ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET TERHADAP SERANGAN *SYSTEM FAILURE* PADA TOKO SERVICES W-ELEKTRIK BATAM

SKRIPSI

Oleh:

Windri Nofedrinata

180210047

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

2023

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET TERHADAP SERANGAN *SYSTEM FAILURE* PADA TOKO SERVICES W-ELEKTRIK BATAM

SKRIPSI

Untuk memenuhi salah satu syarat
memperoleh gelar sarjana

Oleh:
Windri Nofedrinata
180210047

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

2023

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini saya:

Nama	: Windri Nofedrinata
Npm	: 180210047
Fakultas	: Teknik dan Komputer
Program studi	: Teknik Informatika

Menyatakan bahwa "Skripsi" yang saya buat dengan judul:

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET TERHADAP SERANGAN SYSTEM FAILURE PADA TOKO SERVICES W-ELEKTRIK BATAM

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, didalam naskah Skripsi. Ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata didalam Skripsi. Ini dapat dibuktikan terdapat unsur-unsur Plagiasi, saya bersedia naskah Skripsi. Ini digugurkan dan Skripsi yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.
Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 27 January 2023

Windri Nofedrinata

180210047

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET TERHADAP SERANGAN SYSTEM FAILURE PADA TOKO SERVICES W-ELEKTRIK BATAMA

SKRIPSI

Untuk memenuhi salah satu syarat
memperoleh gelar sarjana

Oleh:
Windri Nofedrinata
180210047

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera dibawah ini

Batam, 27 Januari 2023

Andi Maslan, S.T., M.SI.
Pembimbing

ABSTRAK

Jaringan komputer mempunyai dua media transmisi data yaitu kabel dan nirkabel. Sedangkan system failure adalah kegagalan dari sistem atau komponen dalam jaringan yang menyebabkan terganggunya konektivitas atau performa jaringan. Penelitian ini membahas evaluasi tingkat keamanan fasilitas Wi-Fi di Toko Services W-elektrik Batam. Metode yang digunakan Observasi pengambilan data menggunakan Aplikasi InSSIDer dan Ettercap, Inssider adalah sebuah tools analisis jaringan wireless yang digunakan untuk mengevaluasi kualitas sinyal dan menemukan masalah dengan jaringan wireless. Ettercap adalah tools packet sniffer yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Hasil dari penelitian ini adalah dengan terdeteksinya keberadaan dan keamanan Wi-Fi yang terbuka atau tanpa pengamanan dan terekamnya username dan password. Oleh karena itu disarankan kepada pihak Toko Services W-Elektrik Batam lebih meningkatkan proteksi jaringan agar tidak mudah di retas.

Kata Kunci : Jaringan, Ettercap, *System Failure*.

ABSTRACT

Computer networks have two data transmission media, namely wired and wireless. Meanwhile, system failure is a failure of a system or component in a network that disrupts network connectivity or performance. This study discusses the evaluation of the level of security of Wi-Fi facilities at the Batam W-electric Service. The method used Observation of data collection using the InSSIDer and Ettercap applications, Inssider is a wireless network analysis tool used to evaluate signal quality and find problems with wireless networks. Ettercap is a packet sniffer tool that is used to analyze network protocols and audit network security, which also has the ability to block traffic on LAN networks, steal passwords, and perform active eavesdropping on common protocols. The results of this study are the detection of the presence and security of Wi-Fi that is open or without security and the username and password are recorded. Therefore it is suggested to the Batam W-Electric Service Store to increase network protection so that it is not easily hacked.

Keywords: Jaringan, Ettercap, *System Failure*.

KATA PENGANTAR

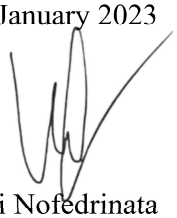
Segala Puji Bagi Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika di Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada :

1. Rektor Universitas Putera Batam, Ibu Nur Elfi Husda, S.Kom.,M.SI.
2. Dekan Fakultas Teknik dan Komputer, Bapak Welly Sugianto, S.T.,M.Mm.
3. Ketua Program Studi Teknik Informatika Bapak Andi Maslan,.S.T.,M.SI. Sekaligus sebagai Pembimbing Skripsi.
4. Rahmat Fauzi, S.Kom., M.Kom. selaku pembimbing akademik selama saya berkuliah di program studi Teknik Informatika Universitas Putera Batam.
5. Dosen dan Staff Universitas Putera Batam
6. Kedua orang Tua penulis yang selalu berdoa dan mendukung penulis hingga selesai tugas akhir skripsi ini
7. Rekan kerja yang mau memberi ilmunya dan berbagi pendapat dalam pembuatan skripsi ini

8. Rekan-rekan mahasiswa Universitas Putera Batam yang juga memberikan doa dan dukungan
9. Teman-teman kampus yang selalu memberikan dukungan kepada penulis dalam menyelesaikan skripsi ini
10. Serta pihak yang tidak dapat disebutkan satu per satu Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Aamiin.

Batam,27 January 2023



Windri Nofedrinata

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan teknologi berbasis *Wireless* (Wi-Fi) sudah semakin banyak, baik digunakan untuk pendidikan maupun untuk komersial. Toko Services w-elektrik batam adalah toko yang bergerak di bidang jasa perbaikan khususnya *handphone* dan laptop serta penyedia *sparepart* elektronik. Toko services w-elektrik batam dibuka pada tahun 2020, dalam pengerjaan suatu perbaikan membutuhkan komputer dan laptop yang sangat membutuhkan akses internet atau berbasis *Wireless* (Wi-fi).

Wireless Fidility atau yang sering disebut dengan Wi-Fi merupakan perangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (*Wireless Local Area Network*/WLAN) yang didasari pada spesifikasi IEEE 802.11 dalam (Samsumar, 2017). Jaringan nirkabel atau *wireless* yang saat ini sangat sering digunakan bahkan dikembangkan karena jaringan nirkabel bisa digunakan pada setiap aspek skenario. Namun penggunaan jaringan nirkabel tidak luput dari kejahatan-kejahatan siber yang dilakukan dari pihak yang tidak bertanggung jawab yang bisa berakibat merugikan orang lain. Berdasarkan data Badan Siber dan Sandi Negara (BSSN), pada tahun 2020 terdapat total 495,4 juta upaya kejahatan siber di Indonesia, jauh lebih tinggi di bandingkan tahun 2019 yang hanya berkisar 290,3 juta upaya kejahatan siber. Terjadinya kenaikan serangan siber pada tahun 2020 (BSSN, 2020). Maka dari itu pentingnya menerapkan suatu sistem keamanan jaringan yang cukup aman, sehingga bisa meminimalisir serangan-serangan

terhadap jaringan, berupa pencurian data, ketidaktersediaan data atau informasi, hilangnya integritas atau keaslian data atau informasi dan lainnya yang berakibat merugikan. Pada toko services w-elektrik batam diketahui ada serangan trojan pada Jaringan Komputer yaitu serangan aktif. Serangan aktif adalah penyerang mendapatkan akses tidak sah ke jaringan dan kemudian memodifikasi data, baik menghapus, mengenkripsi atau merusaknya. Seperti yang sudah di ketahui toko w-elektrik batam sering terjadinya kegagalan sistem saat menggunakan software baik tools eror dan data yang corrupt oleh serangan trojan pada jaringan internet jelas ini dapat mengakibatkan terkendalanya pengerjaan perbaikian mau *software* ataupun *hardware*. Sehingga peneliti ingin menganalisis apa penyebab sering terjadinya *system failure* pada saat terkoneksi internet mau kabel ataupun nirkabel sehingga peneliti harus menerapkan keamanan jaringan.

Untuk menerapkan sistem keamanan jaringan yang cukup aman perlu dilakukan analisa terhadap sistem keamanan jaringan. Hasil dari analisa terhadap sistem keamanan bisa dijadikan sebagai bahan untuk melakukan evaluasi terhadap sistem keamanan jaringan. Pada toko services w-elektrik batam telah menyediakan fasilitas berupa jaringan nirkabel untuk digunakan sebagai media dalam membantu memenuhi kebutuhan informasi. Berdasarkan hal tersebut peneliti mengangkat judul **"ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET TERHADAP SERANGAN SYSTEM FAILURE PADA TOKO SERVICES W-ELEKTRIK BATAM".**

1.2 Indentifikasi Masalah

Tingkat kegagalan merupakan masalah yang selalu diupayakan untuk diminimalisir oleh suatu da dan juga dilakukan oleh toko sevices w-elektrik batam Identifikasi masalah sebagai berikut.

1. Adanya serangan trojan mengakibatkan *system failure.*
2. Dalam jaringan-jaringan komputer atau internet yang memiliki tingkat keamanan yang masih rendah dan rentan terinfeksi trojan toko sevices w-elektrik batam.

1.3 Rumusan Masalah

Berdasarkan uraian latar belakang informasi yang diberikan di atas, maka permasalahan yang dapat diangkat dalam penelitian ini adalah bagaimana menganalisis keamanan jaringan fasilitas internet terhadap serangan *system failure* pada toko services w-elektrik batam.

1.4 Batasan Masalah

1. Peneliti hanya menawarkan langkah-langkah yang harus diterapkan untuk mencegah serangan, bukan pemutakhiran keamanan jaringan yang ada trojan kembali.
2. Peneliti hanya Evaluasi keamanan fasilitas internet (Wi-Fi) toko sevices w-elektrik
3. Peneliti hanya fokus menganalisis keamanan jaringan fasilitas insternet (Wi-Fi) terhadap serangan trojan dengan menggunakan tools Ettercap dan inSSIDer.

1.5 Tujuan Penelitian

Untuk menganalisis keamanan jaringan fasilitas internet (Wi-Fi) terhadap serangan *system failure* pada toko services w-elektrik batam.

1.6 Manfaat Penelitian

Manfaat penelitian dalam menganalisis tingkat keamanan fasilitas jaringan internet (Wi-Fi) serta trojan sehingga terjadinya *system failure*.

1.6.1 Secara Teoritis

Memberikan pengarahan bagaimana cara antisipasi terjadinya kegagalan pada sistem komputer sebagai sarana dalam menentukan keputusan akhir pada penelitian ini.

1. Menjelaskan bagaimana cara antisipasi terjadinya *system failure* yaitu mengolah data dari berbagai sumber terkait dan memproses data tersebut menjadi sebuah kesimpulan penelitian.
2. Sebagai tambahan pengetahuan bagi peneliti dan memperoleh gambaran praktek langsung dalam menganalisis keamanan jaringan *wireless(*Wi-Fi*)* yang mengakitbatkan *system failure*.

1.6.2 Secara Praktis

Secara praktis adapun manfaat adalah memudahkan mahasiswa mengetahui keamanan sistem pada jaringan internet(Wi-Fi) serta cara menganalisis dan membaca kondisi keamanan yang ada.

BAB II

TINJAUAN PUSTAKA

2.1 Teori dasar

2.1.1 Jaringan Komputer Dan Internet

Jaringan Komputer (*computer networks*) adalah himpunan interkoneksi sejumlah komputer antonomous. Dalam bahasa yang populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer serta perangkat yang lain seperti router, switch dan sebagainya yang saling terhubung satu sama lain melalui media perantara.(Suwandi et al., 2018)

Secara historis, jaringan komputer hadir setelah berbagai keterbatasan dari komputer sebagai alat komputasi, dan secara konsep, teori mendukung perkembangan baru dari berbagai bidang keilmuan yang lain, baik secara rekayasa maupun sumber daya yang lain. Bagaimanapun juga, inovasi terus tumbuh sejalan dengan kepentingan manusia terhadap teknologi, tentunya teknologi tidaklah terbiarkan berjalan sekehendaknya tanpa batasan yang memberikan manusia wewenang untuk memutuskan arah tujuan kehidupannya. Tulisan ini menjembatani perkembangan inovasi yang mungkin dari jaringan komputer.

(Komputer & Nasution, 2019).

2.1.2 Standar Jaringan Komputer Dan Internet

Standar korespondensi diperlukan agar ada konsistensi, sehingga korespondensi dapat dilakukan. Berikutnya adalah enam asosiasi standar yang mengambil bagian dalam organisasi PC, tepatnya:

1. *Internet Engineering Task Force* (IETF), adalah asosiasi yang menggabungkan orang atau asosiasi yang melengkapi atau membina organisasi PC dan web.
2. *International Telecommunications Union* (ITU), adalah asosiasi global yang memiliki hak istimewa untuk menjamin, mengarahkan dan menormalkan komunikasi siaran dan radio di seluruh dunia di bidang media dan organisasi yang digunakan, administrasi dan organisasi komunikasi media dapat berjalan sesuai dengan yang diharapkan.
3. *International Organization for Standardization* (ISO) adalah asosiasi untuk normalisasi global. Sesuai dengan nama asosiasi, asosiasi ini dipercaya untuk menormalkan berbagai bidang yang meliputi organisasi korespondensi informasi. Salah satu model yang paling populer adalah OSI (*Open Framework Interconnection*).
4. *American National Standards Institute* (ANSI), adalah asosiasi atau yayasan yang tugasnya mengarahkan penggunaan dan pembuatan peraturan yang mempengaruhi bisnis di setiap daerah. Asosiasi juga mengatur prinsip-prinsip AS dengan norma-norma global sehingga barang-barang AS dapat digunakan oleh seluruh dunia.
5. *Electronic Industries Association* (EIA), adalah hubungan para pembuat organisasi atau perangkat khusus yang memiliki tanggung jawab terhadap pemeliharaan dan peningkatan prinsip-prinsip industri dalam rangka penanganan informasi dan korespondensi informasi. Afiliasi juga

dipercaya untuk memastikan bahwa peralatan yang dibuat oleh produsen, meskipun asli, tetap layak pakai.

6. *Institute Electrical and Electronic Designers* (IEEE) adalah perkumpulan yang terpanggil untuk membuat berbagai norma termasuk organisasi bidang korespondensi informasi. Modelnya adalah IEEE 802.3 dan IEEE 802.5.

2.1.3 Jenis Jaringan Komputer Dan Internet

Jaringan komputer dibuat menggunakan kombinasi perangkat keras dan perangkat lunak, dan merupakan jenis jaringan telekomunikasi yang memungkinkan komputer untuk bertukar data satu sama lain. Sebenarnya ada komponen jaringan komputer yang merupakan pihak yang menerima atau meminta layanan yang disebut klien dan yang memasok atau mengirim disebut server ketika dua komputer atau lebih saling berkomunikasi atau bertukar data. Sistem Client-Server adalah nama umum untuk arsitektur semacam itu. (3 et al., 2018).

Ada beberapa jenis jaringan komputer yang sering ditemukan dan diklasifikasikan menurut cangkupan areanya, yaitu:

1. LAN (*Local Area Network*)

   LAN atau Local Area Network adalah konsep yang menghubungkan perangkat jaringan dalam jarak yang relatif pendek. Biasanya digunakan untuk gedung sekolah, kantor, rumah, dll. Konsep jaringan LAN ini cenderung menggunakan konektivitas tertentu, terutama Ethernet dan Token Ring. Ada juga LAN yang menggunakan teknologi

jaringan Wireless atau nirkabel dengan WI-FI dan dikenal dengan nama Wireless Local Area Network (WLAN).

2. MAN (*Metropolitan Area Network*)

   MAN atau *Metropolitan Area Network* adalah konsep yang menghubungkan perangkat jaringan dari satu Kota ke Kota lainnya. Penggunaan LAN sudah tidak memungkinkan untuk membangun jaringan maka jaringan MAN akan digunakan, karena cangkupannya lebih besar dari LAN maka MAN menggunakan perangkat khusus dan memerlukan operator telekomunikasi yang bertugas sebagai penguhubung antar jaringan komputer(3 et al., 2018).

3. WAN (*Wide Area Network*)

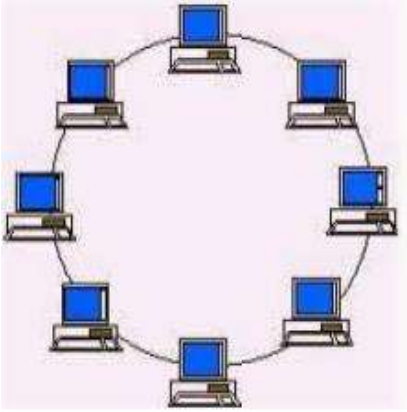
   WAN atau *Wide Area Network* adalah konsep yang menghubungkan perangkat jaringan komputer yang mencangkup wilayah sangat luas dan menggunakan peralatan yang sangat canggih apabila dibandingkan dengan MAN dan LAN(3 et al., 2018). Konsep jaringan ini sendiri biasanya digunakan untuk mengubungkan suatu jaringan dari negara satu dengan negara lainnya antar negara bahkan bisa juga antar benua. Salah satu contoh peralatan yang sangat canggih adalah fiber optic dimana pemasangannya ditanam didalam tanah maupun dibawah laut.

Dalam pembangunan jaringan komputer ini sendiri tidak lepas dari namanya topologi, dimana topologi ini sendiri bisa dibilang sebagai bentuk atau struktur virtual jaringan yang mengacu pada tata letak perangkat yang terhubung, walaupun bentuk ini tidak selalu sesuai dengan tata letak fisik sebenarnya dari perangkat jaringan. Menurut Pratama (2014:18) Topologi jaringan komputer didefinisikan sebagai "suatu teknik, cara, dan aturan didalam merangkai dan menghubungkan berbagai komputer dan perangkat terhubung lainnya ke dalam sebuah jaringan komputer sehingga membentuk sebuah hubungan yang bersifat geometris". Topologi bersifat sebuah rancangan (desain) yang kemudian dapat diimplementasikan secara langsung melalui sejumlah perangkat keras penghubung pada jaringan komputer.

Topologi jaringan dapat dikategorikan ke dalam tipe dasar berikut, yakni:

1. *Topologi Ring*

   Menurut Pratama (2014:26) Topologi ring merupakan "salah satu topologi yang relative sederhana pada jaringan komputer". Topologi jaringan ini hanya menghubungkan setiap komputer (atau disebut juga sebagai node) satu per satu, sehingga membentuk sebuah rangkaian cincin (*Ring*).



Gambar 2. 1 Topologi Ring

Sumber: *http://www.adalahcara.com*

Beberapa kelebihan yang dimiliki oleh Topologi Ring antara lain:

a. Dilihat bentuk topologinya, maka dapat disimpulkan bahwa topologi ring relatif lebih hemat biaya untuk implementasinya. Misalkan untuk penyediaan kabel jaringan, router switch, hub dan lain-lain.
b. Dibandingkan dengan Topologi Star, Topologi Ring relatif lebih baik.

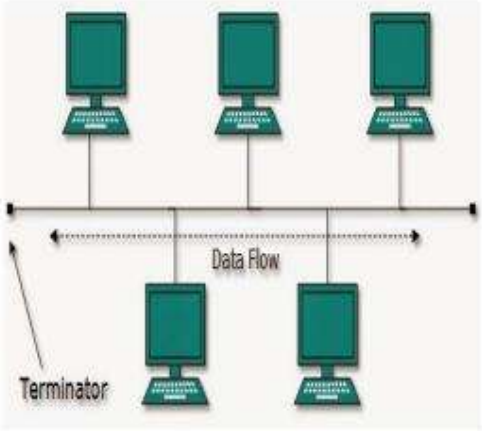
Beberapa kekurangan yang dimiliki oleh Topologi Ring antara lain:

a. Topologi Ring memerlukan teknisi yang memiliki kemampuan dan pemahaman terhadap jaringan komputer dan konfigurasinya dengan baik, sebab Topologi Ring memerlukan konfigurasi yang relatif lebih tinggi (sulit).
b. Topologi Ring memerlukan ketelitian tinggi di dalam implementasinya, sebab memiliki kepekaan tinggi terhadap adanya kesalahan di dalam konfigurasi maupun implementasi.

c. Sifat Scalable pada jaringan komputer tidak didukung penuh oleh Topologi Ring, dilihat dari sulitnya mengembangkan jaringan dengan Topologi Ring ke dalam skala jaringan yang lebih besar (luas).

2. Topologi Bus

Menurut Pratama (2014:19) Topologi Bus merupakan "salah satu topologi yang paling awal digunakan didalam model topologi pada jaringan komputer, terutama dimasa-masa awal jaringan komputer di kembangkan". Topologi Bus hanya menggunakan sebuah jalur koneksi, yang kemudian digunakan secara bersama-sama oleh beberapa buah komputer dan perangkat jaringan komputer terhubung lainnya.



Gambar 2. 2 Topologi Bus

Sumber: http://www.nesabamedia.com

Beberapa kelebihan yang dimiliki oleh Topologi Bus antara lain:

a. Topologi Bus sangat sederhana dan mudah untuk diimplementasikan tanpa memerlukan pengetahuan teknis yang dalam terhadap jaringan komputer.

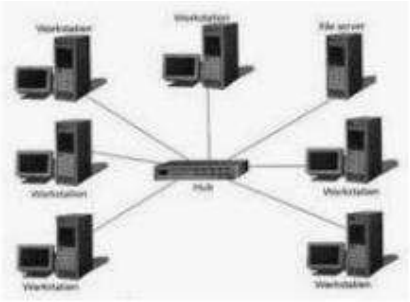
b. Topologi Bus memerlukan biaya yang relatif lebih sedikit. Selain sederhana dan mudah untuk diimplementasikan, Topologi Bus juga memerlukan biaya yang relatif lebih sedikit (jika dibandingkan dengan topologi lainnya di dalam jaringan komputer).

Beberapa kekurangan yang dimiliki oleh Topologi Bus antara lain:

a. Topologi Bus tidak mendukung untuk jaringan berkecepatan tinggi. Hal ini disebabkan karena Topologi Bus belum mampu menangani masalah-masalah yang disebabkan oleh beban trafik pada jaringan komputer.
b. Topologi Bus tidak cocok diterapakan pada jaringan komputer berskala besar. Topologi Bus memang sangat cocok diterapkan pada jaringan komputer cepat saji (instan), pada jaringan local dan mencakup para pengguna pemula yang belum memiliki pengetahuan teknis memandai.

3. Topologi Star

Menurut Pratama (2014:21) Topologi Star adalah "topologi di dalam jaringan komputer, dimana terdapat sebuah komputer (ataupun perangkat jaringan komputer beruba hub atau switch) yang menjadi pusat dari semua komputer yang terhubung ke dalamnya".



Gambar 2. 3 Topologi Star

Sumber: *http://www.adalahcara.com*

Beberapa kelebihan yang dimiliki oleh *Topologi Star* antara lain:

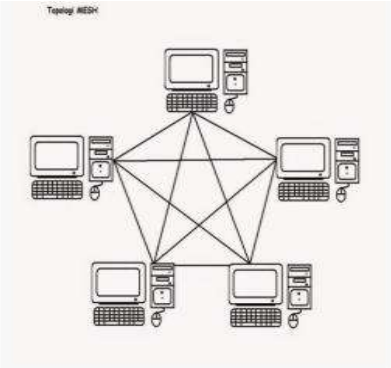
a. *Topologi Star* lebih mendukung didalam jaringan, dimana kemungkinan untuk terjadinya tabrakan paket data (*Collision*) kecil atau tidak ada sama sekali.
b. *Topologi Star* mudah diimplementasikan, cukup dengan hanya menghubungkan komputer ke komputer server (termasuk juga pada switch atau hub jika dalam bentuk perangkat penghubung jaringan).

Beberapa kekurangan yang dimiliki oleh Topologi Star antara lain:

a. Pada *Topologi Star*, biaya jauh lebih besar, mengingat diperlukan kabel jaringan yang jauh lebih banyak.
b. Pada *Topologi Star*, apabila trafik jaringan padat (misalkan terdapat banyak pertukaran data antar komputer, yang mana semua lalu lintas data melewati komputer pusat/server (maupun *hub* atau *switch*), akan berakibat pada lalu lintas pertukaran data yang makin melambat.

4. *Topologi Mesh*

Menurut Pratama (2014:29) *Topologi Mesh* adalah "salah satu jenis topologi pada jaringan komputer yang menghubungkan semua computer secara penuh (*Fully Connected*)". *Topologi Mesh* merupakan topologi yang paling kompleks dan paling banyak digunakan pada penyedia layanan akses internet (*ISP/Internet Service Provider*), sebab Topologi Mesh mampu menjaga agar kerusakan atau gangguan yang terjadi pada salah satu komputer tidak akan mempengaruhi komputer lain atau jaringan secara keseluruhan.



Gambar 2. 4 Topologi Mesh

Sumber: *http://www.adalahcara.com*

Beberapa kelebihan yang dimiliki oleh Topologi Mesh antara lain:

a. *Topologi Mesh* mempercepat adanya deteksi terhadap adanya kesalahan dan gangguan pada jaringan komputer, tanpa mengganggu komputer lainnya ataupun jaringan komputer itu sendiri.
b. *Topologi Mesh* aman dari gangguan komputer lainnya (didalam jaringan yang sama), sehingga mampu menjaga produktifitas dan layanan pada jaringan komputer.

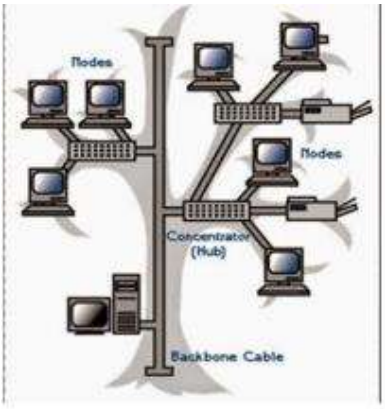
Beberapa kekurangan yang dimiliki oleh Topologi Mesh antara lain:

a. *Topologi Mesh* memerlukan tenaga ahli di bidang jaringan komputer, sebab proses instalasi dan konfigurasinya memerlukan kemampuan yang lebih tinggi dibandingkan topologi sederhana lainnya (misalnya Topologi Bus).
b. *Topologi Mesh* memerlukan biaya besar untuk penyediaan perangkat keras penghubung pada jaringan komputer. Misalkan saja kabel jaringan, router, switch, hub,wireless dan lain-lain.

5. *Topologi Tree*

Menurut Pratama (2014:27) *Topologi Tree* merupakan "salah satu topologi yang juga paling banyak diterapkan didalam jaringan computer dengan bentuk geometris menyerupai pohon (*Tree*)". Pada topologi Tree terdapat sebuah komputer (atau perangkat jaringan komputer berupa *hub* atau pun switch) pada level teratas (disebut dengan root) yang menjadi

pusat utama komunikasi bagi semua komputer lain yang terhubung dengannya.



Gambar 2. 5 Topologi Tree

Sumber: *http://www.adalahcara.com*

Beberapa kelebihan yang dimiliki oleh Topologi Tree antara lain:

a. *Topologi Tree* mudah untuk dikembangkan sesuai kebutuhan dan mudah diperbaiki jika terdapat permasalahan maupun kesalahan.
b. *Topologi Tree* mendukung koneksi Point to Point pada jaringan komputer.

Beberapa kekurangan yang dimiliki oleh Topologi Tree antara lain:

a. Pada *Topologi Tree*, potensi untuk terjadinya Collision (tabrakan) paket data sanagat besar.
b. *Topologi Tree* memerlukan usaha yang besar untuk melakukan perawatan dan perbaikan (maintenance) pada skala jaringan besar.
c. Apabila salah satu komputer central ataupun komputer root mengalami gangguan, maka komputer-komputer yang ada di bawahnya (secara hirarki) akan ikut terganggu.

2.1.4 Keamanan Jaringan Komputer

Menurut Gollmann dalam (Rajendra, 2022) keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer. Sedangkan menurut keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagai sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Menurut (David Icove, 1997) berdasarkan lubang kemanan, keamanan komputer dapat dibagi menjadi 4 macam, yaitu :

1. Keamanan Fisik (*Physical Security*) Termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh : Wiretapping atau hal-hal yang berhubungan dengan akses ke label atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
2. *Denial Of Service*, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan)
3. *Syn Flood Attack*, dimana sistem (*host*) yang dituju dibanjiri oleh permintaan sehingga menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem (*hang*).

4. Keamanan yang berhubungan dengan orang Contoh : *Identifikasi user* (username dan password), profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).

2.1.5 Jenis-jenis ancaman keamanan jaringan

1. Packet sniffer

Aplikasi yang disebut packet *sniffer* mengumpulkan data dari paket saat melakukan perjalanan melalui jaringan. Nama pengguna, kata sandi, dan informasi penting lainnya yang dikirimkan melalui jaringan dalam bentuk teks dapat disertakan dalam data ini. Ada ratusan atau mungkin ribuan paket yang bisa dicegat daripada hanya satu. (Fauzi dan Suartana, 2017:12)

2. Probe

Probe, juga dikenal sebagai probing, adalah upaya untuk mendapatkan akses ke sistem dengan memeriksa semua akun yang tidak aktif untuk melihat apakah terkunci atau tidak terkunci sehingga pengguna dapat masuk dengan cepat.

3. *Denial of service* (Dos)

Denial of service adalah strategi penyerangan yang mencoba menghabiskan sumber daya jaringan yang berharga, seperti database dan layanan yang ditawarkan oleh perusahaan pemilik jaringan, sehingga pengguna tidak dapat mengakses layanan jaringan..

4. ARP spoofing / ARP poisoning

Oktavianto dalam (Fauzi dan Suartana, 2017) digambarkan sebagai metode penyerangan jaringan komputer lokal menggunakan media kabel atau nirkabel, peracunan ARP (*Address Resolution Protocol*) memungkinkan penyerang mendeteksi bingkai data di jaringan lokal dan mengubah atau bahkan mengganggu komunikasi. *Spoofing* ARP, sering dikenal sebagai MITM, adalah gagasan serangan penyadapan antara dua mesin yang berkomunikasi (*Man in The Middle Attack*). Ide dasar di balik serangan peracunan ARP ini adalah untuk mengeksploitasi kelemahan dalam teknologi penyiaran arp, yang digunakan dalam jaringan komputer. Alamat MAC adalah alamat pada *layer* 2, tempat ARP berada. Misalnya, jika *host* (misalnya, PC) yang terhubung ke LAN ingin menghubungi host lain di LAN itu, ia memerlukan informasi alamat MAC komputer lain.

5. Reveal SSID

Merupakan serangan yang dilakukan dengan mengungkapkan SSID titik akses, yang sengaja disembunyikan oleh administrator jaringan komputer.

6. MAC Address Spoofing

MAC Address Spoofing adalah upaya *hacker* untuk menyiasati keamanan penyaringan alamat MAC di jaringan komputer dengan memanfaatkan alamat MAC dari pengguna yang berwenang untuk mengakses layanan jaringan komputer.

7. Authentication Attack

serangan terhadap pengguna terotentikasi yang melumpuhkan atau memutus pengguna resmi memanfaatkan layanan jaringan, penyerang menggunakan teknik ini untuk mengakses sumber daya yang lebih dalam.

8. Eavesdropping

adalah jenis serangan yang melibatkan mendengarkan setiap paket yang dikirim oleh pengguna di dalam jaringan komputer yang tidak dilindungi oleh enkripsi.

9. Session Hijacking

adalah jenis serangan yang menargetkan sesi pengguna dalam upaya mendapatkan akses ke layanan yang sedang digunakan oleh pengguna yang berwenang.

10. Man In The Middle Attack

Merupakan serangan yang dilakukan dengan melakukan spoofing terhadap *user* sah sehingga transmisi yang dilakukan target adalah menuju attacker, sehingga attacker mendapatkan semua informasi yang di transmisikan oleh target (Manuaba, Hidayat dan Kusumawardani, 2012)

11. Malicious code (Kode berbahaya)

Kode berbahaya yaitu program yang menyebabkan kerusakan kerangka kerja saat dijalankan trojan, *worm*, dan penipuan adalah jenis kode berbahaya. Cara paling efektif untuk menebak ini harus terlihat dalam lima model berikut:

a. Berikan perhatian pada user tentang bahaya ancaman trojan.

b. Gunakan program antivirus yang layak di komputer, server, dan pintu web (jika anda memilikinya).
c. Tunjukkan dan latih user cara menggunakan program antivirus.
d. Sebagai admin, harus selalu menyegarkan program antivirus dan basis informasi data base. Latihlah secara teratur agar user tidak membuka record koneksi email atau dokumen apapun dari *floppy* sebelum 100 persen yakin apakah koneksi/*record* sudah sempurna.
e. Pastikan kebijakan keamanan terbaru dan terpercaya.

2.1.6 Model OSI layer

Kerangka kerja konseptual yang dikenal sebagai OSI, atau *Open System Interconnection,* berfungsi sebagai model referensi untuk protokol konektivitas untuk komputer. Model referensi OSI ini dikembangkan untuk bertindak sebagai panduan bagi vendor dan pengembang sehingga perangkat lunak atau produk yang mereka buat dapat diintegrasikan, atau digunakan dengan sistem atau produk lain tanpa harus melakukan upaya ekstra oleh pengguna. Hasilnya, model OSI dibagi menjadi tujuh tingkat, dengan setiap lapisan memainkan peran baik di lapisan di atasnya maupun di bawahnya. Tujuh level OSI dijelaskan di bagian selanjutnya.(Klarisa Anugrah, 2017)

2.1.7 Kelemahan jaringan

Kerentanan jaringan nirkabel umumnya terbagi dalam dua kategori: kerentanan konfigurasi dan kerentanan tipe enkripsi. Kemudahan yang saat ini dapat diatur jaringan nirkabel adalah salah satu ilustrasi dari kelemahan

pengaturan. Adalah umum untuk menemukan perangkat nirkabel yang terus menggunakan pengaturan nirkabel default vendor karena banyak vendor menawarkan fitur yang membuatnya lebih mudah bagi pengguna atau administrator jaringan. Dalam jaringan nirkabel, celah tersebut biasanya mencakup empat lapisan, di mana keempat lapisan tersebut sebenarnya adalah metode pertukaran data. Media wireless. Sebenarnya ada lubang yang menunggu untuk diisi di setiap lapisan media komunikasi nirkabel. (Riyan Feraldi, 2019). Maka dari itu, keamanan jaringan *wireless* menjadi begitu lemah dan perlu dicermati dengan ekstra teliti. *Layer-layer* beserta kelemahannya tersebut adalah sebagai berikut:

1. *Physical Layer*

Seperti pengetahuan umum, lapisan fisik komunikasi data akan membahas pembawa data secara luas. Media perantara dalam sistem komunikasi data nirkabel tidak lain adalah ruang terbuka. Data berupa sinyal radio dalam frekuensi tertentu dapat bergerak bebas di udara terbuka. Tentu saja, Anda dapat membayangkan betapa terekspos nya keamanan data akibat lalu lintas di lingkungan. Siapa pun mungkin dapat mengambilnya, mengetuknya, atau bahkan membacanya secara langsung tanpa menyadarinya. Tidak terlalu riskan jika ada yang menyadap atau membacanya jika hanya untuk kepentingan pribadi. Namun, bagaimana jika kelemahan-kelemahan ini terdapat pada jaringan *wireless* perusahaan yang didalamnya terdapat berbagai transaksi bisnis, proyek- proyek perusahaan, info-info rahasia, rahasia keuangan dan banyak lagi informasisensitif di dalamnya. Tentu penyadapan tidak dapat ditoleransi lagi jika perusahaan

tidak menjadi target orang (Riyan Feraldi, 2019)

2. Network Layer

Network layer (*layer* jaringan) biasanya akan banyak berbicara seputar perangkat-perangkat yang memiliki kemampuan untuk menciptakan sebuah jaringan komunikasi yang disertai juga dengan sistem pengalamatannya. Pada jaringan komunikasi *wireless*, perangkat yang biasa digunakan sering disebut dengan istilah *Access Point* atau disingkat AP. Sistem pengalamatan IP tentu akan banyak ditemukan pada perangkat ini, karena melayani komunikasi menggunakan media bebas yang terbuka, maka AP-AP tersebut juga dapat dikatakan sebagai perangkat yang terbuka bebas. Perangkat jaringan yang tidak diverifikasi dan dikontrol dengan baik akan dapat menjadi sebuah pintu masuk bagi para pengacau. Mulai dari hanya sekadar melihat isinya, diubah sedikit sampai dibajak penuh, ini sangat mungkin dialami oleh sebuah *AP*. Untuk itu, perlu diperhatikan juga keamanan AP-AP pada jaringan *wireless* yang ada. Selain itu, antar-AP juga harus dicermati dan perhatikan keamanannya (Riyan Feraldi, 2019)

3. *User layer*

Selain memahami bagaimana jaringan telekomunikasi beroperasi, penting juga untuk mengenali dan mengidentifikasi setiap orang yang menggunakan jaringan nirkabel yang tersedia. Jaringan nirkabel sering menggunakan media publik untuk data lalu lintas, namun jika tidak berfungsi sebagai jaringan publik yang dapat diakses oleh siapa saja, maka harus menyertakan hambatan terkait akses. Tidak terlalu buruk bagi pengguna yang tidak memiliki izin untuk menggunakan jaringan nirkabel. Tentu hal ini akan sangat merugikan para pengguna lain yang

memang berhak jika sembarangan pengguna dapat menggunakan jaringan yang ada. Setiap jaringan nirkabel yang andal harus memiliki pemahaman bahwa hanya pengguna yang dikenal, dapat dipercaya, dan benar-benar istimewa yang diizinkan mengakses jaringan. Perangkat-perangkat jaringan yang biasanya terhubung ke jaringan nirkabel tersebut juga harus dapat dilacak dan dipantau secara akurat. (Riyan Feraldi, 2019)

4. *Application Layer*

Aplikasi yang cukup luas dapat dimanfaatkan oleh jaringan yang hanya menggunakan media kabel, khususnya jaringan nirkabel yang lemah di semua tingkatan. Aplikasi bisnis yang memanfaatkan media nirkabel tidak diragukan lagi sangat rentan terhadap ancaman keamanan, termasuk peretasan sederhana dan serangan *denial-of-service* (*Denial of Service*). Karena itu, jaringan nirkabel yang kuat juga harus dapat melindungi program operasi apa pun sehingga tidak mudah terganggu. (Riyan Feraldi, 2019) Dengan adanya kelemahan dan celah keamanan seperti diatas, beberapa kegiatan dan aktifitas yang dapat dilakukan untuk mengamankan jaringan *wireless* antara lain:

a. Mengubah Sistem Identitas (ID)

   Biasanya suatu layanan nirkabel dilengkapi dengan suatu standart pengamanan identitas atau yang sering disebut SSID *(Service Set Identifier) or* ESSID *(Extended Service Set Identifier)*. Sangat mudah bagi seorang hacker untuk mencari tahu identitas default dari suatu layanan atau jaringan, jadi sebaiknya segera mengubahnya menjadi suatu identitas yang unik, yang tidak mudah ditebak orang lain.

b. Mematikan Identitas Pemancar

Memberitahukan kepada umum jika memiliki suatu jaringan nirkabel akan membuat para *hacker* penasaran untuk membobol jaringan nirkabel. Mempunyai suatu jaringan nirkabel bukan berarti harus memberitahukannya kepada semua orang. Periksa secara manual perangkat keras yang dipakai untuk jaringan nirkabel tersebut, dan pelajari bagaimana cara mematikannya.

c. Menyedikan Enkripsi

WEP *(Wired Equivalent Privacy) and* WPA *(Wi-Fi Protected Access)* dapat meng-enkripsi data sehingga hanya penerima saja yang diharapkan dapat membaca data tersebut. WEP *(Wired Equivalent Privacy)* mempunyai banyak kelemahan yang membuatnya mudah dibobol. Kunci 128-bit hanya mempunyai tingkat pencapaian yang relatif rendah tanpa peningkatan keamanan yang signifikan, sedangkan untuk 40-bit atau 64-bit pada beberapa perlengkapan lainnya, mempunyai enkripsi yang sama baiknya. Menggunakan cara pengamanan yang standart tetap akan mudah bagi *hacker* untuk menyusup, namun dengan cara enkripsi ini pastilah akan membuat jaringan lebih aman dari *hacker*. WPA dapat sangat menjanjikan dalam menjamin keamanan jaringan nirkabel, namun masih tetap dapat dikalahkan oleh serangan DOS *(denial ofservices)*.

d. Membatasi dari Penggunaan *Traffic* yang Tidak Perlu.

Banyak *router* jaringan kabel maupun nirkabel yang dilengkapi *firewalls*.

Firewalls membantu dalam pertahanan keamanan jaringan. Membaca petunjuk manual dari perangkat keras dan pelajari cara pengaturan konfigurasi *router*, sehinggahanya *traffic* yang sudah seijin saja yang dapat dijalankan .

e. Mengubah Kata Sandi *Default Administrator*

Hal ini baik untuk semua penggunaan perangkat keras maupun perangkat lunak. Kata sandi *default* sangat mudah disalah gunakan, terutama oleh para *hacker*. Oleh karena itu, sebaiknya ubah kata sandi dan hindari penggunaan kata dari hal-hal pribadi yang mudah diketahui orang, seperti nama belakang,tanggal lahir, dan sebagainya.

f. Kunci dan lindungi komputer

Menggunakan *firewall*, perangkat lunak AntiVirus, Zone Alarm dan sebagainya dan sebaiknya setiap satu minggu perbaharui Anti Virus.

2.1.8 Kesalahan-kesalahan dalam jaringan

Berikut ini beberapa kesalahan yang sering terjadi di jaringan internet (Wi-Fi):

Tabel 2. 1 Kesalahan dalam jaringan

Bagian	Tipe kesalahan	Tindakan
Media Wireless	waktu Kehilangan koneksi wireless	Mengecek kabel koneksi apakah ada cacat atau kesalahan pasang.
Media Koneksi	Sinyal Lemah	Periksa apakah antena atau radio tidak berfungsi atau ada masalah dengan router atau AP.
Media Koneksi	Sinyal Lemah	Termasuk lebih banyak titik akses. Objek pemblokiran sinyal harus dihilangkan.
Media Wireless	Mati	Soket terlihat tidak rusak, namun konektornya tidak terpasang. kerusakan pada hub atau sakelar, yang merupakan perangkat akses.

2.2 Teori Khusus

2.2.1 *System Failure*

System failure dalam jaringan internet dapat didefinisikan sebagai kegagalan dari sistem atau komponen dalam jaringan yang menyebabkan terganggunya konektivitas atau performa jaringan. Ini dapat terjadi karena berbagai alasan, seperti kerusakan pada perangkat keras, konfigurasi yang salah, atau masalah pada protokol jaringan. Beberapa contoh system failure dalam jaringan internet meliputi:

1. Disebabkan oleh trojan
2. Kerusakan pada kabel atau konektor
3. Keamanan jaringan yang lemah yang mengakibatkan serangan dari pihak luar.

Untuk mengatasi system failure di jaringan internet, perlu dilakukan analisis dan identifikasi masalah yang sebenarnya, serta diimplementasikannya solusi yang tepat dan cepat. Sistem monitoring dan pemeliharaan yang baik juga sangat penting untuk mengidentifikasi masalah sebelum terjadi.

2.2.2.1 Trojan

Istilah "trojan" menggambarkan perangkat lunak berbahaya (*malware*) yang menginfeksi target dengan mendapatkan hak administrator pada sistem operasi Windows. Penyerang dapat mengelola komputer dari jarak jauh dengan membuka akses port pada komputer tersebut. Ide dasar di balik trojan ini adalah penggunaan RAT *(Remote Administration Tool*), yang sering digunakan untuk melakukan tugas jarak jauh pada mesin ketika izin akses telah disetujui. Trojan contoh ini, terkadang dikenal sebagai Trojan Akses Jarak Jauh, adalah jenis yang dapat beroperasi dari jarak jauh melalui akses jarak jauh. Ini berbeda dari apa yang dilakukan trojan karena tidak ada kesepakatan untuk penggunaannya, yang dapat membahayakan korban dan seringkali mengakibatkan kriminalitas. (Chandra et al., 2016)

2.2.2.2 Mendeteksi Trojan

Trojan Detection Analysis adalah sebuah aktivitas untuk mendeteksi dan menganalisa adanya serangan dan Trojan, menggunakan metode dan tools tertentu Tujuannya untuk mengetahui darimana dan Trojan berasal, untuk kemudian menjadi dasar dalam pengambilan keputusan strategis dalam hal akses internet, sehingga aman dari serangan. Mendeteksi keberadaan Trojan merupakan sebuah tindakan yang agak sulit dilakukan. Cara termudah adalah dengan melihat port-port mana yang terbuka dan sedang berada dalam keadaan "listening", dengan menggunakan utilitas tertentu semacam Netstat. Hal ini dikarenakan banyak Trojan berjalan sebagai sebuah layanan sistem, dan bekerja di latar belakang (background), sehingga Trojan- Trojan tersebut dapat menerima perintah dari penyerang dari jarak jauh. Ketika sebuah transmisi UDP atau TCP dilakukan, tapi transmisi tersebut dari port (yang berada dalam keadaan "listening") atau alamat yang tidak dikenali, maka hal tersebut bisa dijadikan pedoman bahwa sistem yang bersangkutan telah terinfeksi oleh Trojan Horse, Komputer yang terserang Trojan sering mengalami satu atau beberapa indikasi sebagai berikut :

1. Layar menampilkan pesan atau gambar yang tidak biasanaya muncul.
2. Musik atau suara yang tidak lazim terdengar secara acak.
3. Memori yang tersedia lebih kecil dari sebenarnya.
4. Program – program atau File – File menjadi hilang.
5. File menjadi rusak.
6. Program atau File tidak bekerja normal.
7. Program atau File yang tidak dikenal muncul secara misterius.

8. Perubahan properti *system* mengakibatkan *system failure*

Tabel 2. 2 Data Karakteristik Trojan

No	Kriteria		blac	ksha	d	dark	com
1	**Tidak memiliki *verified signature***						
2	**Memiliki kemampuan untuk melakukan *self file duplication***						
3	**Memiliki *keylogger***						
4	**Memiliki kemampuan untuk menambahkan *autorun registry* pada sistem**						
5	**Memiliki kemampuan untuk *remote* perubahan *registry***						
6	Memiliki kemampuan untuk melakukan akses *remote* terhadap folder korban						
7	Pada *network traffic* terlihat melakukan komunikasi pertukaran informasi						
8	Memiliki kemampuan untuk *remote desktop / screen viewer*						
9	Memiliki kemampuan untuk mengakses *remote shell* komputer *victim* untuk melakukan fungsionalitas						
10	Memiliki fungsi untuk melakukan *remote execute file* melalui *url*						

Sumber (Chandra et al., 2016)

Tabel 2. 3Data karakteristik pada sample non – trojan

No	Kriteria				
1	**Tidak memiliki *verified signature***	×	×	×	×
2	**Memiliki kemampuan untuk melakukan *self file duplication***	×	×	×	×
3	**Memiliki *keylogger***	×	×	×	×
4	**Memiliki kemampuan untuk menambahkan *autorun registry* pada sistem**	×	×	×	×
5	**Memiliki kemampuan untuk *remote* perubahan *registry***	×	×	×	×
6	Memiliki kemampuan untuk melakukan akses *remote* terhadap folder korban	×	×	×	×
7	Pada *network traffic* terlihat melakukan komunikasi pertukaraninformasi	□	□	□	□
8	Memiliki kemampuan untuk *remote desktop / screen viewer*	□	□	□	□
9	Memiliki kemampuan untuk mengakses *remote shell* komputer *victim* untuk melakukan fungsionalitas	×	□	×	×
10	Memiliki fungsi untuk melakukan *remote download file* melalui *url*	×	×	×	□

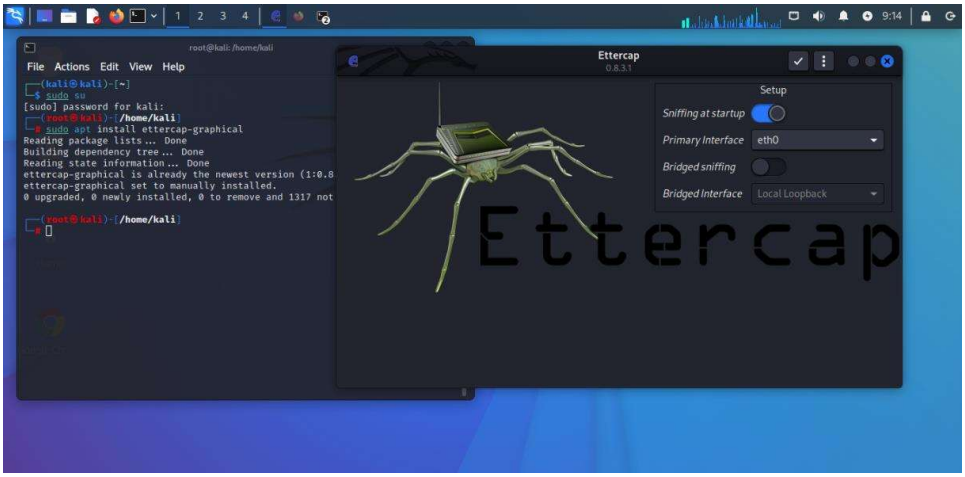
Sumber (Chandra et al., 2016)

2.3 Tools

2.3.1 Ettercap

Ettercap adalah alat untuk analisis protokol jaringan dan audit keamanan. Ettercap memiliki kemampuan untuk mencegat lalu lintas pada jaringan, menangkap password, dan melakukan menguping aktif terhadap protokol umum. Untuk latihan ini peneliti akan menggunakan ARP untuk mendeteksi virus LAN untuk password yang menggunakan SSL (*Hotmail, Gmail, dll*). ARP adalah sebuah protokol jaringan komputer link layer untuk menentukan host jaringan atau alamat hardware saat hanya Internet layernya (IP) atau alamat *Network Layer* dikenal. Fungsi ini sangat penting dalam jaringan area lokal serta untuk lalu lintas internet working routing yang di gateway (*router*). Berdasarkan alamat IP ketika router hop berikutnya harus ditentukan. Jadi, dalam hal yang normal ARP adalah cara untuk mendapatkan alamat MAC dari Host atau Node dari alamat IP. ARP *Spoofing* adalah teknik yang akan digunakan untuk menyerang sebuah kabel atau jaringan nirkabel. ARP *Spoofing* memungkinkan penyerang untuk mendeteksi frame data dari LAN, kemudian memberi kemampuan untuk memodifikasi (baik untuk mengarahkan ke komputer sendiri untuk men-*download* mengeksploitasi korban) atau menghentikan lalu lintas dari memasuki jaringan yang spesifik komputer. Ettercap memungkinkan membentuk serangan melawan protokol ARP dengan memposisikan diri sebagai “penengah, orang yang ditengah” dan, jika sudah berada pada posisi tersebut, maka akan memungkinkan untuk :

1. menginfeksi, mengganti, menghapus data dalam sebuah koneksi
2. melihat password pada protokol-protokol seperti FTP, HTTP, POP, SSH1, dan lain-lain.
3. menyediakan SSL sertifikasi palsu dalam bagian HTTPS pada korban. (Fauzi dan Suartana, 2017).



Gambar 2. 6 Aplikasi Ettercap

Sumber : https://openmaniak.com/id/ettercap.php

2.3.2 *Arp Prepropcessors*

Arp spoof adalah preprocessors yang dirancang untuk mendeteksi jalannya Address Resolution Protocol (ARP). Arp digunakan pada jaringan ethernet untuk memetakan alamat IP ke alamat MAC. Untuk mengurangi jumlah siaran arp pada jaringan modern, sistem operasi perangkat yang terhubung menyimpan cache pemetaan arp. Saat perangkat menerima balasan arp, maka cache pada arp akan diperbarui dengan pemetaan alamat IP ke MAC yang baru

apakah perangkat tersebut mengirim permintaan *arp* atau tidak. Berbagai serangan melibatkan *arp*. *Spoofing ARP* dilakukan dengan menyusun *arp request* dan *reply* paket. Paket balasan *arp* yang ditangguhkan disimpan di *cache arp* dari perangkat penerima meskipun perangkat tidak mengirim permintaan.

Jenis serangan *arp spoof* lainnya adalah serangan *arp* menimpaserangan. Serangan tersebut bekerja dengan mengirimkan paket *arp* yang diterima oleh perangkat untuk alamat antarmuka perangkat itu sendiri tetapi dengan alamat MAC yang berbeda. Ini akan menimpa alamat MAC perangkat itu sendiri di *cache arp* dengan permintaan *arp* yang berbahaya. Hal ini menyebabkan perangkat tidak dapat mengirim dan menerima paket *arp*. Pada gilirannya, ini menyebabkan perangkat dan perangkat lain yang bergantung padanya agar komunikasi tidak dapat mengirim paket satu sama lain. Karena *arp* adalah protokol Layer dua, *arp spoof*hanya mendeteksi serangan yang terjadi pada segmen fisik yang sama seperti sensor *Snort* (Fauzi dan Suartana, 2017). *Arp spoof* memiliki dua pilihan konfigurasi, yaitu:

1. *Host* IP *address* host MAC *address*

   Koziol dalam (Fauzi dan Suartana 2017) Setiap perangkat yang ingin di monitor dengan *arp* spoof harus ditentukan dengan pemetaan alamat Ip dan MAC miliknya sendiri. Masing-masing perangkat terdaftar pada baris baru di file *snort.conf.* Setiap kali pemetaan berubah maka harus mengkonfigurasi ulang file tersebut. Perangkat yang mendapatkan alamat IP mereka melalui DHCP harus dikonversi ke IP statis sebelum *ARPspoof* diaktifkan.

2. Unicast

Pilihan ini akan memungkinkan deteksi serangan Arp unicast. Sebagian besar permintaan arp yang valid dikirim ke alamat broadcast. Permintaan arp yang dikirim ke alamat Unicast seringkali merupakan tanda serangan yang dirancang untuk memodifikasi cache arp. Pilihan ini dinonaktifkan secara default, namun dapat diaktifkan jika terdapat penyalah gunaan Arp yang serius.

2.3.3 inSSIDer

InSSIDer adalah software yang berguna untuk memindai jaringan dalam jangkauan antena Wi-Fi komputer, melacak kekuatan sinyal dari waktu ke waktu, dan menentukan pengaturan keamanan yang digunakan (apakah dilindungi oleh password atau tidak)(Rante & Patras, 2018).

2.3.4 Packet Sniffing

Packet sniffer yang dikenal sebagai network analyzer merupakan sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan. Contohnya adalah aplikasi Ettercap yang sering digunakan oleh banyak user. Packet sniffing juga dapat di salah gunakan oleh pihak yang tidak bertanggung jawab untuk mencuri data penting yang dimiliki oleh user yang sedang terhubung dengan access point (Aykarahmi Umasugi, 2022).

2.4 Penelitian Terdahulu

Penelitian ini dilakukan berdasarkan penelitian terdahulu sebagai acuan peneliti dalam pengumpulan data. Penelitian terdahulu juga berfungsi untuk

menambah kajian pada penelitian yang akan dilakukan peneliti. Berikut adalah penelitian terdahulu yang berhubungan dengan penelitian kali ini:

1. Sari, D. M., Yamin, M., & Aksara, L. B. (2017). " ANALISIS SISTEM JARINGAN KEAMANAN WIRELESS (WEP, WPAPSK/WPA2PSK) MAC ADDRESS MENGGUNAKAN METODE PENETRATION TESTING" Jaringan wireless merupakan jaringan yang banyak digunakan pada institusi maupun tempat umum. Jaringan wireless memiliki sistem keamanan seperti WEP, WPAPSK/WPA2PSK, dan MAC Address filtering. Walaupun memiliki sitem keamanan jaringan wireless masih dapat di diserang oleh para attacker dengan menggunakan jenis serangan Cracking the Encryption dan bypassing WLAN Authentication. Metode penetration testing yaitu metode dengan melakukan pengujian sistem keamanan dengan mensimulasikan bentuk-bentuk serangan terhadap keamanan jaringan. Dari hasil pengujian yang dilakukan bahwa sistem keamanan WEP dengan jenis serangan cracking the encryption dan sistem mac address filtering dengan jenis serangan bypassing WLAN authentication berhasil dilakukan. Sedangkan sistem keamanan WPAPSK/WPA2/PSK dengan jenis serangan cracking the encryption berstatus berhasil pada pengujian 2 dengan menggunakan huruf sebagai Pre-Shared-Key (PSK) dan berstatus gagal pada pengujian 1 dan 3 dengan menggunakan kombinasi ('huruf dan angka', 'huruf, simbol dan angka') Berdasarkan hasil pengujian dan analisis maka disimpulkan sistem keamanan yang tepat untuk diterapkan pada jaringan wireless yaitu sistem

keamanan WPAPSK/WPA2PSK. Kesimpulan bahwa keamanan yang dimiliki oleh jaringan WLAN masih memiliki banyak celah untuk dieksploitasi. Hal ini dibuktikan dengan hasil penelitian dari dua jenis serangan yang dilakukan, yaitu pada jenis serangan cracking the encryption tipe keamanan WEP berstatus berhasil dengan 3 pengujian dengan 3 kombinasi (‘huruf dan angka’,’huruf’, ‘huruf, angka dan simbol’) password yang berbeda, jenis serangan cracking the encryption tipe keamanan WPA dan WPAPSK/WPA2PSK berstatus berhasil pada pengujian 2 dengan menggunakan huruf sebagai Pre-Shared- Key(PSK) dan berstatus gagal pada pengujian 1 dan 3 dengan menggunakan kombinasi (‘huruf dan angka’, ‘huruf, simbol dan angka’). Dan untuk jenis serangan bypassing wlan authentication tipe keamanan MacAddress filtering berstatus berhasil. Oleh karena itu, untuk sistem keamanan WLAN yang paling tepat untuk diterapkan adalah WPAPSK/WPA2PSK.

2. MT Hidayat, FM SN, NI kurniati (2018). ”ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET(Wi-Fi)GRATIS TERHADAP SERANGAN PAKET SNIFFING ” Universitas Siliwangi Tasikmalaya merupakan Perguruan Tinggi Negeri yang memiliki sekitar 10.000 Mahasiswa aktif dari berbagai macam Fakultas yang sudah menerapkan Sistem Administrasi berbasis teknologi informasi. Saat ini telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media pertukaran data/informasi untuk pelayanan umum, kemahasiswaan dan kepegawaian serta informasi penting lainya. Terdapat banyak jaringan

yang terpasang dalam lingkup lokasi UNSIL terdapat 1 pusat ruangan server di ruang pengelola TIKyang terhubung dengan seluruh fakultas dan perpustakaan serta pusat kantor yang lainya, terinstall pada setiap Parodi, Fakultas, perpustakaan, LPPM yang dengan menerapkan jaringan kabel dan terdapat banyak access point sebagai jaringan nirkabel, dan terinstall di seluruh area unsil yang terdapat access point tanpa password. Berdasarakan uraian di atas, perlu dilakukan analisis tingkatkeamanan jaringan di berbagai lokasi di Universitas Siliwangiserta mengetahui tingkat kesadaran pengguna komputer terhadap keamanan informasi. Penelitian ini dilakukan dengan pendekatan *action research modelyang* membagi beberapa tahapan yaitu *diagnosing, action planning, intervention, evaluation, dan reflection.* hasildarimengambil data dan informasi pada target korban yang diserang sesuai dengan keinginan penyerang, dimana kita bisa mengambil foto, username dan password korban serta data data yang lainya sesuai kemanan komputer korban. Penilaian kemanan jaringan dan komputer korban dilakukan.

3. MD Sanjaya. (2019). " ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET(Wi-Fi) TERHADAP SERANGAN PACKET SNIFFING PADA KANTOR INDOSAT OOREDOO " masalah dari penjelasan latar belakang tersebut adalah sebagai berikut "Kantor Indosat Ooredoo Pekanbaru perlu mempunyai pengawasan tentang bahaya nya jaringan komputer kantor dan umum dalam 1 jaringan yang berada di lingkungan Kantor Indosat Ooredoo Pekanbaru". Metode pada simulasi

ini menggambarkan suatu mode kecil topologi jaringan internet Kantor Indosat Ooredoo Pekanbaru yang dalam jaringan Wi-Fi nya digunakan oleh pihak Kantor dan Umum (pengunjung), dan tidak memisahkan penggunaan nya antara jaringan Wi-Fi kantor dengan Wi-Fi untuk umum (pengunjung). Hingga perlu adanya pengawasan tentang bahaya nya jaringan Wi-Fi terhadap penyadapan data. Hasil penelitian ini dapat di simpulkan. Penyerangan Packet Sniffing dapat merekam dan menampilkan username dan *password* target dengan menggunakan aplikasi Wireshark. Dengan melakukan penelitian ini pihak kantor PT Indosat Ooredoo Pekanbaru dapat mengetahui bahayanya penggunaan Wi-Fi tanpa pengaman dan yang berada dalam satu jaringan dengan pengguna umum.

4. Ibrahim, Maulana Muhammad. (2020). "ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET(Wi-Fi) KANTOR PERINTAH KOTA BATAM TERHADAP SERANGAN PACKET SNIFFING " Kantor Pemerintah Kota Batam adalah salah satu Kantor Pemerintah pusat di Kota Batam yang memiliki fasilitas jaringan nirkabel (Wi-Fi) jaringan Wi-Fi sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi terbuka. Diperlukan sistem keamanan yang baik untuk dapat menjaga keamanan data pengguna untuk menghindari serangan yang dilakukan oleh orang-orang yang tidak bertanggung jawab. Penelitian ini membahas menganalisis tingkat keamanan fasilitas Wi-Fi di Kantor Pemerintah Kota Batam menggunakan aplikasi Wireshark. Hasil

dari penelitian ini adalah deteksi keberadaan dan keamanan keamanan Wi-Fi terbuka atau tidak aman dan pencatatan nama pengguna dan kata sandi. Hal ini dapat membahayakan keamanan lalu lintas data pengguna jaringan Wi-Fi dan LAN kabel terutama karyawan / i, sehingga perlu meningkatkan keamanan yang baik untuk dapat mencegah / menangani serangan paket sniffing dan banyak lagi. Kesimpulan menjelaskan asal timbulnya serangan sampai dengan solusi untuk menyelesaikan masalah tersebut.

5. Turkhamun Adi Kurniawan. (2020). "ANALISA KEAMANAN JARINGAN Wi-Fi TERHADAP SERANGAN PACKET SNIFFING " Jaringan komputer mempunyai dua media transmisi data yaitu kabel dan nirkabel. PT. XYZ merupakan sebuah perusahaan yang mempunyai fasilitas jaringan nirkabel (Wi-Fi). Jaringan Wi-Fi sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi bersifat terbuka. Diperlukan *system* pengamanan yang baik untuk dapat menjaga keamanan data pengguna agar dapat terhindar dari berbagai serangan yang dilakukan oleh orang–orang yang tidak bertanggung jawab. Metode penelitian ini adalah sebagai berikut. 1. Perancangan Sistem Tahap ini merupakan tahap awal yang akan dilakukan untuk melakukan penelitian tentang keamanan jaringan pada fasilitas internet Wi-Fi terhadap serangan packet sniffing dengan menggunakan ids. 2. Konfigurasi & Implementasi Install aplikasi Ettercap pada linux yang digunakan untuk melakukan serangan packet sniffing, setelah melakukan instalasi peneliti melakukan konfigurasi

terhadap aplikasi Ettercap dan install juga aplikasi / *tools ids* yang digunakan untuk melakukan pendeteksi adanya serangan packet sniffing, dan juga peneliti juga membuat rule-rule tertentu agar dapat mendeteksi serangan packet sniffing dengan indikasi arp spoofing. Hasil dan kesimpulan dari penelitian ini adalah dengan terdeteksinya keberadaan dan keamanan Wi-Fi yang terbuka atau tanpa pengamanan dan terekamnya username dan password. Hal ini dapat membahayakan keamanan lalulintas data para pengguna jaringan Wi-Fi maupun LAN kabel khususnya para karyawan/i, sehingga diperlukan peningkatan keamanan yang baik untuk dapat mencegah/menangani serangan packet sniffing dan yang lebih lanjut.

6. RIZKYANI. (2020). "ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET(Wi-Fi) TERHADAP SERANGAN PACKET SNIFFING DI KANTOR KORAN SERUYA" bertujuan untuk membantu menganalisis protokol jaringan dan mengaudit keamanan jaringan. Metode yang digunakan dalam penelitian ini yaitu metode pendekatan deskriptif, dimana metode ini dilakukan untuk menganalisis data dengan mendeskripsikan atau menggambarkan data-data yang sudah dikumpulkan tanpa melakukan perubahan ketika melakukan penelitian di Kantor Koran Seruya. hasil analisis keamanan jaringan internet (Wi-Fi) terhadap serangan *packet sniffing* pada Kantor Koran Seruya dapat diambil. Cara melakukan penelitian dengan menyerang dan antisipasi . Hasil dan kesimpulan Kelemahan utama jaringan pada Wi-Fi kantor Koran Seruya

terdapat pada *Network Layer dan Application Layer* karena pada bagian *Network Layer* merupakan bagian perangkat yang menyediakan jaringan, dalam hal ini perangkat *Access Point* yang terdapat pada Wi-Fi Koran Seruya hanya menyediakan satu buah *Access Point* yang jangkauannya tidak terlalu efisien untuk digunakan pada perusahaan beda. Kemudian pada *Application Layer* yaitu bagian yang mengatur keamanan sertatrafficlalulintas jaringan yang dimana pada Wi-Fi Kantor Koran Seruya belum menerapkan keamanan yang efisien.

7. Sahara, R., Abdullah, S., & Saputra, R. (2022, July). "ANALISIS ANCAMAN SNIFFING PADA JARINGAN Wi-Fi DI PT.STEPA WIRAUSAHA ADIGUNA" PT. Stepa Wirausaha Adiguna merupakan suatu perusahaan yang banyak menggunakan fasilitas internet untuk dalam menjalankan aktivitas. Namun ternyata walaupun banyak digunakan tanpa disadari bahwa teknologi internet Wi-Fi ini memiliki kelemahan terutama kelemahan dibidang keamanan. Kelemahan dibidang keamanan ini contohnya serangan hacker, pencurian data data perusahaan, data-data konsumen, data- data *password*. Hal ini dapat terjadi karena komunikasi yang terjadi adalah komunikasi yang terbuka sehingga diperlukan pengamanan yang tepat dan sesuai agar dapat menghindari ataupun meminimalisir serangan tersebut. Metode Pada penelitian ini akan dilakukan percobaan sniffing pada jaringan Wi-Fi di PT. Stepa Wirausaha menggunakan Aplikasi Cain and Abel. Cara peneliti mendapatkan data yang diingin hal yang di lakukan adalah dengan menyerang dan

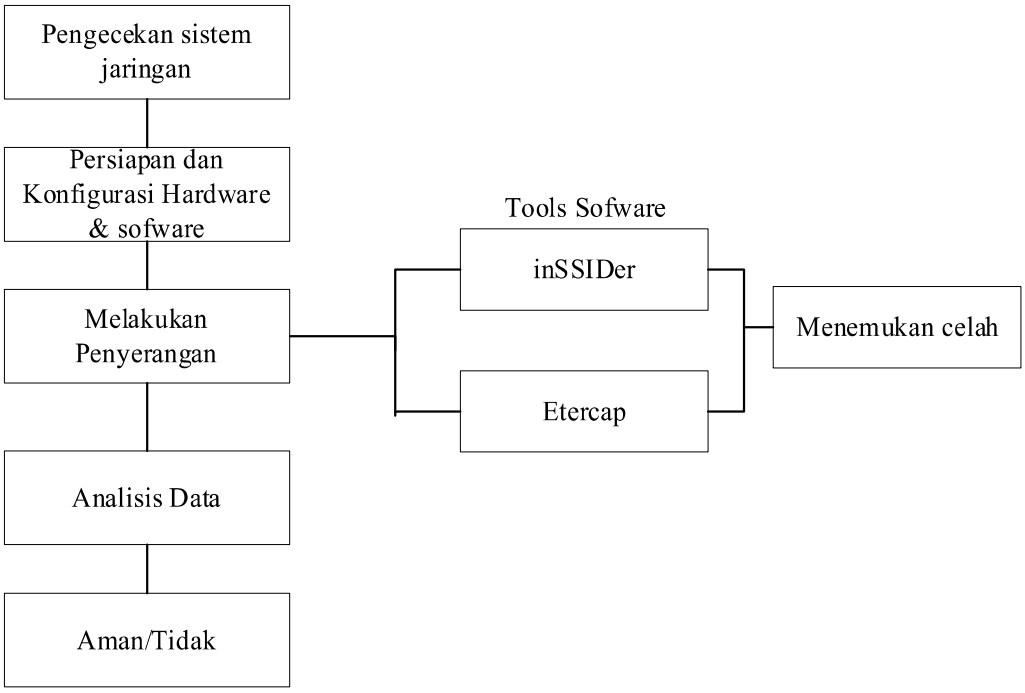
mendapatkan hasil. Hasil percobaan tersebut kemudian akan dianalisis untuk mengetahui tingkat kesulitan dari kegiatan sniffing pada suatu jaringan Wi-Fi. Serta yang tidak kalah penting adalah untuk meningkatkan kesadaran dari para pengguna jaringan Wi-Fi akan pentingnya kesadaran dalam memanfaatkan dan menggunakan jaringan internet di manapun. Kesimpulan yang dapat diambil dari penelitian adalah Aplikasi Cain and Abel mampu membaca lalu lintas jaringan dan menembus di jaringan Wi-Fi PT. Stepa Wirausaha Adiguna. Dengan penelitian ini kita juga dapat mengetahui jika melakukan sniffing dapat dilakukan oleh siapa saja. Salah satu upaya pencegahannya adalah dengan berhati-hati jika terhubung ke jaringan Wi-Fi yang tidak kita kenal agar tidak sembarangan dalam melakukan login terutama pada akun-akun penting.

8. Umasugi, A. (2022). "ANALISIS KEAMANAN JARINGAN Wi-Fi TERHADAP PACKET SNIFFING DI KAMPUS A UNIVERSITAS MUHAMMADIYAH MALUKU UTARA" Di Kampus Universitas Muhammadiyah Maluku Utara khususnya Kampus A *hotspot internet* dan kualitas sangat dibutuhkan karena untuk kebutuhan Dosen, Pegawai Kampus, dan juga Mahasiswa. UMMU telah menyediakan fasilitas internet Wi-Fi yang bida di akses penggun. Pengguna dapat mengakses hotdpot kapan saja tanpa harus meminta password. Namun hanya saja koneksi tersebut dapat saja di ganggu atau di hack oleh orang-orang yang tidak bertanggung jawab, Sebaba itu dibutuhkan network analizer protokol. Metode yang digunakan untuk membuat implementasi yaitu

penganalisaan dan perancangan system yang dimana merancang sebuah topologi, menginstal aplikasi eteercap dan *wireshark* yang nantinya digunakan oleh peneliti. Prosess pengujian menggunakan metode *black box testing* dari sisi perangkat *hardware* dan *software* sehingga proses pengujian berjalan dengan baik. Cara peneliti mendapatkan data yang diingin hal yang di lakukan adalah dengan menyerang dan mendapatkan hasil. Hasil dan kesimpulan berdasarkan penelitian yang dilakukan di kampus UMMU khususnya dikampus A ruangan ICT tentang analisis keamanan jaringan Wi-Fi terhadap serangan packet sniffing yang dimana kemanan Wi-Fi masih sangat rentan dan masih butuh keamanan jaringan yang lebih maksimal lagi.

2.5 Kerangka Pemikiran

Kerangka pikir didalam sebuah penelitian disajikan dalam bentuk sebuah diagram untuk menghasilkan solusi dari sebuah permasalahan. Skema kerangka pikir dalam penelitian ini dapat dilihat pada Gambar 2.9 yang akan disajikan sebagai berikut:



Gambar 2. 7 Kerangka Pemikiran

Agar dapat memahami kerangka pemikiran berikut penjelasan dari kerangka pemikiran :

1. Pengecekkan sistem jaringan

   proses memeriksa kondisi atau kinerja jaringan di toko services w-elektrik batam untuk menentukan apakah semua komponen berfungsi dengan baik dan sesuai dengan spesifikasi. Ini dapat dilakukan dengan menggunakan berbagai alat dan teknik, seperti:

   a. *Ping*: digunakan untuk mengecek konektivitas jaringan dengan mengirimkan paket data dari satu komputer ke komputer lainnya.
   b. *Traceroute:* digunakan untuk mengecek rute yang digunakan oleh paket data saat melintasi jaringan.
   c. *Telnet*: digunakan untuk mengecek konektivitas dengan mencoba untuk terhubung ke server atau perangkat jaringan lainnya melalui protokol Telnet.
   d. SNMP (*Simple Network Management Protocol*) : digunakan untuk mengumpulkan informasi dari perangkat jaringan yang dikonfigurasi untuk mengirimkan informasi melalui SNMP.
   e. *Network monitoring tools* : digunakan untuk mengawasi kinerja jaringan secara real-time dan menerima notifikasi jika ada masalah.

2. Persiapan Konfigurasi Hardware dan Sofware

   Menyiapkan hardware dan software yang dibutuhkkan untuk menunjang pelaksanaan penelitian.

3. Melakukan Penyerangan

Menyiapkan alat dan bahan yang akan digunakan untuk melakukan percobaan penyerangan tools yang akan di gunakan yaitu inssider dan Ettercap. Saat melakukan penyerangan peneliti menemukan Celah , Seperti *account username, password,* akses DNS yang terbuka atau Open.

4. Analisis Data

Analisa dilakukan untuk mengetahui tingkat keamanan yang diterapkan.

5. Aman/tidak

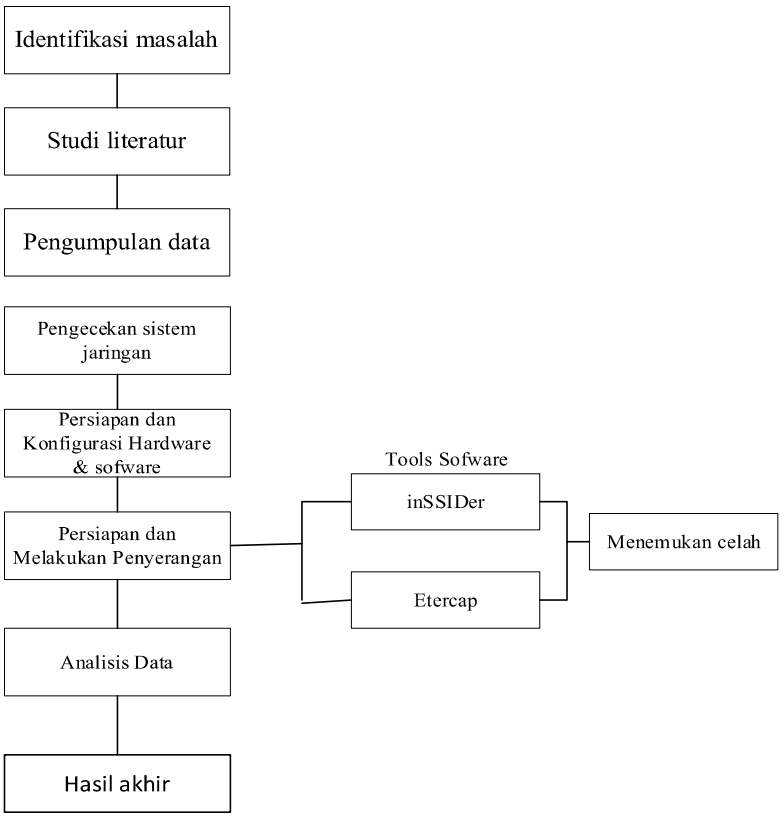
Setelah itu melakukan Analisa data maka langkah terakhir dapat di ketahui status jaringan toko service w-elektrik batam aman atau tidak aman

BAB lll

METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian menyediakan kerangka dan alur kerja mencakup sepanjang proses penelitian. Dalam desain penelitian ini, penulis membagi penelitian menjadi beberapa tahap sebagai berikut :



Gambar 3. 1 Disain Penelitian

Pada Gambar 3.1 desain penelitian didalam sebuah penelitian disajikan dalam bentuk sebuah diagram untuk menghasilkan solusi dari sebuah permasalahan. Berikut penjelasan dari desain penelitian :

1. Identifikasi masalah

   Melakukan identifikasi masalah dengan studi literatur dan pengamatan lapangan (observasi) di tempat penelitian.

2. Studi Literatur

   Melakukan studi literatur yang berhubungan dengan penelitian yaitu data – data yang berasal dari studi pustaka yang berkaitan dengan judul penelitian.

3. Pengumpulan data

   a. Observasi

      Metode ini dilakukan dengan cara pengamatan langsung pada lokasi tempat penelitian yaitu toko services w-elektrik batam dan melakukan pencatatan informasi yang berkaitan dengan obyek penelitian.

   b. Wawancara

      Wawancara adalah salah satu metode yang dilakukan untuk melengkapi hasil pengamatan yang diperoleh melalui observasi. Wawancara dilakukan terhadap pihak-pihak yang mempunyai kapasitas dan informasi yang dibutuhkan dalam hal ini pihak IT pada toko tersebut.

   c. Studi Kepustakaan

      Studi Kepustakaan adalah metode pengumpulan data dengan membaca buku referensi atau dokumentasi yang berhubungan dengan penelitian tentang keamanan jaringan. Dalam hal ini juga dilakukan *browsing* untuk mencari data atau dokumentasi yang berhubungan dengan obyek yang sedang diteliti.

4. Pengecekkan sistem jaringan

   proses memeriksa kondisi atau kinerja jaringan di toko services w-elektrik batam untuk menentukan apakah semua komponen berfungsi dengan baik dan sesuai dengan spesifikasi.

5. Persiapan dan Konfigurasi *Hardware &Software*

   Menyiapkan *hardware* dan *software* yang dibutuhkkan untuk menunjang pelaksanaan penelitian.

6. Persiapan dan melakukan penyerangan

   Menyiapkan alat dan bahan yang akan digunakan untuk melakukan percobaan penyerangan. Melakukan Penyerangan. Melangkah untuk melakukan sebuah percobaan penyerangan kepada jaringan Wi-Fi untuk mendapatkan informasi tentang keamanannya. Dan *tools* yang akan di gunakan yaitu *Inssider* dan Ettercap, saat melakukan penyerangan terdapat celah seperti accun *username* dan *password* yang mudah di dapat.

7. Menganalisa Data

   Analisa dilakukan untuk mengetahui tingkat keamanan yang diterapkan.

8. Hasil akhir

   Membuat laporan sesuai dengan hasil penelitian yang telah dilakukan.

3.2 Analisis Jaringan

3.2.1 Analisis Sistem jaringan

Analisis sistem jaringan adalah proses mengevaluasi kinerja, konfigurasi, dan topologi jaringan komputer untuk menemukan masalah dan meningkatkan kinerja. Analisis ini dapat dilakukan pada jaringan lokal (LAN) atau jaringan luas

(WAN). Berikut adalah beberapa elemen yang dapat di analisis dalam sistem jaringan:

1. *Hardware*: Meliputi perangkat keras seperti router, switch, firewall, server, dan perangkat keras lainnya yang digunakan dalam jaringan.
2. *Software*: Meliputi sistem operasi, aplikasi jaringan, dan perangkat lunak lainnya yang digunakan dalam jaringan.
3. *Topologi*: Meliputi arsitektur jaringan, seperti topologi bus, star, atau mesh, dan konfigurasi koneksi fisik antara perangkat keras.
4. Kinerja: Meliputi kecepatan jaringan, pemakaian bandwidth, dan kapasitas jaringan.
5. Keamanan: Meliputi keamanan fisik, keamanan logika, dan keamanan aplikasi dari jaringan.
6. Dokumentasi: Meliputi dokumentasi jaringan yang diperlukan untuk mengelola dan mengkonfigurasi jaringan.

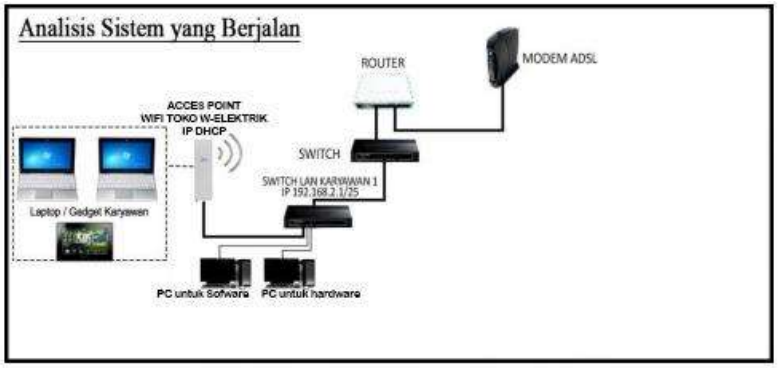
Berikut ini tabel yang dapat digunakan untuk melakukan analisis sistem jaringan:

Tabel 3. 1 Elemen analisis jaringan topologi Star

Elemen	**Deskripsi**	**Status**	**Tindakan**
Hardware	Router	Rusak	Ganti router baru
Software	Sistem operasi	Versi lama	Upgrade ke versi terbaru
Topologi	Star	Konfigurasi salah	Perbaiki konfigurasi
Kinerja	Kecepatan jaringan	Lambat	Tambahkan switch baru
Keamanan	Firewall	Kerentanan	Instal patch keamanan
Dokumentasi	Dokumentasi jaringan	Belum ada	Buat dokumentasi jaringan

Dalam tabel 3.1 Elemen analisis jaringan , setiap elemen dianalisis diberikan status dan tindakan yang diperlukan untuk mengatasi masalah yang ditemukan salah satunya topologi Star.

Sistem keamanan jaringan pada saat ini masih kurang efektif dan efisien dalam mensimulasikan tingkat keamanan pada jaringan internet di toko w-elektrik batam. Dimana keamanan jaringannya masih memiliki celah yang dapat disusupi oleh trojan dan pihak-pihak yang tidak memiliki kewenangan.



Gambar 3. 2 Analisis Sistem berjalan

Gamar 3.2 Menunjukkan analisis sistem yang sedang berjalan atau yang sedang digunakan. alat yang digunaka berupa Modem ADSL,Router,Switch, Wi-Fi Hostpot,PC,Laptop. Untuk keluhan di toko services w-elektrik batam yaitu sering terjadinya *system failure* di komputer untuk software dampaknya software atau tools yang akan di gunakan dalam bekerja tidak berjalan dengan normal, dari gambar tersebut menunjukkan PC 1 untuk software,PC 2 untuk Hardware dan Acces point untuk bebas pakai di gabungkan satu Switch hal ini sangat rentang terjadinya serangan baik virus mau pun trojan.

3.2.2 Analisis data pada jaringan

3.2.2.1 Analisi jaringan menggunakan tools ettercap

Analisis jaringan menggunakan tools Ettercap. ettercap adalah alat open-source yang digunakan untuk melakukan analisis data jaringan dan man-in-the-middle (MITM) attacks. Berikut ini tabel yang dapat digunakan untuk melakukan analisis data jaringan menggunakan tools Ettercap:

Tabel 3. 2 Tools ettercap

Elemen	Deskripsi	Hasil	Tindakan
Target IP	Alamat IP target	192.168.2.1/25	-
Filter	Filter yang digunakan	-	-
Protokol	Protokol yang digunakan	HTTP	-
Data yang ditangkap	Data yang ditangkap dari paket jaringan	Login dan password	-
Serangan	Serangan yang dilakukan	MITM	-
Hasil serangan	Hasil dari serangan	Berhasil mendapatkan Username dan password	-

Bahwa atribut pada tabel 3.2 tools ettercap berupa elemen, Deskripsi, Hasil dan Tindakan. Pada tabel diatas merupakan aktifitas Ettercap mencari celah keamanan.

Tabel 3. 3 celah keamanan menggunakan Ettercap

IP Address	Nama Host	Jenis Perangkat	Konfigurasi Firewall	Routing	Protokol jaringan	Patch dan Update	Status
192.168.1.1	Router	ACER	Aktif	Static	TCP/IP	v1.0.2	• Aman
192.168.1.2	Server	Lenovo	Aktif	Dynamic	TCP/IP	v1.0.3	• Aman
192.168.1.3	Workstation	Dell	Non- Aktif	-	TCP/IP	v1.0.1	• Tidak aman

Bahwa atribut pada tabel 3.3 berupa dari tools Ettercap. Setelah itu dapat ditentukan rule atau aturan suatu hostpot aman atau tidak yang menyebabkan *system failure*, penentuan rule sebagai berikut :

1. IF 192.168.1.1 Router and Konfigurasi firewall Aktif Routing Static TCP/IP patch update v1.0.2 then Status Aman
2. IF 192.168.1.2 Server and Konfigurasi firwall Aktif Routing Dynamic TCP/IP patch update v1.0.3 then Status Aman
3. IF 192.168.1.3 Workstation and Konfigurasi firwall Off Routing there isn't any TCP/IP Patch update v1.0.1 then Status Tidak Aman

Analisis ini menunjukan potensi celah keamanan. Tabel ini menunjukkan beberapa informasi penting mengenai perangkat jaringan, konfigurasi jaringan, patch dan update yang digunakan dan ancaman yang di temukan dalam jaringan.

3.2.2.2 Cara kerja Trojan

Trojan umumnya bergerak melalui tahapan berikut:

1. Pengiriman: Trojan dikirimkan ke komputer korban, biasanya disamarkan sebagai aplikasi yang sah atau disertakan dalam email yang tampaknya tidak berbahaya.
2. Instalasi: Dengan membuka lampiran email yang terinfeksi atau menjalankan program yang disamarkan, korban tanpa sadar menginstal trojan di komputer mereka.
3. Eksekusi: Trojan akan mulai mengeksekusi kode jahatnya di komputer korban setelah diinstal.
4. Kontrol dan Perintah: Trojan terhubung ke server perintah dan kontrol penyerang, memungkinkan penyerang untuk mengontrol komputer yang terinfeksi dari jarak jauh.
5. Ekstraksi dan pengumpulan data: Kata sandi, data keuangan, dan informasi pribadi hanyalah beberapa dari data sensitif yang mulai dicuri trojan dari komputer yang terinfeksi. Server perintah dan kontrol penyerang menerima data ini setelah dieksfiltrasi (ditransfer).
6. Panel kontrol: Komputer yang terinfeksi dapat diakses dari jarak jauh oleh penyerang, yang kemudian dapat menggunakannya untuk melancarkan serangan tambahan, menyebarkan malware, atau bahkan menggunakannya

sebagai titik pivot untuk menyerang sistem jaringan lain. Penting untuk diingat bahwa tidak semua trojan dibuat sama, dan beberapa dirancang untuk tujuan yang berbeda. Akibatnya, langkah-langkah yang disebutkan di atas mungkin tidak selalu diperlukan.

3.2.2.3 Identifikasi Trojan

Tujuan dari identifikasi trojan di toko services w-elektrik batam adalah untuk mengetahui apakah ada trojan yang menyebar di jaringan komputer tersebut, dan jika ada, mengidentifikasi trojan tersebut agar dapat diambil tindakan pencegahan dan penanganan yang tepat. Identifikasi trojan juga bertujuan untuk mencegah penyebaran virus ke sistem lain di jaringan, serta untuk mengurangi risiko keamanan yang disebabkan oleh trojan.

Ada beberapa tools atau perangkat lunak yang dapat digunakan untuk mengidentifikasi trojan pada komputer:

1. Antivirus: Antivirus adalah perangkat lunak yang dirancang untuk mendeteksi dan menghapus virus, Trojan, dan ancaman lain yang mungkin ada pada komputer. Banyak antivirus memiliki fitur pemindaian yang dapat memindai sistem komputer dan menemukan ancaman yang terdeteksi.
2. Malware scanner: Malware scanner adalah perangkat lunak yang dirancang untuk mendeteksi dan menghapus malware, termasuk trojan. Beberapa malware scanner hanya menyaring file yang terinfeksi, sementara yang lain juga dapat memindai sistem untuk menemukan ancaman yang tersembunyi.

3. Security suite: Security suite adalah perangkat lunak yang menyediakan pelindung keamanan lengkap untuk komputer, Termasuk antivirus, firewall, dan fitur-fitur keamanan lainnya. Security suite dapat membantu mengidentifikasi dan menghapus virus trojan yang mungkin ada pada komputer.
4. Online virus scanner: Online virus scanner adalah layanan yang menyediakan pemindaian virus secara online. Dapat menggunakan online virus scanner untuk memindai komputer tanpa perlu menginstall perangkat lunak tambahan.
5. Command-line tools: Command-line tools adalah perangkat lunak yang dapat dijalankan dari command prompt atau terminal. Beberapa command-line tools yang dapat digunakan untuk mengidentifikasi trojan termasuk ClamAV, Chkrootkit, dan Rootkit Hunter.

   Jika mencurigai adanya trojan pada computer.

Tabel 3. 4 Indentifikasi Trojan

Nama Trojan	Lokasi File	Tanggal di Temukan	Tingkat Kerentanan	Tindakan
Trojan.FakeAV	C:\Windows\System32\	01/20/2023	Tinggi	Dihapus dan dihapus
Trojan.Banker	C:\Users\Public\	01/19/2023	Sedang	Dihapus dan dihapus
Trojan.Ransomware	C:\Program Files\	01/18/2023	Tinggi	Dihapus dan dihapus

Untuk mengetahui aktifitas pada tabel 3.4 ada beberapa atribut yang di tampilkan seperti, Nama trojan yang ditemukan, lokasi file, tanggal ditemukan, tingkat kerentanan trojan, dan tindakan yang diambil semuanya ditampilkan di tabel. Maka penentuan rule atau aturan sebagai berikut :

1. IF Trojan.FakeAV Detected Aktif C:\Windows\System32\ and hard to remove. Maka Tingakat kerentanan Tinggi,Tindakan Install ulang Windows
2. IF Trojan.Banker Detected Aktif C:\Users\Public\ and can be deleted.

   Maka Tingkat Kerentanan Sedang Tindakan Upgrade Antirus
3. IF Trojan.Ransomware Detected Aktif C:\Program Files\ and can be deleted but come back.

   Maka Tingkat Kerentanan Tinggi, Tindakan Upgrade windows atau Update antivirus.

3.2.2.4 Analisis jaringan menggunakan tools InSSIDer

Analisis jaringan menggunakan tools InSSIDer, adalah alat yang digunakan untuk menganalisis jaringan nirkabel (Wi-Fi) dan menemukan masalah yang mungkin terjadi. Berikut ini adalah contoh tabel yang dapat digunakan untuk melakukan analisis jaringan menggunakan alat InSSIDer:

Tabel 3. 5 Rule atau aturan pada tools InSSDer

SSID	Signal	Chanel	Security	MAC.Addres	802.11
	-85	10	Wpa2/personal	OC:37:47:92:DF:97	n
	-85	10	Wpa2/personal	OE:37:47:B1:DF:97	n
Rumah putri	-80	11	Wpa2/personal	FC:A6:CD:BB:37:CO	n
Toko w-lektrik	-25	11	Open	36:E9:11:3A:75:99	n
Doraemon	-76	1	Open	68:37:47:92:DF:97	n
	-80	3	Wpa2/personal	C4:A3:66:B1:75:14	n

Untuk mengetahui aktifitas pada tabel 3.5 ada beberapa atribut yang di tampilkan seperti SSID,Signal, Chanel, Security, MAC Addres dan 802.11. Adapun penjelasan atribut pada table,

1. SSID (*Service Set Identifier*) adalah nama unik yang diberikan kepada setiap jaringan wireless. SSID digunakan untuk mengidentifikasi jaringan wireless yang spesifik dan membedakannya dari jaringan wireless lain yang ada di lingkungan yang sama.
2. Signal adalah Kekuatan dan kualitas transmisi data antar perangkat dalam jaringan disebut sebagai sinyal. Istilah "sinyal" digunakan untuk menggambarkan kekuatan sinyal yang diterima perangkat yang terhubung ke jaringan nirkabel.

3. Chanel atau kanal adalah Jalur komunikasi yang digunakan jaringan untuk mengirim dan menerima data dikenal sebagai saluran dalam konteks jaringan internet.
4. Security adalah menjaga kerahasiaan dan integritas data yang dikirimkan jaringan, keamanan jaringan sangat penting. Keamanan jaringan dapat dicapai melalui berbagai teknologi dan pendekatan, WPA2 (Wi-Fi Protected Access 2) adalah standar keamanan jaringan wireless yang digunakan untuk mengamankan jaringan wireless dengan menggunakan metode enkripsi yang kuat. OPEN adalah konfigurasi jaringan nirkabel yang tidak menggunakan keamanan atau enkripsi. Ini menunjukkan bahwa tidak ada kunci enkripsi atau kata sandi untuk jaringan dan siapa pun yang memiliki akses fisik dapat mengaksesnya.
5. MAC (Media Access Control) Address adalah alamat unik yang diberikan kepada setiap perangkat yang terhubung ke jaringan. Alamat ini digunakan untuk mengidentifikasi perangkat yang spesifik dalam jaringan dan membedakannya dari perangkat lain yang terhubung ke jaringan yang sama.
6. "n" dalam konteks InSSIDer merujuk ke jenis jaringan wireless yang menggunakan standar IEEE 802.11n. Standar ini meningkatkan kecepatan data hingga sekitar 300Mbps dan meningkatkan jangkauan sinyal dibandingkan dengan standar sebelumnya, seperti 802.11g.

Maka penentuan rule atau aturan sebagai berikut :

1. IF Rumah putri signal -80 chanel 11 Security Wpa2/personal and MAC Addres 802.11.n then status aman
2. IF Toko w-elektrik -25 chanel 11 security Open And MAC.Addres 802.11n then Status Tidak aman
3. IF Doraemon -75 chanel 1 security Open And MAC.Addres 802.11.n then Status Tidak aman

Tabel 3. 6 Analisis jaringan menggunakan tools InSSIDer

Elemen	**Deskripsi**	**Hasil**	**Tindakan**
Nama jaringan (SSID)	Nama dari jaringan nirkabel	w-eletrik	-
Kanal	Kanal jaringan nirkabel	6	-
Keamanan	Jenis keamanan yang digunakan	WPA2	-
Signal Strength	Kekuatan sinyal	-60dBm	-
Interference	Gangguan yang terdeteksi	Adanya jaringan yang lain pada kanal yang sama	Ganti Kanal jaringan
Kinerja	Kecepatan jaringan	5Mbps	-

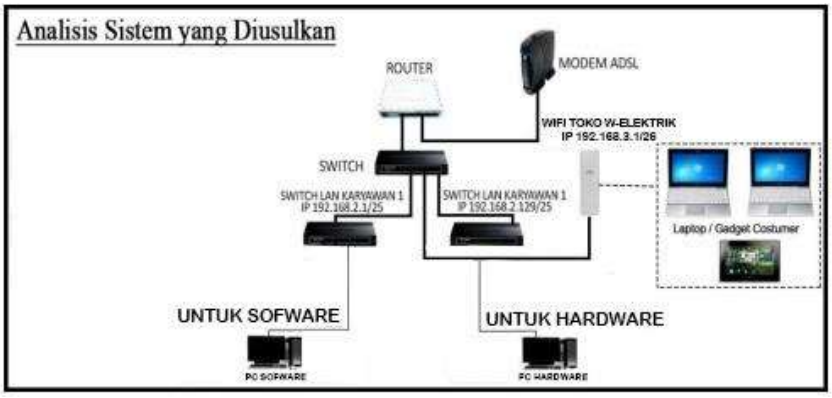
Dalam tabel diatas, setiap elemen dianalisis dan diberikan hasil dan tindakan yang diperlukan untuk mengatasi masalah yang ditemukan. InSSIDer memberikan informasi yang cukup detail mengenai jaringan yang dianalisis, seperti SSID, kanal, keamanan, signal strength, interference dan kinerja, yang dapat membantu mengidentifikasi masalah dan memberikan solusi yang tepat. Untuk menentukan apakah jaringan internet aman atau tidak, beberapa informasi dalam

tabel perlu diperiksa. Beberapa tabel dapat digunakan untuk memeriksa data apakah jaringan aman atau tidak.

3.3 Rancangan Jaringan yang Dibangun/ Diusulkan

3.4.1. Analisis Sistem yang Diusulkan

Analisis sistem yang diusulkan yaitu identifikasi celah keamanan jaringan Wi-Fi dengan tools NetStumbler mengaudit keamanan jaringan dan memblokir lalulintas jaringan yang dianggap sebagai ancaman dalam jaringan internet serta melakukan pengecekan terhadap kesalahan pada bagian media, wireless, dan media koneksinya.



Gambar 3. 3 Analisis sistem yang di usulkan

Gambar 3.3 berupa analisis sistem jaringan yang diusulkan ada beberapa komponen yang di tampilkan berupa Modem ADSL,Router,Switch, Wi-Fi Hotspot, Komputer, laptop. Sebelum peneliti menemukan analisis sistem yang diusulkan, perlu ditentukan tujuan dari jaringan tersebut dan kebutuhan yang harus dipenuhi. Kemudian, perlu dilakukan studi kelayakan untuk menentukan konfigurasi jaringan yang sesuai dan memenuhi kebutuhan tersebut. Setelah itu, perlu dilakukan analisis

kinerja jaringan untuk menentukan kapasitas yang diperlukan dan untuk mengidentifikasi potensi masalah yang mungkin terjadi.

3.4 Lokasi dan Jadwal Penelitian

3.4.1 Lokasi Penelitian

Adapun lokasi yang dijadikan tempat penelitian yaitu toko services w-elektrik batam, di Jl. Kavling Mandiri blok A no 13-14. Waktu penelitian berlangsung pada bulan September 2022 hingga Febuari 2023.

3.4.2 Jadwal Penelitian

Tabel 3. 7 Tabel Penelitian

No	Jenis Kegiatan	Bulan					
		September 2022	Oktober 2022	November 2022	Desember 2022	Januari 2023	Februari 2023
1	Studi Pustaka						
2	Penyusunan Proposal						
3	Pengumpulan Data						
4	Analisis Hasil Penelitian						
5	Penyusunan Laporan						
6	Penyerahan Hasil						
7	Hasil Sidang						

***Sumber** : (Peneliti 2022)*