyal tetapi juga melakukan penyaringan paket data sebelum meneruskannya ke jaringan tujuan. *Switch* biasanya dipasang di ruang lab komputer atau kantor di mana setiap komputer klien terhubung ke *switch* melalui kabel LAN sebelum terhubung ke *router*.



Gambar 9. *Swicth*
Sumber: nesabamedia.com, diakses 24 November 2023, pukul 19.52 wita

g. Kabel

Kabel jaringan adalah media transmisi berupa kabel yang dipakai untuk menghubungkan dua atau lebih komputer guna bertukar data. Meskipun saat ini teknologi nirkabel semakin banyak digunakan, penggunaan kabel jaringan tetap populer dan diminati. Terdapat beberapa jenis kabel yang umum digunakan, seperti *UTP, STP, Coaxial,* dan serat optik. Pemilihan jenis kabel biasanya disesuaikan dengan jenis jaringan dan perangkat yang digunakan. Contohnya, untuk menghubungkan komputer dengan *switch, hub, atau router,* kabel *UTP* adalah pilihan yang paling umum digunakan.



Gambar 10. Kabel
Sumber: nesabamedia.com, diakses 24 November 2023, pukul 19.55 wita

h. *Access Point*

Menurut Zakaria (2020) *access point* adalah perangkat yang terdiri dari antenna dan transceiver yang berfungsi untuk mengurim dan menerima sinyal dari *client* atau sebaliknya. Dengan adanya AP ini memungkinkan pengguna dapat terhubung dengan jaringan LAN secara nirkabel. Dengan kata lain, *access point* ini berfungsi menghubungkan dua jenis jaringan yang berbeda, yaitu antara jaringan nirkabel dan jaringan LAN.



Gambar 11. *Access Point*
Sumber: nesabamedia.com, diakses 24 November 2023, pukul 19.58 wita

12. Kali Linux

Kali linux adalah salah satu distribusi linux yang canggih untuk *penetration testing* dan audit keamanan. Kali linux merupakan pembangunan kembali *backtrack* linux secara sempurna, mengikuti sepenuhnya kepada standar pengembangan *debian*. Semua infrastruktur baru telah terintegrasi ke dengan baik, seluruh alat atau tools telah direvisi dan diintegritaskan, dan kami menggunakan *Git* untuk *VCS* nya (Rusdi & Prasti, 2019).

Kali Linux merupakan distribusi sistem operasi berbasis *debian* yang dikhususkan untuk para profesional di bidang keamanan siber, analis jaringan, dan penguji penetrasi. Sistem operasi ini bersifat open source dan dapat digunakan secara gratis, dilengkapi dengan beragam alat yang sudah terpasang untuk berbagai keperluan pengujian keamanan. (Yohan, 2023).

Menurut Lamichhane (Sanjaya, 2020) kali linux merupakan salah satu distro linux yg dikenal cukup populer untuk kegunaan uji keamanan jaringan dan digital *forensic*. Kali linux memiliki kurang lebih tools uji keamanan dan mampu berjalan di beberpa arsitektur komputer.

Dari penjelasan diatas dapat disimpulkan bahwa kali linux adalah sebuah *software* yang berbasis *debian* yang dapat digunakan sebagai keamanan *siber*, pengujian jaringan dan lain-lainnya.

13. *VirtualBox*

Manurut Alfiadzar (2022), *virtualbox* adalah sebuah perangkat lunak sumber terbuka yang berhubungan dengan teknologi virtualisasi. *Virtualisasi* adalah teknologi yang memungkinkan untuk membangun komputer PC virtual di dalam komputer fisik, yang dapat beroperasi secara mandiri dari sistem operasi utama. Komputer host mensimulasikan semua jenis perangkat keras yang terkait dengan mesin *virtual*.

Menurut Fahri, (2020) *Virtualbox* adalah sebuah aplikasi sumber terbuka yang terkait dengan teknologi *virtualisasi*. *Virtualisasi* yang dimaksud adalah membuat mesin *virtual PC* yang dapat beroperasi secara independen didalam sistem utama. Dengan menggunakan *virtualbox* maka kita bisa menjalankan sistem operasi diatas sistem operasi.

Menurut Anam, dkk., (2020), *virtualbox* adalah perangkat lunak *virtualisasi* yang dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama. *Virtualbox* Fungsi utamanya adalah untuk melakukan *virtualisasi* sistem operasi dan *virtualbox* juga dapat digunakan untuk membuat jaringan komputer *virtual*.

Dari beberapa penjelasan diatas mengenai *virtualbox* dapat disimpulkan bahwa *virtualbox* adalah sebuah perangkat lunak yang dapat digunakan untuk melakukan visualiasi dari sebuah situasi yang sangat mirip dengan situasi tersebut atau dengan kata lain untuk menggambarkan sebuah situasi tertentu dalam bentuk *virtual*.

14. *Drow.io*

Menurut Eko (2022), bahwa *draw.io* merupakan sebuah situs yang didesain khusus untuk menggambar diagram secara *online*. Untuk mengaksesnya hanya diperlukan *browser* yang mendukung HTML5 dan juga koneksi *internet*. *Draw.io* sudah terintegrasi dengan *google drive* untuk penyimpanan file selain mengekspor dalam bentuk JPG/PNG/SVG/XML.

Menurut Ranuwinata dan Suryadi (2022), bahwa *draw.io* merupakan situs *web* & aplikasi buat menciptakan dialog alur. *Draw.io* membantu pada mendesain atau menciptakan diagram *use case* dan diagram aktivitas.

15. *Google Chrome*

Menuut Pradnyana (2022), *google chrome* merupakan aplikasi *browser* di internet yang banyak digunakan. Dengan ini, kita dapat mengeksplor atau berselancar di internet untuk mencari materi pelajaran khusus dibuat untuk keperluan pendidikan.

Google Chrome adalah *platform browser web* yang dikembangkan oleh *google*. *Platform browser web* ini pertama kali dirilis pada tahun 2008 untuk *platform microsoft windows* dan dibangun menggunakan komponen *software* gratis dari *apple webkit* dan *mozilla firefox*. *Google* bertujuan untuk menciptakan produk yang lebih baik untuk dunia modern. Pada saat ini, hanya ada dua *browser* utama yang tersedia di pasar yang memiliki pangsa pasar utama , yaitu *internet explorer* dan *firefox* (Soffya, 2022).

2.2 Hasil Penelitian yang Relevan

1. “Analisis Keamanan Jaringan *Wireless* menggunakan Metode *Penetration Testing Execution Standard* (PTES)” oleh Saputra, dkk., (2023). Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal merupakan tempat layanan publik yang berada di Kecamatan Slawi Kabupaten Tegal yang saat ini menggunakan teknologi jaringan *Wireless Local Area Network* (WLAN) sebagai sarana akses *internet* dan untuk berbagai keperluan baik bersifat administrasi maupun layanan lainnya. Jaringan *wireless* harus memiliki keamanan yang baik untuk menghindari berbagai ancaman kejahatan, maka dari itu diperlukan analisis kemanan jaringan dengan metode *Penetration Testing Execution Standard* (PTES) yaitu suatu kerangka kerja atau panduan yang digunakan sebagai acuan melaksanakan penetrasi jaringan. Dari hasil pengujian sebanyak lima kali menggunakan *virtual machine* sistem operasi kali linux dengan jenis serangan bypassing mac authentication, arp spoofing masing-masing berstatus berhasil sedangkan *cracking the encryption* berstatus mengalami tiga kegagalan dan dua berhasil. Berdasarkan hasil pengujian tersebut dapat disimpulkan sistem keamanan jaringan *wireless* cukup aman namun perlu dilakukan beberapa perbaikan pada sistem konfigurasi serta topologi jaringannya untuk memperkuat sistem keamanan serta menimimalisir ancaman kejahatan (Saputra, dkk., 2023)

   Persamaan penelitian ini dengan penelitian yang relevan adalah melakukan analisis dan evaluasi jaringan pada tingkatan desa. Sedangkan perbedaannya adalah pada penelitian yang relevan analisis dan evaluasi tersebut dilakukan pada balai desa, sedangkan penelitian ini dilakukan di kantor desa.

2. “Analisis Keamanan Jaringan *Wireless* Terhadap Serangan Brute Force Menggunakan Metode Penetration Testing Pada Kantor DesaPelalan Kecamatan Lamasi Timur Kabupaten Luwu” oleh Novita, dkk., (2023). Dalam penelitian ini Sistem keamanan jaringan kantor desa pelalan dengan menggunakan penetration testing. Adapun penerapan dari hasil penetration testingyang telah digunakan dari tahap planing and preparation sampai Reporting. Pada penelitian ini dibagi atas pembahasan hasil, pengumpulan

data, hasil analisis percobaan serangan dan kerentanan jaringan serta memberikan langkah dan solusi untuk mengurangi kerentanan pencurian data yang ditemukan pada jaringan wireless kantor Desa Pelalan. Jenis penelitian yang diguanakan adalah penelitian deskriptif kualitatif. Penelitian deskriptif adalah metode penelitian yang berusaha menggambarkan objek atau subjek yang diteliti secara mendalam, luas, dan terperinci. Metode penelitian ini digunakan untuk memecahkan dan menjawab masalah dengan mengumpulkan data, klafikasi, analisis, kesimpulan, dan laporan (Novita, dkk., 2023).

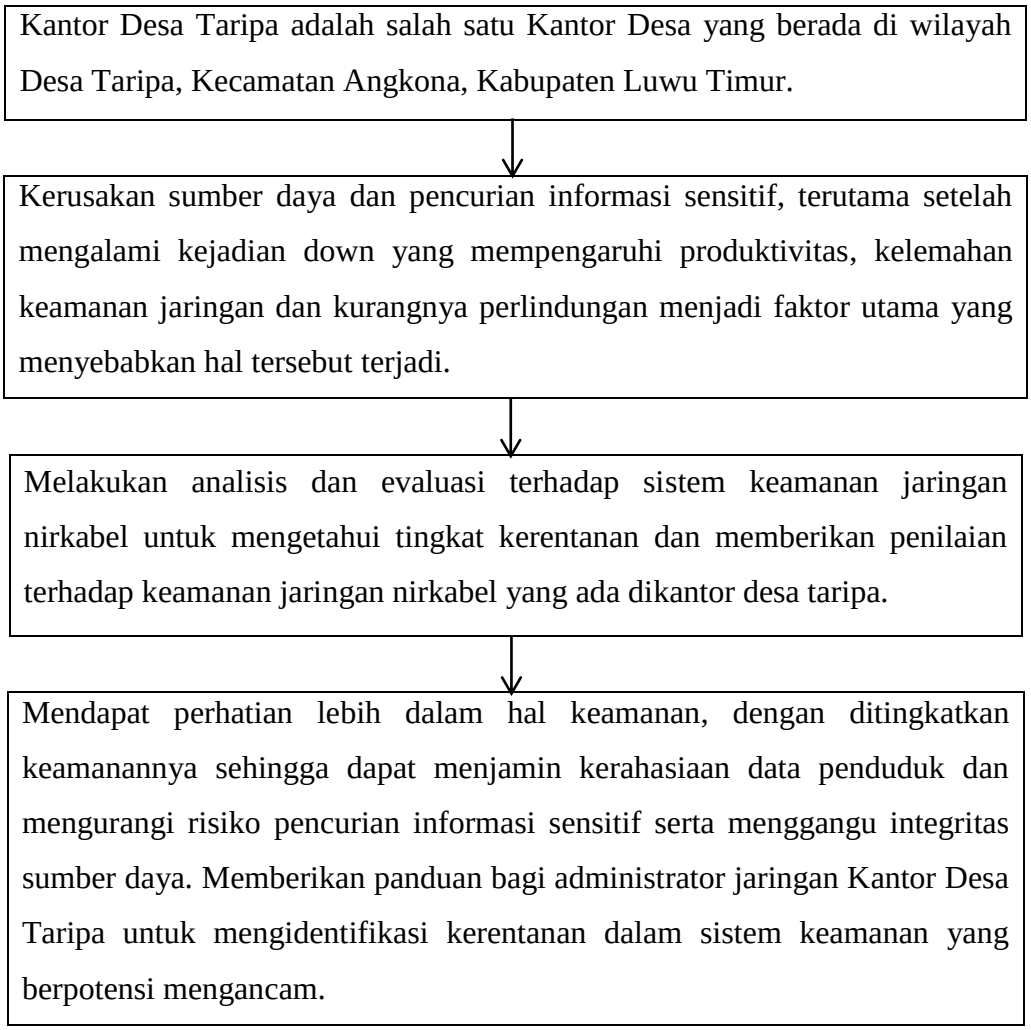
Persamaan yaitu pada metode penyerangan yang sama-sama menggunakan brute force. Untuk perbedaannya adalah pada penelitian yang relevan menggunakan satu serangan sedangkan pada penelitian ini menggunakan tiga jenis serangan.

3. "Analisis *Network Security* Komputer Tingkat Desa Menggunakan Metode *Security Policy Development Life Cycle* (SPDLC)" oleh Yunanri, dkk., (2021). Dunia telekomunikasi semakin berkembang mulai pada tahapan Generasi (1G), Generasi2 (2G), Generasi3 (3G), sampai tahap generasi 4 (4G). manfaat tekneologi ilmu komputer banyak memeberikan kemudahan-kemudahan atau fiture-fiture menarik dan canggih, agar di manfaatkan oleh masyarakat luas di Indonesia salah satunya, pengguna wifi pada pemerintahaan tingkat Desa. Adanya kendala yang menyebabkan menurunnya performa akses *internet*, maka dibutuhkan langkah-langkah menganalisa kendala, faktor utama yang menyebabkan, menurunya performa akses internet kantor Desa. Salah satu metode yang dapat dikembangkan adalah *security policy development life cycle* (SPDLC) dimana berkaitan dengan keamanan jaringan yang mikrotik. suatu faktor yang penting dalam dunia teknologi. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian data-data yang dianggap penting oleh suatu lembaga (Yunanri, dkk., 2021).

   Persamaan penelitian ini dengan penelitian yang relevan adalah melakukan analisis terhadap jaringan nirkabel. Sedangkan perbedaannya terletak metode penelitian yang digunakan.

2.3 Kerangka Pikir

Kerangka pikir adalah penjelasan sementara terhadap suatu gejala yang menjadi objek permasalahan perpaduan antara teori dengan fakta, kajian kepustakaan dilokasi penelitian. Adapun yang menjadi kerangka pikir dalam penelitian ini adalah sebagai berikut:



Gambar 12. Kerangka Pikir
Sumber: Penulis (2023)