BAB II

TINJAUAN PUSTAKA

2.1 Teori dasar

2.1.1 Jaringan komputer

Saat ini, perkembangan teknologi informasi mengalami kemajuan pesat dan telah menjadi elemen integral dalam kehidupan kita. Setiap individu pada era ini umumnya menggunakan teknologi informasi. Dengan kepentingan yang besar terhadap teknologi informasi, banyak perusahaan, institusi pendidikan, sekolah, dan organisasi lainnya merancang infrastruktur teknologi informasi dengan jaringan komputer yang berkualitas tinggi.(Subekti & Subandri, 2019).

Berdasarkan kutipan dari (Komputer & Komputer, 2020), Jaringan komputer merupakan sekumpulan komputer. Ini artinya komputer tersebut lebih dari satu buah yang terpisah-pisah akan tetapi dapat saling berhubungan dalam melaksanakan suatu tugas. Sekelompok komputer tersebut bekerja secara otonom. Ini artinya hanya dapat melakukan pertukaran dalam suatu area atau member tertentu. Pembuatan jaringan komputer ini menggunakan protocol komunikasi melalui media komunikasi yang saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, harddisk, dan sebagainya. Jaringan komputer juga dapat dikatak sebagai kumpulan sejumlah terminal komunikasi yang berada diberbagai lokasi yang terdiri dari satu atau lebih komputer yang saling terkoneksi seperti yang dijelaskan diatas.

2.1.2 Standar Jaringan Komputer

Standar jaringan penting buat meyakinkan perangkat keras dan lunak bisa bekerja sama. Ada beberapa Organisasi yang bertanggung jawab untuk menetapkan standar dalam jaringan komputer yaitu (Galih, 2020).

Tabel 2. 1 Badan Pekerja di IEEE

Working Group	Bentuk Kegiatan
IEEE802.1	Standart LAN/MAN
IEEE802.2	Standart *Logical Link Control* (LLC).
IEEE802.3	Standart untuk *Ethernet Coaxial* atau UTP
IEEE802.4	Standart *Token Bus*.
IEEE802.5	Standart *Token Ring*.
IEEE802.6	Standart MAN-DQDB.
IEEE802.7	Standart LAN *Broadband*
IEEE802.8	Standart FDDI
IEEE802.9	Standart ISDN
IEEE802.10	Standart LAN/MAN untuk VPN
IEEE802.11	Standart LAN nirkabel untuk *Wifi*
IEEE802.12	Standart DPAM (*Demand Priority Access Method*)
IEEE802.15	Standart PAN nirkabel untuk IrDA dan *Bluetooth*
IEEE802.16	Standart *WiMAX*

2.1.2.1 Serangkaian standar IEEE802

Norma-norma IEEE 802 adalah serangkaian standar yang diperkenalkan oleh Institute of Electrical and Electronics Engineers (IEEE) untuk jaringan komunikasi lokal (*LAN*) dan nirkabel. Standar ini mencakup beragam teknologi jaringan, melibatkan Ethernet kabel, *Wi-Fi*, dan Bluetooth sebagai contoh teknologinya.

Dalam konteks *Wi-Fi*, terdapat sejumlah standar yang tergolong dalam kategori IEEE 802.11. Berikut beberapa standar *Wi-Fi* yang umum digunakan:

1. IEEE 802.11b: Diperkenalkan pada tahun 1999, standar ini memberikan kecepatan transfer data hingga 11 Mbps dalam jaringan nirkabel dan beroperasi pada frekuensi 2,4 GHz.
2. IEEE 802.11a: Diperkenalkan pada tahun 1999, standar ini menawarkan kecepatan transfer data hingga 54 Mbps. Berbeda dengan 802.11b, standar ini beroperasi pada frekuensi yang lebih tinggi yaitu 5 GHz dan memiliki jangkauan yang lebih pendek.
3. IEEE 802.11g: Diperkenalkan pada tahun 2003, standar ini menggabungkan fitur 802.11b dan 802.11a. Ini beroperasi pada frekuensi 2,4 GHz dan menawarkan kecepatan transfer data hingga 54 Mbps.
4. IEEE 802.11n: Diperkenalkan pada tahun 2009, standar ini adalah salah satu standar *Wi-Fi* yang paling banyak digunakan saat ini. Meningkatkan kecepatan transfer data hingga 600 Mbps dan memperluas jangkauan jaringan nirkabel. Dapat beroperasi pada frekuensi 2,4 GHz dan/atau 5 GHz.

5. IEEE 802.11ac: Juga dikenal sebagai *Wi-Fi* 5, standar ini diperkenalkan pada tahun 2013 dan menawarkan kecepatan transfer data hingga beberapa Gbps. Ini beroperasi pada frekuensi 5 GHz, yang memiliki kinerja lebih baik dan jangkauan lebih luas dibandingkan dengan 802.11n.
6. IEEE 802.11ax: Juga dikenal sebagai *Wi-Fi* 6, standar ini diperkenalkan pada tahun 2019. *Wi-Fi* 6 menggunakan teknologi seperti akses ganda pembagian frekuensi ortogonal (OFDMA) dan multiplexing multiplexing multi-pengguna (MU-MIMO) untuk meningkatkan efisiensi dan kecepatan transfer data. Ini beroperasi pada frekuensi 2.4GHz dan/atau 5GHz.
7. IEEE 802.11ay: Standar ini masih dalam pengembangan dan diharapkan dapat diperkenalkan di masa mendatang. Ini beroperasi pada frekuensi 60 GHz dan diharapkan memberikan kecepatan transfer data hinggaGbps.

2.1.3 Jenis Jaringan Komputer

Jenis jaringan komputer bisa dibagi sesuai kriteria seperti sebagai berikut:

Jaringan komputer berdasarkan jangkuan dibagi menjadi 4 jenis, yaitu

(Moshinsky, 2019).

1. *Local Area Network* (*LAN*) atau Jaringan Area Lokal

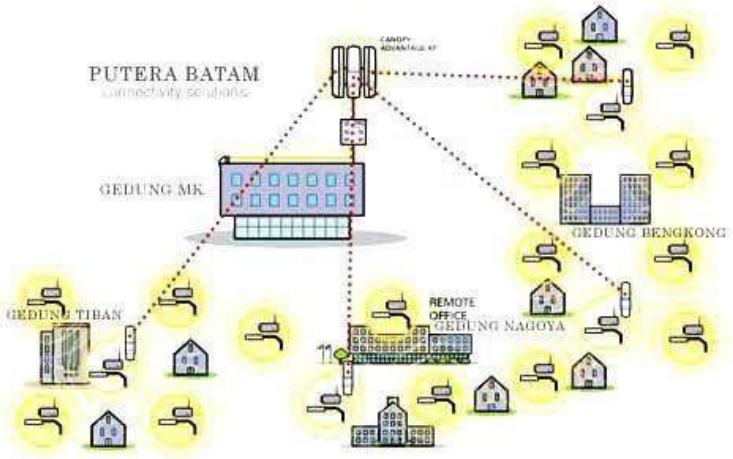
Jaringan area lokal (*LAN*) adalah jaringan dengan area lokal terbatas, terbatas pada lingkungan tertentu, seperti rumah atau kantor di sekolah, dengan luas maksimal mendekati 1 kilometer persegi. Pada beberapa contoh konfigurasi jaringan area lokal, salah satu komputer digunakan sebagai file *server* yang berfungsi sebagai tempat penyimpanan komputer-komputer yang mendukung fungsi jaringan atau komputer-komputer yang dapat digunakan oleh komputer-

komputer dalam jaringan, seperti workstation. Workstation lebih kecil dari *server* file dan menampilkan aplikasi offline yang disimpan di hard drive. Kebanyakan *LAN* menggunakan media kabel untuk menghubungkan satu komputer dengan komputer lainnya.

Gambar 2. 1 *LAN (Local Area Network)*

2. *Metropolitan Area Network* (MAN) atau Jaringan Area Metropolitan

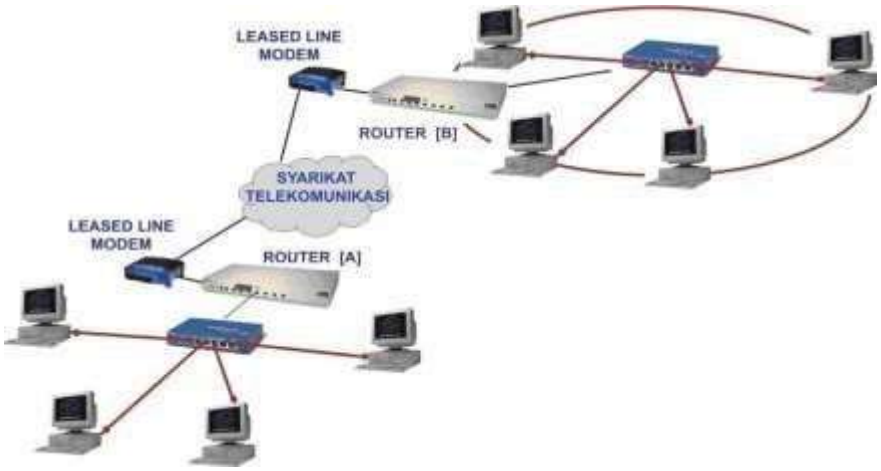
MAN adalah versi *LAN* yang lebih besar dan menggunakan teknologi yang sama dengan *LAN*. Seorang pria dapat meliput kantor perusahaan atau kota terdekat, dan dapat digunakan untuk keperluan pribadi atau publik. MAN dapat mengirimkan data dan suara dan juga dapat terhubung ke jaringan televisi.



Gambar 2. 2 *MAN (Metropolitan Area Network)*

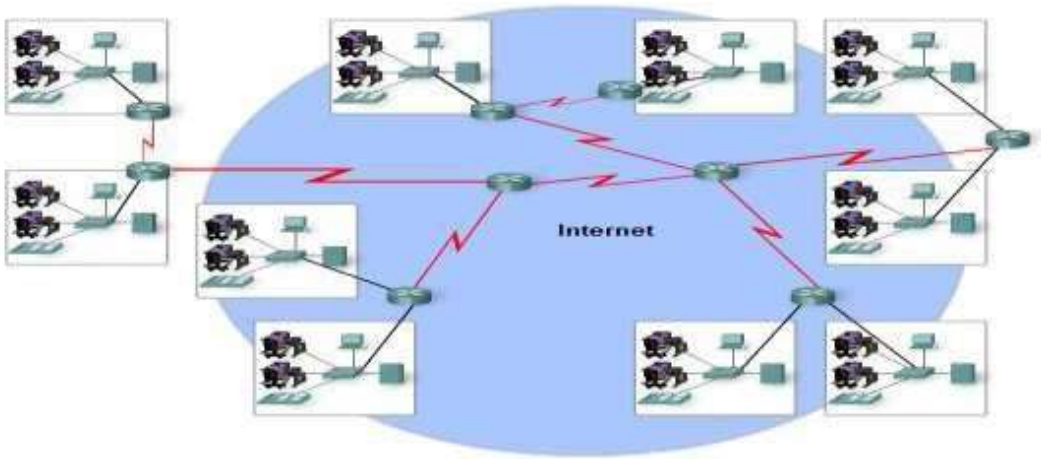
3. *Wide Area Network* (WAN) atau Jaringan Area Skala Besar

WAN adalah jaringan yang dapat mencakup wilayah geografis yang luas, termasuk sebagian besar negara. WAN sering kali menggunakan satelit dan kabel bawah tanah. Internet adalah contohnya.



Gambar 2. 3 *WAN (Wide Area Network)*

4. Internet (jaringan yang saling terhubung) menjangkau seluruh dunia, termasuk *LAN* tradisional, *WAN*, dan *MAN*.



Gambar 2. 4 Internet *(Interconnected Network)*

2.1.4 Keamanan jaringan komputer

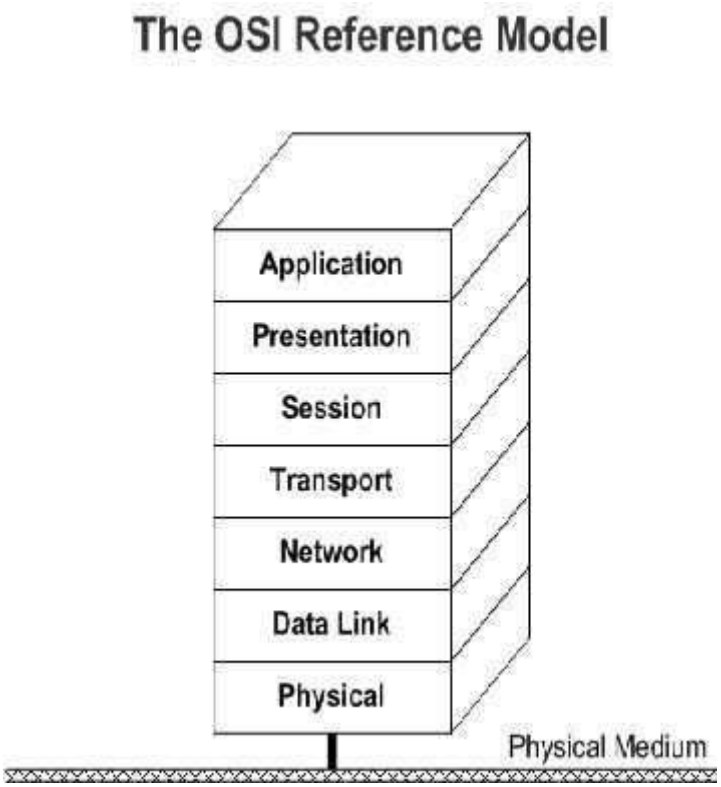
2.1.5 Jenis Ancaman Jaringan Komputer

Keamanan jaringan komputer memiliki empat kategori utama yang mewakili berbagai jenis ancaman keamanan jaringan komputer: Ancaman keamanan jaringan komputer dibagi menjadi empat kategori: penggunaan informasi Internet of Things yang berbahaya, serangan penolakan layanan di latar belakang, kerusakan integritas jaringan komputer. lingkungan jaringan komputer dan aliran komputer. Pertama, *Internet of Things* memiliki banyak kesalahan terkait penggunaan komputer, karena pengguna mengabaikan potensi masalah dan fokus pada aktivitas seperti mengakses situs web dan mengunduh *file*. Situs *web, file,* atau tautan mungkin berisi virus atau *file* berbahaya lainnya, yang dapat membahayakan keamanan jaringan komputer Anda. Tanpa aplikasi pemindaian *virus* atau *file* berbahaya, informasi di komputer Anda dapat rusak atau bahkan terhapus. Kedua, serangan layanan latar belakang melibatkan upaya penolakan layanan untuk mencegah pengguna mengakses atau mengganggu situs web atau mengunduh *file* tanpa izin. Hal ini dapat menyebabkan beberapa kompromi dalam keamanan jaringan komputer. Ketiga, keamanan jaringan komputer terganggu ketika kelompok atau individu jahat menggunakan metode ilegal untuk menyalahgunakan keamanan jaringan komputer, sehingga mengancam integritas keamanan komputer secara keseluruhan. Keempat, pelanggaran informasi komputer terjadi ketika informasi dikirimkan secara langsung melalui jaringan komputer ke pihak yang tidak berwenang tanpa izin. Hal ini membuat informasi

anda rentan. Risiko lalu lintas komputer yang umum mencakup intrusi virus dan *trojan horse,* kerentanan sistem pengguna, pencurian frekuensi radio, pemasangan alat pengawasan, dan fitur keamanan jaringan komputer lainnya. (Laporan Uji Keamanan Jaringan).

2.1.6 Model OSI layer

Sebelum tahun 1990, model hierarki yang dominan dalam literatur komunikasi dan jaringan adalah model Open Systems Interconnection (OSI) yang disebutkan oleh Andi Basoalf. Model OSI diciptakan pada tahun 1947 oleh organisasi multinasional yang dikenal sebagai Organisasi Internasional untuk Standardisasi (ISO) dan berfungsi sebagai badan pembuat standar dunia. ISO juga merupakan badan penerbitan standar jaringan telekomunikasi yang mencakup seluruh aspek dan mengacu pada model OSI. Untuk memahami keamanan jaringan komputer, terlebih dahulu kita harus memahami cara kerja jaringan komputer sesuai dengan gagasan Andi Basoalfi (Anuigrah, 2018). Untuk menyederhanakan pemeliharaan dan meningkatkan kompatibilitas antara berbagai pihak yang terlibat, jaringan komputer mengikuti standar ISO/OSI dan dibagi menjadi beberapa lapisan yang saling eksklusif. Menurut standar OSI/ISO, lapisan jaringan ini adalah: Lapisan fisik, Lapisan komunikasi data, Lapisan jaringan, Lapisan transport, Lapisan sesi, Lapisan presentasi dan Lapisan aplikasi menggunakan antarmuka seperti Ethernet, USB, HDMI, dan SATA. (Anugrah, 2018).

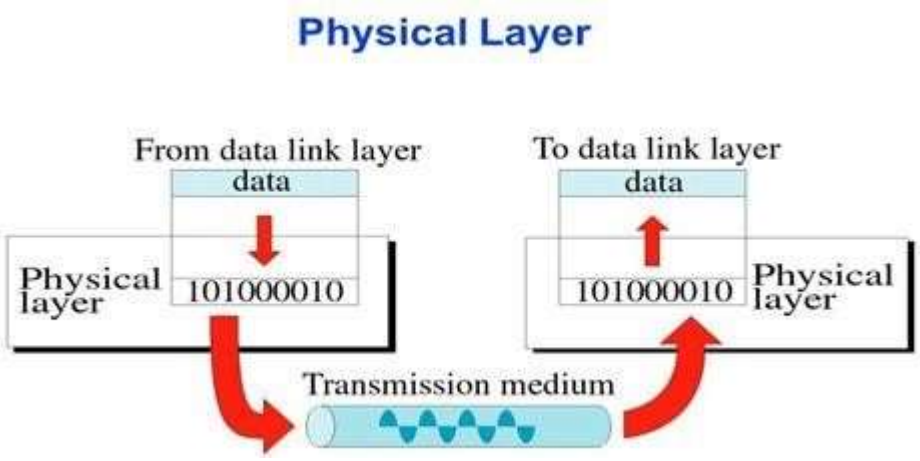


Gambar 2. 5 *Model OSI Layer*

Tujuh lapis model layer

1. Fisik (Physical Layer)

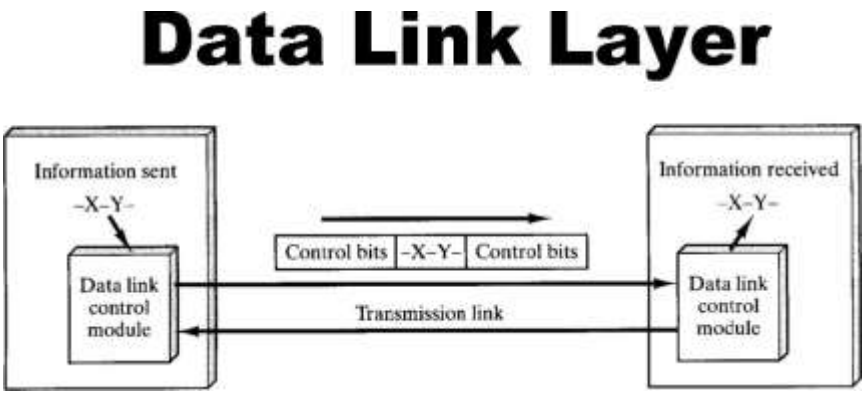
Lapisan fisik jaringan mencakup penggunaan kabel fisik, serat optik atau kartu, dan penggunaan perangkat keras dan perangkat elektronik lainnya yang mendukung infrastruktur jaringan. Tujuan dari lapisan ini adalah untuk mengubah data digital menjadi sinyal yang dapat ditransmisikan melalui kabel selama transmisi data. Sinyal-sinyal ini bisa berupa sinyal listrik yang berasal dari serat optik atau diubah menjadi sinyal non-listrik seperti sinyal optik atau jenis sinyal lain yang dapat dikodekan secara digital.



Gambar 2. 6 *Physical layer*

2. Hubungan data (*Data Link Layer*)

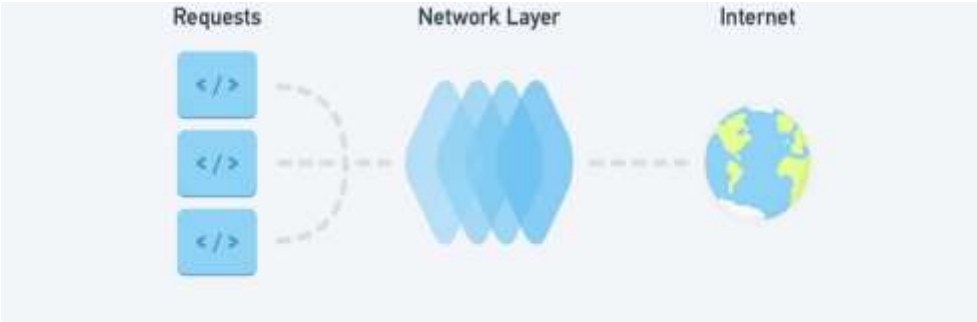
Lapisan data link adalah tempat kelompok informasi disusun menjadi "masalah". Ini dikoordinasikan, dihubungkan bersama dan dikirim ke lapisan yang lebih tinggi. Pada dasarnya, lapisan data link memproses data mentah dari lapisan fisik dan mengubah informasi dari berbagai lapisan di atasnya menjadi data mentah yang dikirim melalui lapisan fisik. Lapisan data link bertanggung jawab untuk mendeteksi dan mengkompensasi kesalahan yang mungkin terjadi pada lapisan fisik.



Gambar 2. 7 *Data link layer*

3. Jaringan (*Network Layer*)

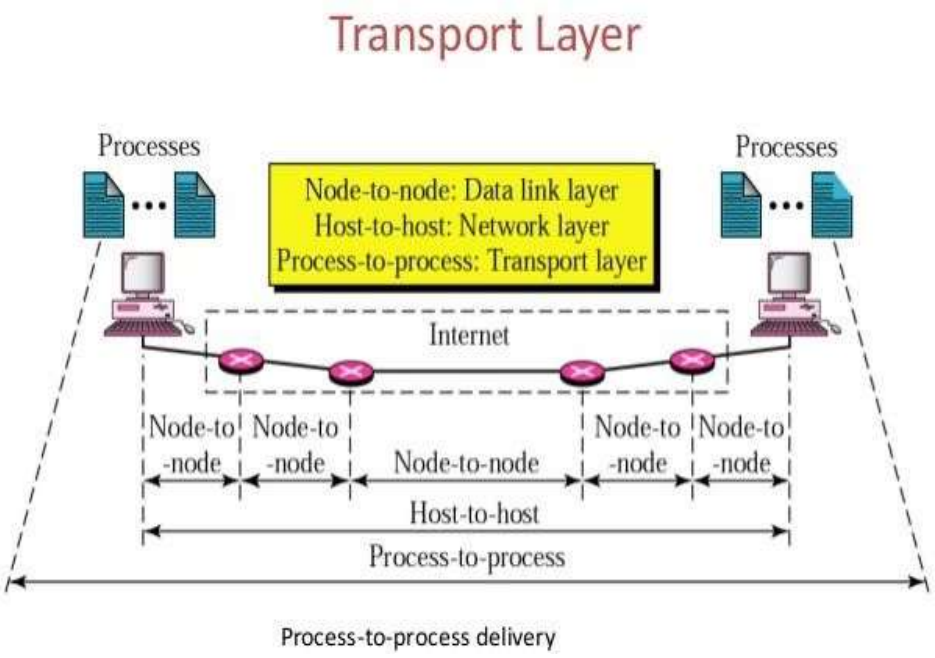
Lapisan jaringan merupakan titik tujuan data masuk dan keluar. Ini adalah lapisan penting di mana router memastikan bahwa data dirutekan dengan benar sebelum dikirim ke jalur paket berikutnya. Pada lapisan ini, router beroperasi untuk memastikan bahwa data dapat diarahkan kembali secara efisien sebelum diteruskan ke jalur paket selanjutnya.



Gambar 2. 8 *Network layer*

4. Transportasi *(Transport Layer)*

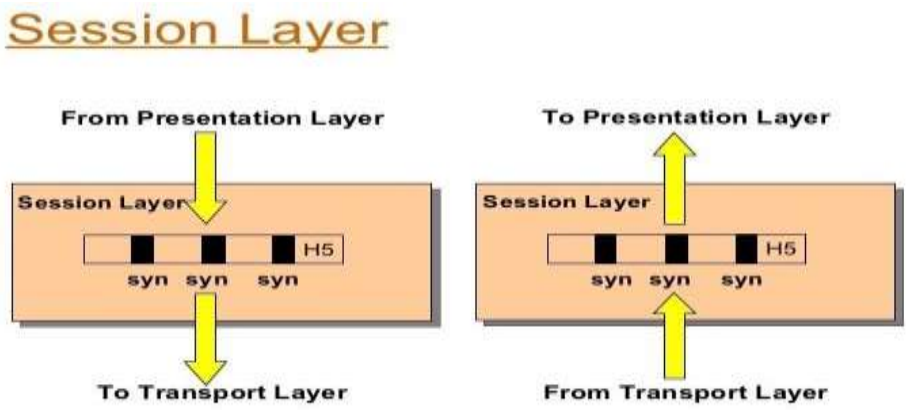
Lapisan ini bertugas untuk mengatur jalur data melalui jaringan. Pada level ini, data tidak diproses sebagai akun individu, namun dalam konteks percakapan. Untuk mencapai tingkat ini, protokol, yang dianggap sebagai standar komunikasi, memainkan peran penting. Protokol ini memantau transmisi seluruh rangkaian paket, memeriksa kesalahan pada setiap percakapan, mengetahui transmisi yang berhasil, dan meminta transmisi ulang jika kesalahan terdeteksi.



Gambar 2. 9 *Transport layer*

5. Sesi *(Session Layer)*

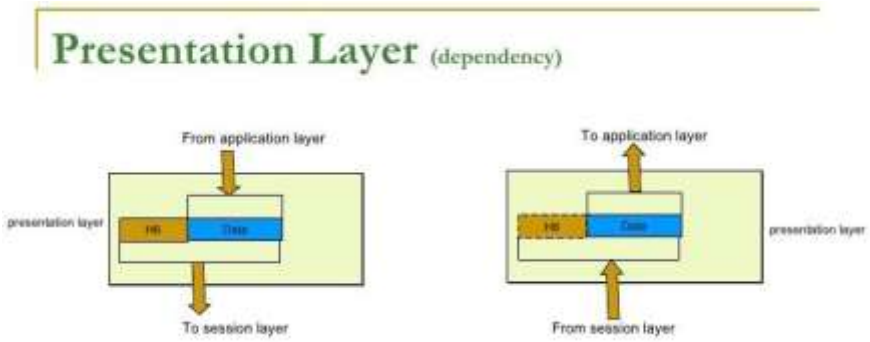
Lapisan lokal adalah tempat koneksi jaringan dibuat, dipelihara, dan diakhiri. Pada dasarnya, lapisan ini terhubung dengan permintaan data yang mengalir melalui jaringan. Sementara lapisan transport mengelola aliran data aktual, lapisan tujuan bertindak sebagai perantara dan memastikan bahwa program dan aplikasi dapat meminta dan mengirimkan data yang mereka perlukan. Dari sudut pandang teknis, lapisan sesi bertanggung jawab atas sinkronisasi data siaran.



Gambar 2. 10 *Session layer*

6. Presentasi *(Presentation Layer)*

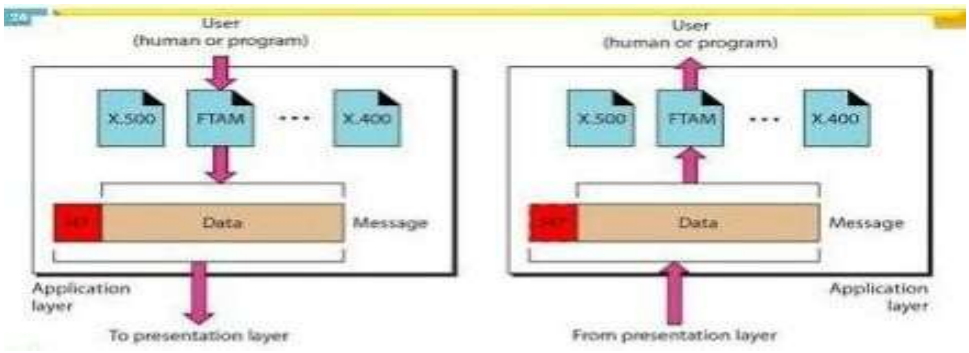
Lapisan presentasi merupakan tempat di mana data yang akan diterima diubah menjadi format tertentu agar dapat dipahami oleh aplikasi tersebut. Fungsi yang dilakukan pada lapisan ini dapat dianggap sebagai fungsi terjemahan. Misalnya, data dienkripsi di lapisan presentasi sebelum dikirim ke lapisan lain. Setelah data diterima, data tersebut didekripsi dan diubah ke format yang diharapkan oleh aplikasi yang diinginkan.



Gambar 2. 11 *Presentation layer*

7. Aplikasi *(Aplication Layer)*

Lapisan aplikasi bertanggung jawab untuk mengkoordinasikan akses jaringan agar perangkat lunak dapat berjalan di komputer atau perangkat. Protokol lapisan aplikasi menangani permintaan berbeda dari perangkat lunak berbeda untuk berkomunikasi dengan jaringan. Misalnya, jika pengguna ingin menjelajahi web untuk melihat gambar tertentu, pengguna email ingin memeriksa *server*, atau program berbagi file mengunggah file film atau video ke lapisan aplikasi, membuat dan memelihara aplikasi.



Gambar 2. 12 *Aplication layer*

2.2 Teori Khusus

Peneliti meneliti konsep-konsep tertentu yang berkaitan dengan penelitiannya dengan merujuk informasi dari penelitian sebelumnya dalam buku atau jurnal. Dalam konteks teori khusus ini, peneliti memilih variabel-variabel yang akan digunakan dalam penelitian untuk membuat struktur data penelitian, dan kemudian menjelaskan pada setiap poin konsep atau variabel sebagai landasan penelitian.yang akan dijelaskan sebagai berikut :

2.2.1 *WiFi*

Wi-Fi adalah suatu standar jaringan nirkabel yang diberikan pada *Wireless Local Area Network (WLAN).* Ini merupakan jaringan komputer yang menggunakan gelombang sinyal radio sebagai media transmisi untuk pertukaran data. *Wi-Fi* memungkinkan perangkat untuk terhubung ke jaringan tanpa kabel, hanya dengan komponen yang memadai (Jurnal et al., 2023).

Peran teknologi nirkabel sangat krusial dalam meningkatkan kecepatan, kenyamanan, dan akurasi akses informasi. Dengan kemampuan akses tanpa kabel, pengguna dapat terhubung ke jaringan Internet atau lokal dari berbagai lokasi, memungkinkan mobilitas dan meningkatkan efisiensi kerja.(Ali et al., 2023)

2.2.2 *Sniffing*

Adalah serangan yang dilakukan dengan memonitor atau mengawasi lalu (Jurnal et al., 2023) lintas data yang melewati jaringan komputer, baik melalui jaringan kabel maupun nirkabel *(wireless),* dengan tujuan mencuri informasi sensitif seperti *username*, *password,* nomor kartu kredit, atau informasi penting lainnya yang dapat digunakan untuk tindakan penipuan atau kejahatan lainnya. *Sniffing* umumnya dilakukan dengan menggunakan alat atau program yang dikenal sebagai "*Sniffer*" atau "*packet Sniffer*." (Hidayat et al., 2018).

Sniffing pada dasarnya bukanlah teknik hacking yang kompleks atau sulit dilakukan, tetapi dapat sangat efektif dalam mencuri informasi jika dilakukan dengan bijak dan tanpa diketahui oleh korban atau pengelola jaringan. Oleh karena itu, pemanfaatan teknik *sniffing* untuk tujuan ilegal atau tanpa izin dapat

menimbulkan tindakan hukum dan merugikan banyak pihak.(Hidayat et al., 2018).

2.3 *Tools*

Dalam konteks keamanan jaringan, *Wireshark* dapat dimanfaatkan untuk mendeteksi dan menganalisis serangan jaringan, termasuk serangan *DDoS*, serangan *phishing*, dan sejenisnya. Program ini juga dapat digunakan untuk memantau kinerja jaringan dan memberikan bantuan dalam penanganan masalah jaringan yang terjadi. (Jaya et al., 2022).

2.3.1 *Kali Linux*

Kali Linux merupakan distribusi Linux tingkat lanjut yang dikhususkan untuk Penetration *Testing* dan audit keamanan. Distribusi ini merupakan penyempurnaan dari *BackTrack Linux*, dibangun secara menyeluruh dengan mematuhi standar pengembangan Debian (Dayan et al., 2023).

Adapun Tujuan Utamanya sebagai berikut:

1. Keamanan dan Penetrasi

Kali Linux dirancang untuk mendukung profesional keamanan informasi dalam menjalankan pengujian penetrasi dan mengevaluasi keamanan sistem.

2. Berbasis Debian

Kali Linux memiliki dasar distribusi Debian yang populer, memberikan stabilitas dan dukungan komunitas yang luas.

3. Tools Keamanan Terintegrasi

Dengan menyediakan berbagai alat keamanan terintegrasi seperti *Metasploit, Wireshark, Nmap, Burp Suite,* dan sejumlah lainnya, Kali Linux menjadi sarana penilaian keamanan dan pengujian penetrasi yang efektif.

4. Penggunaan *Ethical Hacking*

Dalam praktik *ethical hacking* atau penilaian keamanan yang sah, *Kali Linux* sering digunakan oleh profesional keamanan untuk mengidentifikasi dan memperbaiki celah keamanan dalam sistem atau jaringan.

5. Forensik Digital

Kali Linux juga digunakan untuk keperluan forensik digital, yaitu proses pengumpulan, analisis, dan pemulihan bukti digital dalam konteks penyelidikan keamanan.

Penggunaan *Kali Linux* harus dilakukan dengan itikad baik, hanya untuk tujuan yang legal dan etis. Penetrasi dan uji penetrasi hanya boleh dilakukan dengan izin penuh dan kepemilikan dari pemilik sistem atau jaringan yang diuji.

2.3.1 *Wireshark*

Wireshark merupakan sebuah software yang melakukan tugas menganalisis jaringan dan memonitor paket data yang dikirim dari jaringan. Aplikasi ini memungkinkan pengguna untuk menangkap dan menganalisis paket data dari berbagai protokol jaringan, termasuk TCP/IP, HTTP, DNS, dan metode lainnya. (Jaya et al., 2022).

Salah satu alat yang dapat digunakan adalah Wireshark, karena dalam Wireshark, kita dapat merekam dan menampilkan berbagai informasi yang berkaitan dengan proses keluar-masuknya data dalam jaringan komputer.

Wireshark mampu merekam informasi forensik, seperti daftar alamat IP yang mencoba masuk, beserta tindakan-tindakan yang dilakukan oleh setiap alamat IP tersebut.(Choiruman et al., 2022).

Peralatan pengukuran yang akan dipakai dalam penelitian ini mencakup:

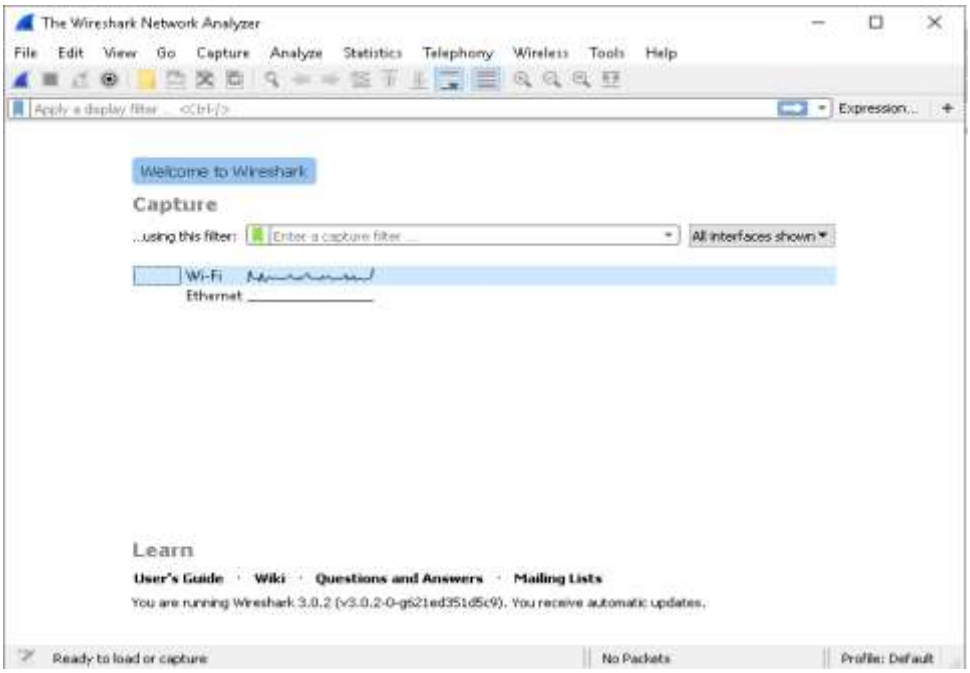
1. Ketersediaan perangkat keras dan sistem operasi.

    a. Laptop HP EliteBook 840 G3 dengan prosesor i5 2,6 GHz, RAM 8 GB, SSD 256 GB.

    b. Sistem operasi Windows 10 Pro

2. Kebutuhan Perangkat lunak

    a. Sofware *Wireshark veri 3.0.2 64 bit*



Gambar 2. 13 *Wireshark versi 3.0.2*

2.4 Penelitian Terdahulu

1. Nama : MT Hidayat,FM SN,NI kurniati

Judul : ”ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (*WIFI*) GRATIS TERHADAP SERANGAN PAKET *SNIFFING* ”

ISSN/ISBN : 112-119.

Vol/No/Tahun : I/2/2018

“Universitas Siliwangi (UINSIL) telah mengimplementasikan jaringan komputer baik kabel maupun nirkabel untuk pertukaran layanan publik, kegiatan kemahasiswaan, personalia dan informasi penting lainnya. Jaringan ini tersebar di beberapa situs UINSIL, antara lain *server* pusat di ruang kendali TIK yang terhubung dengan seluruh fakultas, perpustakaan, pusat perkantoran dan lain-lain. Fasilitas jaringan meliputi studi sarjana, fakultas, perpustakaan, LPPM yang menggunakan kabel dan disediakan banyak access point nirkabel di seluruh area UINSIL tanpa *password*. Oleh karena itu dilakukan analisis keamanan jaringan dan pemahaman keamanan informasi pengguna komputer di berbagai lokasi di Universitas Siliwangi. Penelitian ini menggunakan pendekatan model tindakan dengan tahapan diagnosis, perencanaan tindakan, intervensi, evaluasi dan refleksi. Atas permintaan peneliti, informasi korban sasaran dan hasil pengumpulan data memungkinkan akses terhadap foto, nama pengguna dan kata sandi korban serta informasi lainnya sesuai dengan keamanan komputer korban. Keamanan jaringan dan komputer korban juga dinilai.”

2. Nama : MD Sanjaya

Judul : “ ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET(*WIFI*) TERHADAP SERANGAN PACKET *SNIFFING* PADA KANTOR INDOSAT OOREDOO “

ISSN/ISBN : -

Vol/No/Tahun : XIII/12/2019

Masalah yang dijelaskan dalam latar belakang tersebut adalah perlunya pengawasan terhadap bahaya jaringan komputer kantor dan umum di Kantor Indosat Ooredoo Pekanbaru. Simulasi menggunakan model topologi jaringan internal di kantor tersebut, dengan penggunaan *WiFi* yang tidak memisahkan antara kantor dan umum. Hal ini menyebabkan potensi bahaya pada jaringan *WiFi* terkait penyadapan data. Hasil penelitian menunjukkan bahwa Packet *Sniffing* dapat merekam dan menampilkan *username* dan *password* target dengan Wireshark. Tujuan dari penelitian ini adalah untuk memastikan bahwa kantor PT Indosat Ooredoo Pekanbaru menyadari risiko yang terkait dengan penggunaan *WiFi* nirkabel di jaringan yang sama dengan pengguna biasa.

3. Nama : RIZKYANI

Judul : ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET(*WIFI*) TERHADAP SERANGAN PACKET *SNIFFING* DI KANTOR KORAN SERUYA”

ISSN/ISBN : 119-124.

Vol/No/Tahun : IV/02/2019

“Tujuan dari penelitian ini adalah untuk menganalisis log dan memeriksa keamanan jaringan di surat kabar Seruiya. Metode yang digunakan adalah

pendekatan deskriptif, dimana data dianalisis tidak berubah selama penelitian dilakukan di kantor surat kabar Seruiya. Hasil analisis keamanan jaringan *Wi-Fi* serangan paket surat kabar Seruiya dapat diambil. Kajian tersebut mencakup skrining dan tindakan preventif. Kelemahan utama jaringan *WiFi* kantor Koran Seruiya terdapat pada Network Layer dan Application Layer karena penggunaan satu Access Point yang cakupannya tidak efisien untuk perusahaan besar. Selain itu, pada Application Layer, keamanan dan lalu lintas jaringan tidak efisien pada *WiFi* Kantor Koran Seruiya".

4. Nama : Turkhamun Adi Kurniawan

   Judul : "ANALISA KEAMANAN JARINGAN *WIFI* TERHADAP SERANGAN PACKET *SNIFFING* "

   ISSN/ISBN : 16.2: 11

   Vol/No/Tahun : II/09/2020

" Studi ini mengevaluasi keamanan PT dari jaringan *Wi-Fi* perusahaan. XYZ terhadap serangan packet *sniffing* menggunakan IDS. Melalui perancangan sistem dan konfigurasi aplikasi Wireshark, penelitian ini menentukan aturan untuk mendeteksi serangan packet *sniffing*, khususnya serangan spoofing ARP. Hasilnya menunjukkan bahwa jaringan *Wi-Fi* yang tidak terlindungi dapat membahayakan keamanan data pengguna karyawan khususnya, seperti penyimpanan nama pengguna dan kata sandi. Oleh karena itu, peningkatan keamanan yang efektif diperlukan untuk mencegah dan mengalahkan serangan packet *sniffing* dan ancaman lainnya di jaringan PT *Wi-Fi* dan *LAN* kabel. XYZ."

5. Nama : SUNDARI, S.

Judul : ” ANALISIS KEAMANAN JARINGAN KOMPUTER PADA FASILITAS WIRELESS FIDELITY (*WIFI*) TERHADAP SERANGAN PAKET *SNIFFING* DI SENTRAL YAMAHA”

ISSN/ISBN : 203-208

Vol/No/Tahun : III/2/ 2021

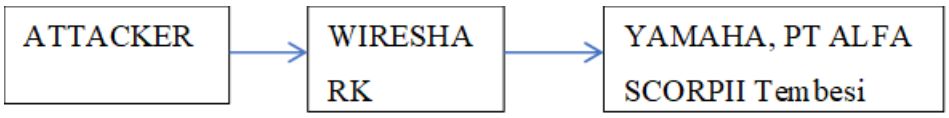
"Pertumbuhan teknologi informasi, termasuk dalam pengembangan jaringan komputer, menimbulkan tantangan keamanan yang signifikan, sebagaimana disampaikan oleh Suindari. Jaringan komputer pertama kali muncul di Amerika pada tahun 1940 dalam proyek pengembangan komputer Model I oleh kelompok riset Bell Laboratory dan Universitas Harvard di bawah pimpinan Profesor Howard Aiken (Riska et al., 2018). Perkembangan jaringan komputer terus pesat seiring dengan evolusi perangkat keras dan perangkat lunak. Pengembangan ini melibatkan integrasi jaringan komputer dengan Internet of Things (Crnjac dan Bandurka, dalam Agni, Krismadinata, 2018). Pada abad ke-21, teknologi jaringan komputer dapat mencakup seluruh dunia dengan menghubungkan komputer dan *server* melalui jaringan area lokal hingga jaringan area luas yang semakin mudah (Syafrizal, 2020).

Pemerintah Republik Indonesia telah mengeluarkan kebijakan keamanan data melalui peraturan seperti UU No. 11/2008 tentang Informasi dan Transaksi Elektronik, yang diubah dengan UU No. 19 Tahun 2016. Kebijakan ini bertujuan untuk menjamin keamanan informasi dengan menjaga infrastruktur komunikasi dan memberikan peraturan perlindungan terhadap ancaman keamanan informasi. Keamanan internet, terutama dalam penggunaan jaringan area lokal nirkabel

(W*LAN*), menjadi sangat krusial saat ini. Jaringan yang terhubung ke internet secara mendasar rentan dan dapat dieksploitasi oleh peretas (Rizal, 2018). Ancaman keamanan mendasar tersebut dapat dieksploitasi pada jaringan area lokal (*LAN*) maupun jaringan area lokal nirkabel. Pengguna fasilitas base station juga berhadapan dengan ancaman serangan Packet *Sniffing* (Ariyanto, 2018).

Packet *Sniffing* merupakan bentuk kejahatan siber di mana pelaku secara sengaja atau tidak sengaja mencuri nama pengguna dan kata sandi orang lain. Akun yang berhasil dicuri dapat disalahgunakan untuk merusak atau menghapus informasi milik korban (Noveinzo, Mas*LAN*, 2020). Penelitian ini menyoroti serangan Packet *Sniffing* dengan menggunakan alat seperti Ettercap. Ettercap berfungsi sebagai Packet *Sniffer* yang mampu menganalisis protokol jaringan, menangkap lalu lintas di *LAN*, mencuri kata sandi, dan melakukan penyadapan aktif menggunakan berbagai protokol. Serangan Packet *Sniffing* dapat disalahgunakan oleh pihak yang tidak bertanggung jawab untuk mencuri informasi sensitif pengguna terkait base station. Penelitian ini menggunakan alat internal, yaitu alat peretas *WiFi*, untuk mendeteksi sinyal nirkabel yang terhubung dan menyusup ke dalam jaringan. Yamaha Palopo, dealer di Sulawesi Selatan, menggunakan jaringan nirkabel untuk komunikasi dan layanan umum. Komputer *server* di Yamaha Palopo mengatur lalu lintas transfer data atau file yang diminta atau dikirim oleh komputer klien. Oleh karena itu, risiko keamanan, terutama terkait dengan serangan Packet *Sniffing*, perlu mendapat perhatian guna melindungi informasi penting pengguna jaringan."

2.5 Kerangka Pemikiran



Gambar 2. 14 *Kerangka Pemikiran*

Agar dapat memahami kerangka pemikiran berikut penjelasan dari kerangka pemikiran :

1. Penyerang (Attacker):

Menyiapkan alat dan bahan untuk memantau pergerakan data mencurigakan.

Penyerang berupaya mendapatkan akses atau kontrol tidak sah ke dalam sistem atau jaringan komputer, data, atau sumber daya digital lainnya.

2. Wireshark

Tools yang digunakan peneliti untuk menganalisis jaringan *WiFi* pada YAMAHA, PT ALFA SCORPII Tembesi

3. Yamaha, PT Alfa Scorpii Tembesi:

Peneliti menyimpulkan dan menjelaskan asal timbulnya serangan hingga solusi untuk menyelesaikan masalah tersebut.

Kerangka pemikiran ini mencakup persiapan penyerangan, alat analisis (Wireshark), serta obyek penelitian (Yamaha, PT Alfa Scorpii Tembesi) dengan kesimpulan dan solusi terkait serangan yang terjadi.

.