BAB 2
LANDASAN TEORI

2.1 Jaringan Komputer

Jaringan Komputer merupakan infrastruktur telekomunikasi yang memfasilitasi komunikasi dan pertukaran data antara komputer-komputer yang terhubung. Jaringan ini terdiri dari perangkat keras dan perangkat lunak yang bekerja sama. Ketika dua atau lebih komputer berinteraksi dan berbagi data, terdapat dua peran utama: client yang meminta layanan dan server yang memberikan layanan. Model ini dikenal sebagai Sistem *Client-Server*.[3]

Terdapat beberapa klasifikasi jaringan komputer berdasarkan cakupan area, yang sering kita jumpai. Sebagai berikut :

2.1.1 LAN (Local Area Network)

Local Area Network adalah suatu sistem yang menghubungkan perangkat-perangkat jaringan dalam jarak yang relatif dekat, seringkali digunakan di gedung-gedung seperti sekolah, kantor, atau rumah. LAN sering kali menggunakan jenis konektivitas tertentu, seperti Ethernet dan Token Ring. Selain itu, terdapat juga LAN yang menggunakan teknologi nirkabel, yang dikenal sebagai *Wireless Local Area Network* (WLAN) dan menggunakan *Wi-fi* sebagai media transmisi.

Jaringan LAN memungkinkan pengguna untuk berbagi sumber daya seperti printer, file, dan koneksi internet, serta untuk melakukan komunikasi antar perangkat dengan cepat dan efisien. Dengan adanya LAN, pengguna dapat bekerja secara kolaboratif, mengakses informasi yang sama, dan menggunakan layanan yang tersedia di jaringan dengan mudah.

Meskipun cakupan jaringan LAN terbatas dalam jarak, namun ia memiliki kecepatan transfer data yang tinggi dan relatif stabil. Ini membuatnya menjadi pilihan yang ideal untuk lingkungan lokal yang memerlukan komunikasi yang cepat dan efisien antar perangkat.

2.1.2 MAN (Metropolitan Network)

Metropolitan Area Network adalah sebuah konsep yang menghubungkan perangkat jaringan dari satu kota ke kota lainnya, memungkinkan pertukaran data antar lokasi yang berbeda dalam suatu wilayah metropolitan. Ketika jaringan LAN tidak lagi cukup untuk mencakup area yang dibutuhkan, MAN menjadi solusi yang tepat. MAN memiliki cakupan yang lebih besar daripada LAN, sehingga membutuhkan penggunaan perangkat khusus dan keterlibatan operator telekomunikasi yang berperan sebagai penghubung antar jaringan komputer di berbagai lokasi. Dengan demikian, MAN memungkinkan organisasi atau komunitas yang berada di wilayah metropolitan untuk terhubung dan berkomunikasi secara efisien, meskipun berada di lokasi yang berbeda.

2.1.3 WAN (Wide Area Network)

Wide Area Network adalah sistem jaringan yang menghubungkan komputer yang berada pada jarak geografis yang jauh satu sama lain. Jaringan global ini menghubungkan berbagai jaringan lokal. WAN mencakup wilayah geografis yang luas, termasuk jaringan lokal dan infrastruktur telekomunikasi lainnya. Dalam perkembangan saat ini, karena kebutuhan untuk menghubungkan pengguna dari berbagai kota dan negara bagian semakin meningkat, LAN secara bertahap berkembang menjadi jaringan yang lebih luas (WAN), yang dapat mencakup jumlah komputer yang bervariasi, mulai dari puluhan hingga ribuan.

2.1.4 Jaringan WLAN (Wireless Local Area Network)

Jaringan *Wireless Local Area Network* (WLAN) menggunakan frekuensi radio dan inframerah sebagai sarana transmisi data. Istilah "nirkabel" sering kali dipakai sebagai sinonim untuk WLAN. Evolusi komunikasi tanpa kabel ini dimulai dengan pengembangan perangkat berbasis gelombang radio seperti walkie-talkie, remote control, ponsel, dan perangkat radio lainnya. Keinginan untuk memudahkan mobilitas komputer

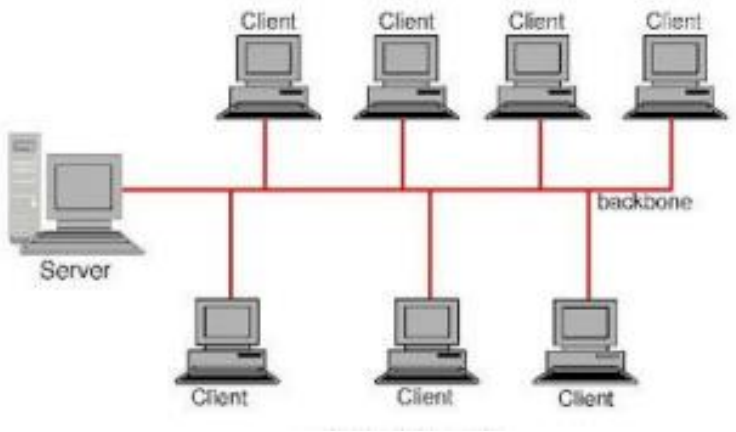
dan integrasi dengan jaringan yang sudah ada mendorong perkembangan teknologi wireless dalam konteks jaringan komputer.

WLAN mirip dengan jaringan LAN, namun setiap perangkat atau node yang terkoneksi menggunakan perangkat nirkabel untuk bertukar data dan informasi. WLAN memiliki dua mode konfigurasi utama: infrastruktur dan Ad-Hoc. Konfigurasi infrastruktur memungkinkan komunikasi antara Personal Computer (PC) melalui sebuah access point dalam jaringan WLAN. Perangkat yang terhubung menggunakan channel frekuensi dan SSID yang sama[9]

2.1.5 Topologi Jaringan

1. Bus

Topologi bus adalah struktur jaringan di mana semua perangkat terhubung ke satu jalur komunikasi utama, disebut bus. Setiap perangkat terhubung langsung ke bus tanpa perangkat tambahan. Data dikirim melalui bus dan dapat diterima oleh semua perangkat, meskipun hanya perangkat tujuan yang memprosesnya. Topologi ini umumnya digunakan dalam jaringan kecil karena kemudahan instalasi dan biayanya yang rendah

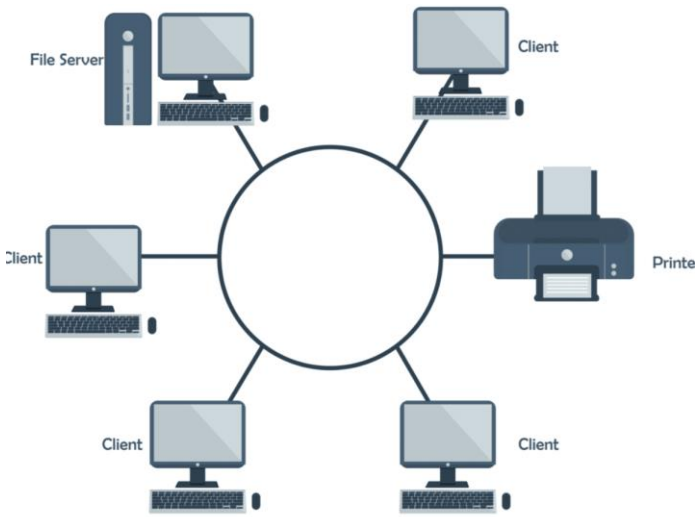


Gambar 2.1 Topologi Bus

2. Ring

Topologi ring adalah susunan di mana setiap perangkat

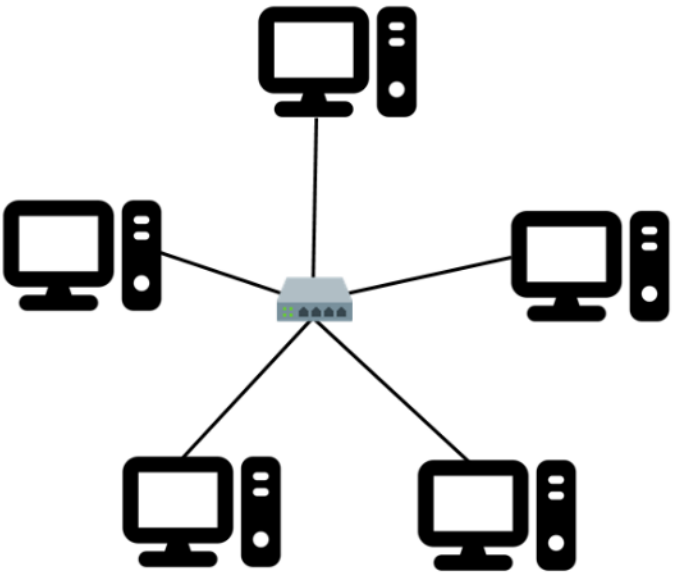
terhubung ke dua perangkat tetangga secara langsung, membentuk lingkaran. Data mengalir dalam satu arah sepanjang cincin, melalui setiap perangkat sebelum mencapai tujuan. Setiap perangkat bertindak sebagai penerima dan pengirim data secara bergantian. Jika satu perangkat mengalami masalah, jaringan bisa terganggu. Topologi ring sering digunakan di jaringan yang memerlukan kinerja stabil, seperti dalam jaringan telepon.



Gambar 2.2 Topologi Star

3. Star

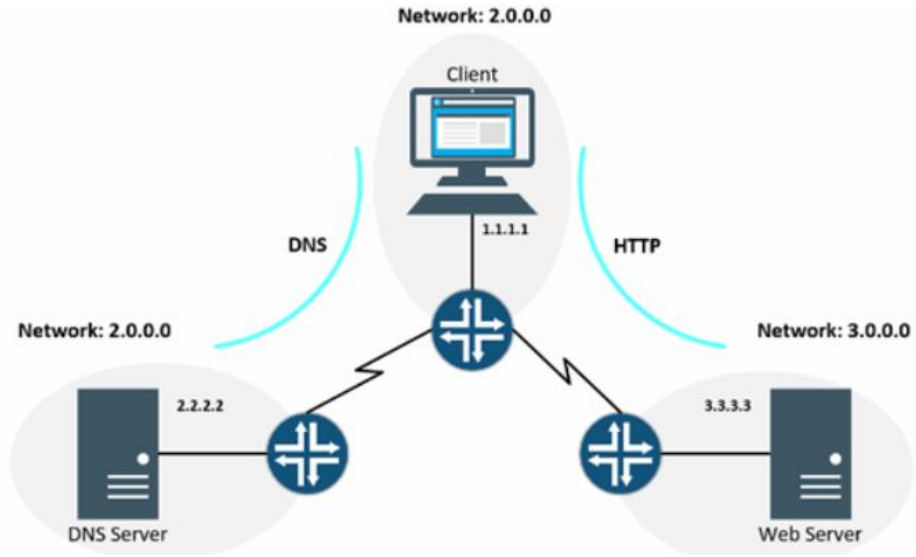
Topologi star adalah susunan jaringan di mana setiap perangkat terhubung ke satu titik pusat, seperti hub atau switch. Semua komunikasi antar perangkat berlangsung melalui titik pusat ini. Setiap perangkat hanya memiliki koneksi langsung ke titik pusat, bukan ke perangkat lainnya. Topologi star umum dalam jaringan komputer karena manajemennya yang mudah, fleksibilitas dalam perubahan, dan kemampuannya untuk membatasi dampak jika satu koneksi mengalami masalah.



Gambar 2.3 Topologi Star

2.1.6 Protokol Jaringan

Protokol jaringan adalah serangkaian aturan yang memfasilitasi komunikasi dan pertukaran data antara dua atau lebih komputer yang terhubung ke jaringan. Aturan-aturan ini mencakup pedoman untuk berbagai aspek jaringan, seperti cara mengakses internet, kecepatan pengiriman data, dan lain-lain. Protokol jaringan berfungsi sebagai alat komunikasi antara komputer dalam suatu jaringan.[4]



Gambar 2.4 Protokol Jaringan

1. TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP (Transmission Control Protocol/Internet Protocol) adalah seperangkat protokol komunikasi yang digunakan untuk mengatur pertukaran data di dalam jaringan komputer. Ini adalah standar dominan yang digunakan di internet dan jaringan lokal (LAN), yang mendasari semua komunikasi data antar perangkat yang terhubung dalam jaringan. Protokol TCP/IP terdiri dari dua komponen utama:

Transmission Control Protocol (TCP): Bertugas untuk memastikan pengiriman data yang andal antara perangkat dalam jaringan. TCP memastikan bahwa data sampai dengan benar, dalam urutan yang benar, dan tidak hilang selama perjalanan antara perangkat.

Internet Protocol (IP): Mengatur pengalamatan dan pengiriman paket data dalam jaringan. IP menetapkan alamat untuk perangkat (dalam bentuk alamat IP) dan mengatur cara data dipaketkan, diarahkan, dan diterima di jaringan.

Kombinasi TCP dan IP membentuk protokol yang sangat efektif untuk mengelola komunikasi data di dalam jaringan. TCP/IP

adalah standar universal yang digunakan oleh berbagai perangkat dan sistem operasi, yang memungkinkan berlangsungnya komunikasi yang mulus dan terintegrasi di seluruh internet dan jaringan lokal.

2. UDP (User Datagram Protocol)

UDP (User Datagram Protocol) adalah protokol komunikasi yang digunakan untuk mentransfer data dalam bentuk paket di dalam jaringan komputer. Berbeda dengan TCP (Transmission Control Protocol) yang menjamin pengiriman data yang handal, UDP tidak terikat dengan koneksi, sehingga tidak ada mekanisme untuk memastikan paket data yang dikirimkan tiba dengan aman atau dalam urutan yang benar.

3. DNS (Domain Name System)

DNS (Domain Name System) adalah sistem yang mengubah nama domain menjadi alamat IP. Ini memungkinkan akses ke situs web dengan menggunakan nama yang mudah diingat. Dengan DNS, pengguna tidak perlu menghafal alamat IP rumit.

DNS berfungsi sebagai direktori yang besar dan terdistribusi di seluruh internet. Ketika Anda memasukkan nama domain ke dalam browser web Anda, DNS bekerja di belakang layar untuk mencari alamat IP yang sesuai dengan nama domain tersebut. Proses ini melibatkan komunikasi antara komputer pengguna, server DNS lokal, dan server DNS di seluruh dunia untuk menemukan alamat IP yang benar.

4. HTTP (Hypertext Transfer Protocol)

HTTP (Hypertext Transfer Protocol) adalah protokol komunikasi yang digunakan untuk mentransfer data di internet. Protokol ini digunakan untuk mengirimkan permintaan dari klien ke server web, dan juga untuk menerima respons dari server kembali ke klien. HTTP adalah dasar dari pengiriman

informasi di World Wide Web. Saat Anda mengetikkan alamat situs web di browser dan menekan enter, browser akan mengirim permintaan HTTP ke server yang meng-host situs web tersebut. Server akan merespons dengan mengirim kembali data yang diminta, seperti halaman HTML atau gambar, melalui protokol HTTP.

5. **HTTPS (Hypertext Transfer Protocol Secure)**

   HTTPS (Hypertext Transfer Protocol Secure) adalah varian dari HTTP yang lebih aman, yang menggunakan teknologi enkripsi untuk melindungi kerahasiaan data saat ditransfer. Protokol ini digunakan untuk mengamankan komunikasi data sensitif di internet. Saat Anda mengunjungi situs web yang menggunakan HTTPS, interaksi antara peramban Anda dan server web dilindungi dengan enkripsi SSL/TLS (Secure Sockets Layer/Transport Layer Security).

6. **SSL**

   SSL (Secure Socket Layer) adalah salah satu protokol enkripsi yang paling umum digunakan di internet. SSL tidak hanya digunakan untuk mengamankan koneksi web, tetapi juga digunakan dalam berbagai aplikasi yang membutuhkan enkripsi jaringan.

7. **FTP (File Transfer Protocol)**

   FTP (File Transfer Protocol) adalah protokol yang digunakan untuk mengirim dan menerima file antara komputer melalui jaringan. Dengan FTP, pengguna dapat mengunggah dan mengunduh file dari atau ke server melalui internet.

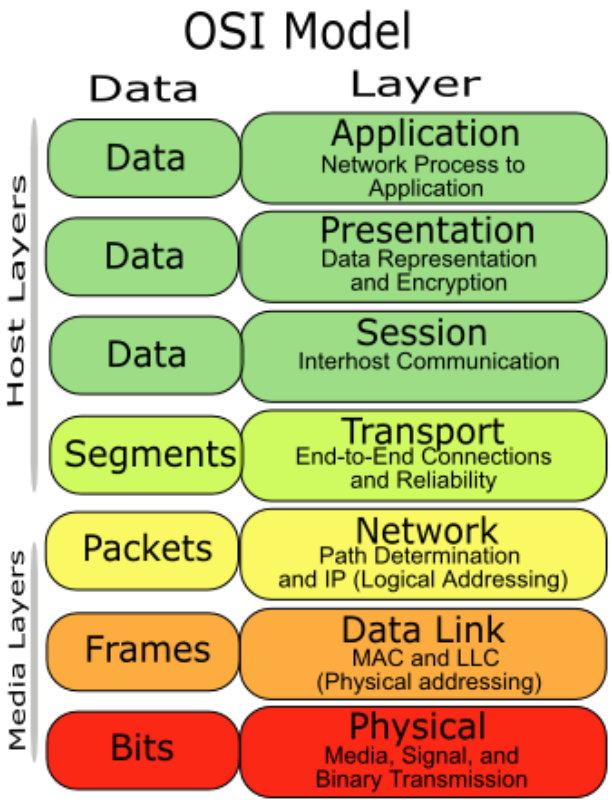
8. **DHCP (Dynamic Host Configuration Protocol)**

   DHCP (Dynamic Host Configuration Protocol) adalah protokol jaringan yang secara otomatis menetapkan alamat IP kepada perangkat dalam jaringan. Protokol ini memungkinkan perangkat untuk mendapatkan konfigurasi jaringan secara

dinamis tanpa memerlukan pengaturan manual. Ini mempermudah manajemen jaringan dengan efisien mendistribusikan alamat IP kepada perangkat yang terhubung.

2.2. OSI Layer

Model OSI (Open Systems Interconnection) adalah kerangka kerja referensi yang digunakan untuk memahami komunikasi dalam jaringan komputer secara umum. Selain itu, model OSI juga dapat berfungsi sebagai panduan untuk mengimplementasikan langkah-langkah keamanan dalam jaringan[8]. OSI Layer terdiri atas lapisan berjumlah 7 buah yaitu : *Physical Layer , Data Link Layer , Network Layer, Transport Layer, Session Layer, Presentation Layer , Application Layer.*



Gambar 2.5 OSI Layer

1. Physical Layer

   Physical layer adalah lapisan pertama atau terbawah dalam model OSI. Lapisan ini bertanggung jawab untuk transfer data

yang terkait dengan media transmisi itu sendiri. Pada sistem komunikasi data nirkabel, lapisan ini berperan sebagai penghubung utama. Kelemahan pada lapisan ini dapat dimanfaatkan melalui serangan seperti evil maid pada laptop atau jaringan, di mana perangkat keras pada physical layer dimanipulasi, seperti pemasangan keylogger atau perangkat lunak berbahaya pada BIOS atau bootloader, serta serangan wiretapping dengan memasang perangkat penyadap pada kabel jaringan untuk merekam komunikasi yang dilakukan oleh peretas yang memiliki akses fisik ke jaringan.

2. Data Link Layer

   Data Link layer bertugas untuk mendeteksi dan memperbaiki kesalahan selama proses transmisi data serta mengatur struktur data ke dalam frame-frame yang lebih kecil. Kelemahan pada lapisan ini dapat dieksploitasi melalui serangan yang menargetkan protocol Address Resolution Protocol (ARP), yang memungkinkan peretas untuk memanipulasi tabel ARP dalam jaringan. Hal ini dapat mengakibatkan pengiriman data ke alamat MAC yang salah.

3. Network Layer

   Network layer bertugas untuk menentukan jalur komunikasi yang digunakan untuk mentransfer data antara perangkat dalam jaringan. Lapisan ini menggunakan alamat seperti IP untuk mengidentifikasi setiap perangkat dalam jaringan dan mendukung proses routing data. Kelemahan pada lapisan ini dapat dimanfaatkan dalam serangan DDoS yang dapat mengakibatkan lumpuhnya jaringan DNS. Hal ini dapat menyebabkan tidak dapat diaksesnya sejumlah situs web yang diakses oleh pengguna karena gangguan pada akses internet.

4. Transport Layer

   Transport layer bertugas untuk mengatur pengiriman data

antara dua atau lebih host dalam jaringan. Lapisan ini juga bertanggung jawab atas pemecahan dan penggabungan pesan, serta mengelola kehandalan dan keselamatan dari jalur koneksi yang disediakan. Contoh protokol yang umum digunakan di transport layer adalah TCP. Kelemahan pada lapisan ini dapat dieksploitasi melalui serangan seperti Heartbleed, yang memanfaatkan kerentanan pada OpenSSL yang digunakan dalam lapisan ini. Serangan ini memungkinkan peretas untuk mengakses informasi sensitif seperti kata sandi dan data pengguna pada berbagai situs web yang menggunakan OpenSSL.

5. Session Layer

   Session Layer bertugas untuk mengatur dan mengontrol dialog sesi, termasuk pembukaan, pengelolaan, dan penutupan koneksi antar komputer. Kelemahan yang mungkin terjadi pada layer ini dalam konteks jaringan kabel dan nirkabel adalah "akses tidak sah" ke jaringan. Penyerang dapat memanfaatkan port hub/switch yang tidak aman untuk menghubungkan perangkat mereka ke jaringan, memungkinkan mereka untuk memata-matai atau bahkan memanipulasi data yang dipertukarkan antar aplikasi.

6. Presentaion Layer

   Presentation Layer bertugas untuk menetapkan sintaks yang digunakan oleh host dalam komunikasi jaringan. Kelemahan pada lapisan ini dapat dieksploitasi melalui serangan seperti Heartbleed pada OpenSSL, yang memanfaatkan kerentanan pada protokol enkripsi OpenSSL untuk mengakses memori server dan mencuri informasi rahasia seperti kunci enkripsi.

7. Application Layer

   Application Layer adalah lapisan paling atas dalam model OSI yang mengatur antarmuka antara protokol jaringan dan aplikasi yang berjalan di komputer. Kelemahan pada lapisan ini dapat dimanfaatkan dengan menggunakan alat seperti SolarWinds

untuk serangan siber, di mana peretas mengeksploitasi kerentanan pada perangkat lunak Orion yang digunakan untuk manajemen jaringan. Serangan ini dapat berhasil memasukkan malware ke dalam sistem yang terinfeksi melalui kerentanan pada perangkat lunak tersebut.

2.1 Keamanan Sistem Informasi

Teknologi yang terus berkembang dengan cepat di era modern membuat informasi menjadi lebih mudah diakses. Namun, keamanan juga menjadi hal yang penting, tidak hanya untuk memastikan keandalan informasi, tetapi juga untuk melindungi data dari akses yang tidak sah. Konsep keamanan dalam teknologi informasi dikenal dengan istilah CIA Triad, yang memiliki tiga prinsip utama sebagai berikut, Kerahasiaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability) [5]. Tiga prinsip mempunyai hubungan yang erat antara satu dengan yang lain sehingga membentuk sebuah segitiga.

Gambar 2.6 CIA Triad

1. **Confidentiality**

   Aspek Kerahasiaan, atau Confidentiality, bertujuan untuk mencegah akses yang tidak sah terhadap informasi sensitif, sementara memastikan bahwa pihak yang berhak memiliki akses penuh. Ini melibatkan pembatasan akses hanya kepada individu yang diotorisasi untuk melihat data yang bersangkutan. Selain itu, sering kali data diklasifikasikan berdasarkan potensi kerusakan yang dapat terjadi jika jatuh ke tangan yang tidak diinginkan.

2. **Integrity**

   Aspek Integritas, atau Integrity menekankan bahwa data atau informasi tidak boleh dimodifikasi tanpa persetujuan dari pemiliknya. Data yang diterima harus tetap konsisten dengan data yang dikirimkan. Jika ada perubahan antara data yang dikirimkan dan yang diterima, maka prinsip integritas tidak terpenuhi. Salah satu contoh masalah yang harus diatasi adalah spoofing, di mana pihak lain memodifikasi data tanpa izin.

3. Availability

Aspek ketersediaan, atau Availability berkaitan dengan ketersediaan informasi dan data. Informasi dan data yang ada dalam sistem jaringan komputer tersedia dan dapat diakses oleh pengguna yang berwenang. Ketersediaan ini menyangkut kemampuan untuk mengakses data atau informasi saat dibutuhkan.

2.2 Jenis Jenis Ancaman Keamanan Jaringan

Berikut jenis jenis ancaman keamanan jaringan :

Tabel 2.1 Ancaman Keamanan Jaringan

No	Ancaman	Keterangan
1	Packet Sniffer	Packet Sniffer atau yang sering disebut mengendus paket adalah aktivitas untuk menangkap paket-paket data yang mengalir dalam sebuah jaringan. Sniffing digunakan untuk mendapatkan informasi penting seperti kata sandi, email, teks, dan transfer file dari jaringan tersebut. Sniffer umumnya menargetkan protokol seperti Telnet, HTTP, POP, IMAP, SMB, FTP, dan lainnya. Dalam konteks hacking, sniffing dibagi menjadi dua jenis: passive sniffing dan active sniffing. Menghadapi gangguan ini cukup sulit karena nature dari packet sniffing yang bersifat pasif (penyerang hanya mendengarkan tanpa melakukan tindakan aktif)[10]
2	*Arp Spoofing / Arp Poisoning*	Address Resolution Protocol (ARP) adalah protokol dalam suite TCP/IP yang beroperasi di lapisan jaringan (network layer) dan lapisan data link (data link layer). Protokol ini bertanggung jawab untuk memetakan atau menyesuaikan alamat IP ke alamat media access control (MAC Address) dan hasilnya

		disimpan dalam ARP cache. ARP spoofing adalah teknik serangan di mana penyerang mencoba untuk memata-matai komunikasi antara dua mesin yang sedang berkomunikasi, yang dikenal sebagai serangan Man-in-The-Middle (MITM). Prinsip serangan ARP poisoning ini memanfaatkan kelemahan dalam teknologi jaringan komputer yang menggunakan ARP broadcast. ARP beroperasi pada layer 2, di mana alamat yang digunakan adalah MAC address. Sebagai contoh, ketika sebuah host (misalnya Personal Computer) yang terhubung dalam sebuah LAN ingin berkomunikasi dengan host lain dalam LAN tersebut, host tersebut membutuhkan informasi MAC address dari host tujuan
3	*Scan*	Scanning adalah proses pengujian yang dilakukan dalam skala besar dan otomatis menggunakan alat-alat khusus. Alat-alat ini dapat secara otomatis mengidentifikasi port-port yang terbuka pada host lokal maupun host remote, menemukan alamat IP yang aktif, dan bahkan dapat digunakan untuk mendeteksi sistem operasi yang digunakan oleh host yang disasarkan.
4	*Denial Of Service (DOS)*	Denial of Service (DoS) adalah jenis serangan di mana penyerang berupaya untuk menghabiskan sumber daya jaringan komputer. Akibat dari serangan DoS ini adalah sistem komputer tidak dapat berfungsi dengan normal. Sumber daya jaringan yang berharga seperti komputer, database, dan layanan yang disediakan oleh organisasi

		menjadi tidak dapat diakses oleh pengguna jaringan, yang seringkali memanfaatkannya untuk meningkatkan efisiensi kerja mereka. Ketika layanan-layanan ini tidak tersedia karena berbagai alasan, hal ini tentu saja dapat mengakibatkan penurunan produktivitas. Beberapa contoh penyebab serangan denial of service meliputi: a. Jaringan menjadi tidak berfungsi karena terlalu banyaknya lalu lintas data (traffic). b. Infeksi virus yang menyebar dan mengakibatkan sistem komputer melambat atau bahkan tidak berfungsi sama sekali. c. Perangkat yang melindungi jaringan mengalami kerusakan atau tidak berfungsi dengan baik.
5	*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 medapatkan semua informasi yang di transmisikan oleh target.

2.3 VAPT

VAPT, singkatan dari Vulnerability Assessment and Penetration Testing, adalah metode yang digunakan untuk mengevaluasi keamanan sistem informasi dengan mengidentifikasi dan menilai kerentanan yang mungkin ada, serta melakukan uji penetrasi untuk menentukan tingkat kerentanan sistem terhadap serangan oleh pihak yang tidak sah. VAPT terdiri dari dua makna yaitu Vulnerability Assessment dan Penetration Testing.[2]

Gambar 2.7 Metode VAPT

Vulnerability Assesstment adalah suatu proses sistematis yang digunakan untuk mengidentifikasi, mengevaluasi, dan mengukur kerentanan dalam sistem komputer atau jaringan. Tujuannya adalah untuk menemukan titik lemah yang mungkin dieksploitasi oleh pihak yang tidak berwenang, dengan melakukan pemeriksaan menyeluruh terhadap perangkat lunak, konfigurasi, dan infrastruktur jaringan. Hasil dari proses ini dapat digunakan untuk menyusun strategi pengelolaan risiko dengan merekomendasikan langkah-langkah perbaikan yang diperlukan untuk mengurangi risiko terkait dengan kerentanan yang ditemukan.[6]

Penetration Testing adalah suatu proses yang dilakukan untuk mengevaluasi keamanan suatu sistem atau jaringan dengan cara melakukan serangkaian uji coba. Tujuannya adalah untuk menemukan dan mengidentifikasi kerentanan atau kelemahan yang mungkin dimanfaatkan oleh pihak yang tidak berwenang. Dalam proses ini, pengujian dilakukan dengan pendekatan yang mirip dengan serangan yang dilakukan oleh pereta. Hasil dari tes ini digunakan untuk mengevaluasi efektivitas mekanisme pertahanan suatu sistem dan untuk mengidentifikasi area yang memerlukan perbaikan keamanan.[6]

Berikut tahapan dari VAPT :

1. Information Gathering

Information Gathering merupakan tahap awal untuk pengumpulan informasi yang dapat membantu penguji dalam melakukan proses penetration testing

2. Threat Modeling

Threat Modeling merupakan tahap untuk melakukan pemodelan ancaman agar memudahkan penguji menentukan serangan terhadap target

3. Vulnerability Analysis

Vulnerability Analysis merupakan tahap untuk mencari dan menganalisa informasi kerentanan terhadap sistem berdasarkan ancaman yang ditemukan

4. Exploitation

Exploitation merupakan tahap pentetrasi terhadap target yang dilakukan berdasarkan temuan celah yang ditemukan pada tahap sebelumnya

5. Post Exploitation

Post Exploitation merupakan tahap lanjutan dari *exploitation* yang bertujuan untuk menyusun rencanan setelah dilakukannya *exploitation* serta melakukan analisis kerentanan yang paling beresiko.

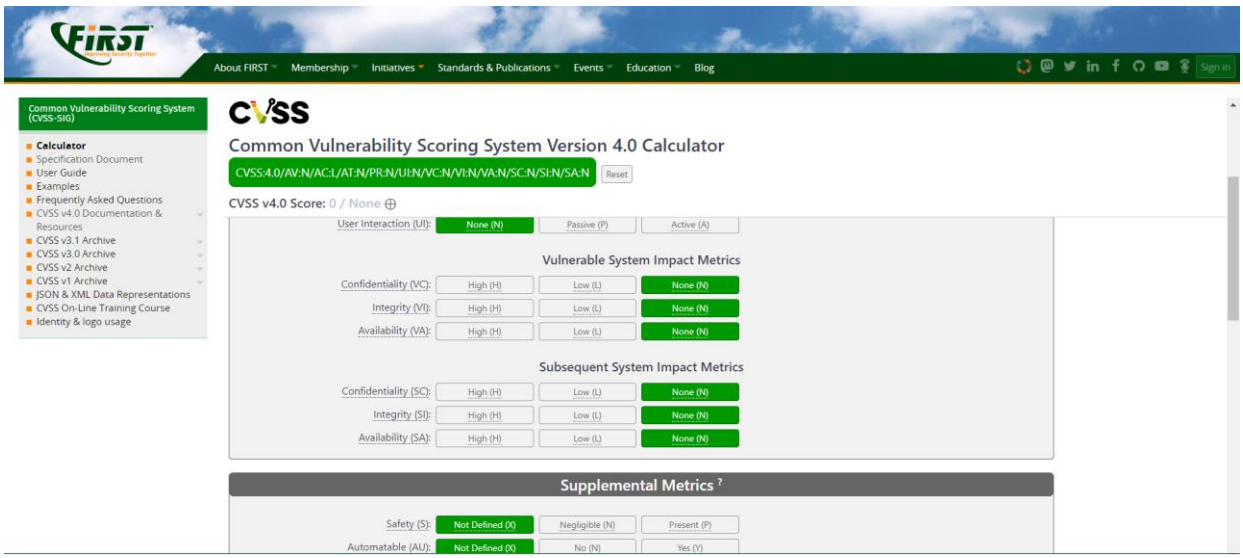
6. Reporting

Reporting merupakan tahap membuat laporan dari hasil uji *penetration testing* dengan melaporkan resiko yang ditemukan dan bagaimana cara penaggulangan resiko pada kerentanan yang ditemukan.

2.4 CVSS (Common Vulnerability Scoring System)

*Common Vulnerability Scoring System (*CVSS) adalah sebuah sistem terbuka yang digunakan untuk menggambarkan sifat dan tingkat kerentanan dalam perangkat lunak. CVSS terdiri dari tiga kategori metrik, yaitu *Base, Temporal*, dan *Environmental*. [7]

The National Vulneribility Database NVD menyediakan penilaian CVSS khusus untuk kerentanan yang diketahui secara publik. Federal Information Processing Standars (FIPS), menggunakan kategori keamanan dari skor CVSS NVD untuk memberikan penilaian dampak yang disesuaikan dengan lingkungan lembaga. Hal ini memungkinkan badan-badan federal untuk mendapatkan informasi yang relevan terkait dampak kerentanan yang disesuaikan dengan konteks lembaga mereka.



Gambar 2.8 CVSS CALCULATOR

Kalkulator CVSS ini di gunakan untuk mengukur seberapa jauh mana tingkat kerentanan pada sebuah sistem untuk kemudian dijadikan acuan untuk rekomendasi perbaikan dan lain sebagainya. Untuk menilai tingkat kerentanan suatu sistem menggunakan kalkulator CVSS, diperlukan beberapa metrik kunci. Metrik-metrik ini akan membantu dalam menentukan seberapa parahnya kerentanan tersebut dan potensi dampaknya. Metrik yang harus dimasukkan ke dalam kalkulator CVSS meliputi:

1. *Base Metrics* (Metrik Dasar)

   Meliputi skor dasar yang mencermikan keparahan kerentanan, eksploitabilitas, dan dampak potensial

2. *Temporal Metrics* (Metrik Temporal)
   Menyediakan penilaian yang berubah seiring waktu terkait dengan kematangan kode eksploitasi, tingkat perbaikan, dan dampak kerahasiaannya
3. *Enviromental Metrics* (Metrik Lingkungan)
   Mengukur potensi dampak tambahan dan distribusi target dari kerentanan dalam linkungan yang spesifik

2.5 Mikrotik

MikroTik adalah sistem operasi dan perangkat lunak yang mengubah komputer menjadi router. PC yang menjalankan MikroTik dilengkapi dengan berbagai fasilitas dan perangkat, baik untuk jaringan kabel maupun nirkabel. MikroTik banyak digunakan oleh ISP, penyedia hotspot, startup, dan pemilik warnet. Dikenal karena stabilitas perangkat keras berbasis PC, MikroTik juga terkenal dengan kontrol kualitas dan fleksibilitas dalam mengelola berbagai jenis data dan proses routing. Selain routing, MikroTik juga dapat digunakan untuk aplikasi seperti manajemen bandwidth, firewall, wireless access point (WiFi), backhaul link, sistem hotspot, server virtual private network (VPN), dan berbagai aplikasi lainnya[11]

Mikrotik Router OS memiliki tingkatan level. Tiap level memiliki kemampuan masing-masing, mulai dari level 3, hingga level 6. Secara singkat, level 3 digunakan untuk router berinterface ethernet, level 4 untuk wireless client atau serial interface, level 5 untuk wireless AP, dan level 6 tidak mempunyai limitasi apapun. Untuk aplikasi hospot, bisa digunakan level 4 (200 user), level 5 (500 user) dan level 6 (unlimited user).

2.6 Bettercap

Bettercap adalah sebuah tool open-source untuk melakukan berbagai manipulasi dan analisa jaringan. Tool ini dirancang untuk membantu penggiat keamanan jaringan dalam melakukan tugas-tugas seperti:

1. Pengintaian dan serangan MITM (Man-in-the-Middle):

Bettercap bisa melakukan scan pada jaringan *WiFi, Bluetooth Low Energy (BLE),* dan kabel. Selain itu, Bettercap bisa melancarkan serangan MITM untuk mencegat dan manipulasi traffic jaringan.

2. Analisa Paket Jaringan: Bettercap bisa menangkap paket jaringan dan menganalisanya untuk mencari informasi penting seperti username dan password.
3. Spoofing : Bettercap bisa melakukan spoofing terhadap protokol jaringan seperti *ARP, DNS, NDP,* dan *DHCPv6* untuk melancarkan serangan MITM.
4. Proxy : Bettercap menyediakan fitur proxy yang bisa beroperasi di level paket, TCP, dan aplikasi HTTP/HTTPS. Proxy ini bisa dikontrol dengan script sehingga fleksibel untuk berbagai kebutuhan.

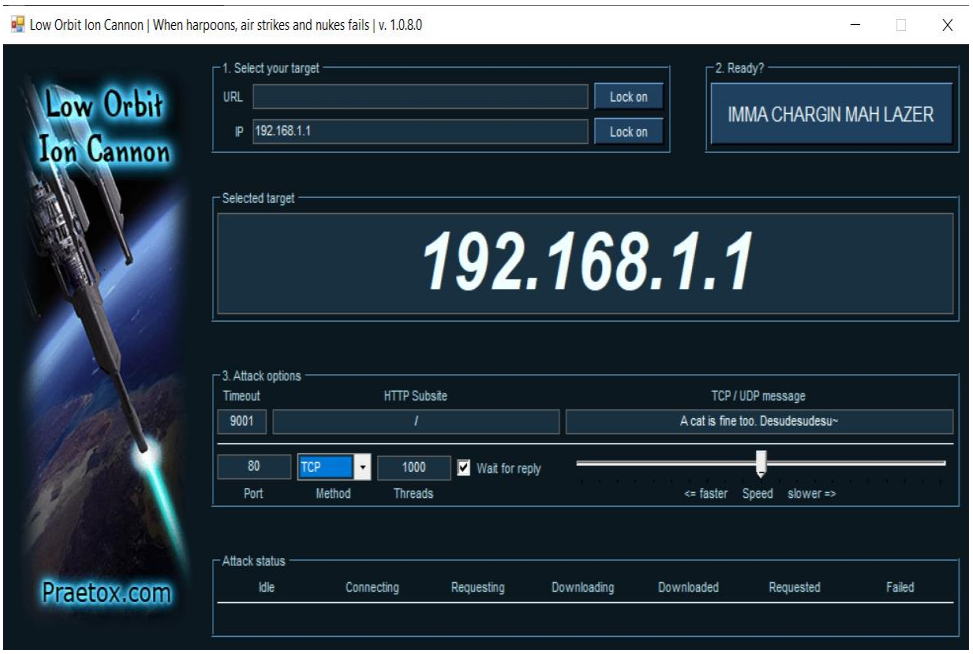
Gambar 2.9 Logo Bettercap

2.7 LOIC *(Low Orbit Ionn Cannon)*

Low Orbit Ion Cannon (LOIC) adalah sebuah alat open-source yang dirancang untuk melakukan serangan Denial-of-Service (DoS) terdistribusi. Serangan DoS bertujuan untuk membuat sebuah layanan atau aplikasi tidak dapat diakses oleh pengguna yang sah. LOIC bekerja dengan mengkoordinasikan banyak komputer untuk mengirim paket HTTP ke

target secara bersamaan. Hal ini dapat membebani server target sehingga tidak dapat menangani permintaan yang sah. LOIC memiliki cara kerja seperti dibawah ini :

1. Pengguna memasukkan alamat IP target dan port yang ingin diserang.
2. LOIC kemudian mengirim pesan broadcast ke jaringan untuk mencari komputer lain yang ingin berpartisipasi dalam serangan.
3. Komputer yang merespon pesan broadcast kemudian bergabung dengan botnet LOIC.
4. LOIC kemudian mengkoordinasikan botnet untuk mengirim paket HTTP ke target secara bersamaan.



Gambar 2.10 Tampilan LOIC