BAB II
LANDASAN TEORI

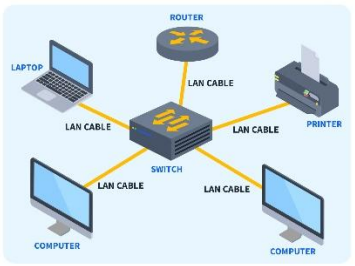
2.1 Jaringan Komputer

Jaringan komputer adalah kumpulan dua atau lebih komputer yang saling terhubung. Jaringan ini memiliki kemampuan untuk berbagi file, termasuk data dan software, serta peralatan jaringan, seperti modem, scanner, dan CDROM. Mereka juga dapat berbagi peralatan jaringan pada berbagai lokasi, seperti email dan tautan ke video konferensi [7].

Dalam istilah awam, jaringan komputer adalah kumpulan beberapa komputer serta perangkat tambahan seperti sakelar, *router*, dan periferal lainnya. Jaringan komputer adalah kumpulan komputer yang saling terhubung [8]. Jika dilihat berdasarkan jarak atau jangkauannya, berbagai jenis jaringan komputer yang ada di dunia termasuk:

1. *Local Area Network* (LAN)

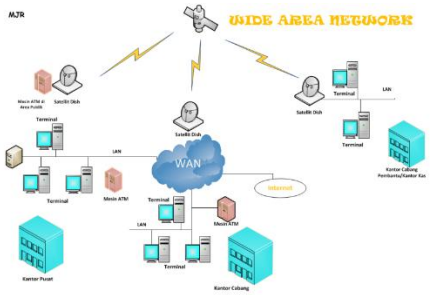
   LAN merupakan jaringan komputer yang mencakup area yang lebih kecil, seperti kampus, kantor, gedung, sekolah, rumah, atau area yang lebih kecil lainnya. Kebanyakan LAN saat ini menggunakan perangkat *switch* yang berbasis pada teknologi IEEE 802.3 Ethernet, yang memiliki kecepatan transfer data 10, 100, atau 1000 Mbit/s. Teknologi 802.11b (juga dikenal sebagai Wi-fi) juga sering digunakan untuk membentuk LAN, dan lokasi yang terhubung ke Wi-fi disebut *hotspot*. Berbeda dengan konsep dump terminal, pada sebuah LAN, setiap *node* atau komputer memiliki daya komputasi sendiri [9].



Gambar 2.1 Jaringan LAN [7]

2. *Wide Area Network* (WAN)

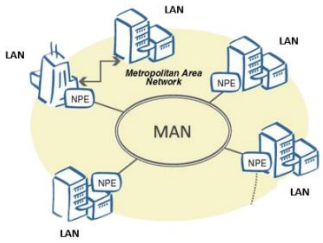
   WAN merupakan jenis jaringan yang memanfaatkan penyedia layanan sebagai titik transit dan menggunakan infrastuktur nirkabel untuk menghubungkan situs yang jauh satu sama lain. Ini mencakup kumpulan LAN atau workgroup yang terhubung melalui alat komunikasi modem dan jaringan internet, serta dari atau ke kantor pusat dan kantor cabang [10].



Gambar 2.11 Jaringan WAN [11]

3. *Metropolitan Area Network* (MAN)

   Metropolitan Area Network merupakan versi LAN dengan area yang lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor perusahaan di sekitarnya atau di kota, dan dapat digunakan untuk keperluan publik atau swasta. MAN memiliki kemampuan untuk mendukung data dan suara, dan bahkan dapat terhubung ke jaringan televisi kabel.



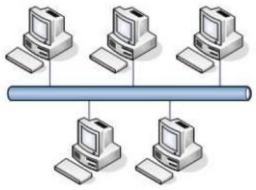
Gambar 2.12 Jaringan MAN [11]

2.2 Topologi Jaringan

Topologi jaringan komputer adalah cara komputer terhubung satu sama lain untuk membentuk jaringan. Jenis topologi yang dipilih dalam sebuah jaringan mempengaruhi kecepatan komunikasi. Oleh karena itu, analisis kelebihan dan

kekurangan setiap topologi didasarkan pada karakteristiknya [12]. Secara umum topologi terbagi menjadi 5 yaitu sebagai berikut:

1. Topologi Bus, adalah topologi jaringan yang menggunakan kabel utama sebagai tulang punggung (*backbone*). Keuntungan dari topologi ini adalah biaya kabel yang rendah, *layout* kabel yang sederhana, dan pengembangannya yang mudah [13].

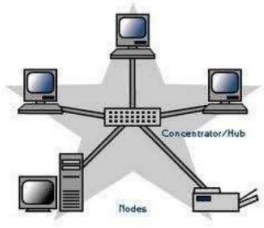


Gambar 2.2 Topologi Bus [14]

2. Topologi Ring, Topologi Ring mirip dengan topologi Bus, dimana Media transmisi mengangkut data atau informasi dari satu komputer ke komputer berikutnya. Topologi ini memiliki kekurangan, yaitu jika salah satu komputer (simpul) mengalami kegagalan, semua hubungan komputer akan terputus [15].

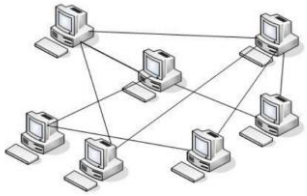
Gambar 2.2 Topologi Ring [14]

3. Topologi Star, Dalam topologi ini, salah satu perangkat digunakan sebagai pusat. Sistem ini memiliki tingkat kerumitan yang lebih tinggi dibandingkan dengan sistem mesh, yang membuat sistem lebih ekonomis. Namun, pusat sistem menanggung beban yang cukup besar, yang meningkatkan kemungkinan kerusakan dan gangguan [16].



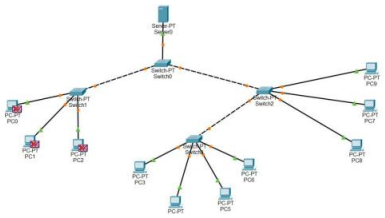
Gambar 2.2 Topologi Star [16]

4. Topologi *Mesh*, jenis topologi di mana setiap unitnya terhubung secara langsung tanpa menggunakan perantara seperti yang terlihat dalam topologi lainnya. Komputer yang rusak tidak akan mempengaruhi komputer yang lain. Dengan demikian, komputer yang rusak hanyalah yang tidak dapat terhubung ke jaringan. Ini adalah karakteristik topologi mesh [17].



Gambar 2.2 Topologi Mesh [14]

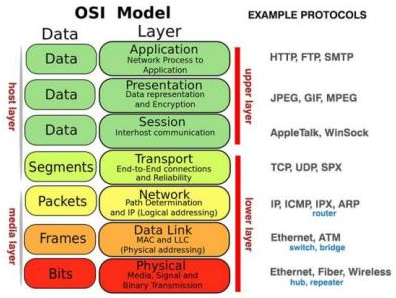
5. Topologi *Tree*, pengembangan atau generalisasi topologi bus. Ini dimulai dari suatu titik yang disebut "*headend*", di mana beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung beberapa terminal dalam bentuk bus atau dicabang lagi hingga menjadi rumit. Media transmisi adalah satu kabel yang bercabang tetapi *e-government* tidak tertutup [14].



Gambar 2.2 Topologi *Tree* [18]

2.3 OSI Layer

Open System Interconnection (OSI) adalah model komunikasi yang digunakan oleh semua jaringan komputer di seluruh dunia. Ini memungkinkan semua perangkat yang berasal dari berbagai pabrikan dan sistem operasi untuk berkomunikasi melalui jaringan [19]. Lapisan *Open Systems Interconnection* (OSI) terdiri dari tujuh lapisan dan dibagi menjadi dua kelompok: lapisan atas dan lapisan bawah, selain itu suatu standar komunikasi yang terdiri dari tujuh lapisan, atau etintas. Ketujuh lapisan ini berbeda satu sama lain dalam fungsinya dalam jaringan. Setiap lapisan bertanggung jawab atas proses komunikasi data [20].



Gambar 2.3 Model Osi Layer [19]

1. *Physical Layer*, bertanggung jawab untuk menentukan media transmisi jaringan; setelah itu, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, dan pemasangan kabel
2. *Data Link Layer*, menentukan bit data yang akan dikelompokkan ke dalam bingkai. Koreksi kesalahan, kontrol aliran, pengalamatan perangkat keras, dan penentuan hubungan antara perangkat jaringan adalah semua tugas lapisan ini.
3. *Network Layer*, bekerja sama dengan lapisan data link. Pada lapisan ini, frame dikirim ke lapisan jaringan, dan kemudian lapisan jaringan pembuat header paket memasukkan IP sipengirim dan sipenerima data.
4. *Transport Layer*, lapisan ini membagi data menjadi paket paket data dan memberi mereka nomor seri sehingga paket-paket ini dapat ditata ulang ketika sampai ke penerima.
5. *Session Layer*, Bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan dijelaskan di lapisan ini.
6. *Presentation layer*, yang merupakan lapisan ke enam, menerjemahkan format data yang ingin dikirimkan aplikasi ke format yang akan dikirimkan melalui koneksi.
7. *Application Layer* aplikasi adalah lapisan yang berhubungan dengan pengguna akhir. Ini mengelola fungsionalitas aplikasi, mengelola pengoperasiannya, dan mengeluarkan pesan salahan ketika terjadi kesalahan [21].

2.4 Keamanan Jaringan

Keamanan jaringan adalah sistem yang mengidentifikasi pengguna yang tidak memiliki hak akses dalam jaringan untuk mencegah aktivitas yang tidak diinginkan. Orang lain dapat mengakses, mengubah, atau menghapus data dalam jaringan setelah komputer terhubung ke komputer lain melalui jaringan kabel atau nirkabel [19]. Keempat komponen utama ancaman keamanan jaringan komputer adalah penyalahgunaan data *Internet of Things* (IoT), serangan penolakan layanan, kerusakan integritas lingkungan jaringan komputer, dan kebocoran data komputer.

Metode berlapis digunakan dalam keamanan jaringan untuk melindungi baik di dalam maupun di luar jaringan. Kerentanan ada di semua hal, dari jalur data dan perangkat hingga aplikasi dan pengguna. Semua bisnis, dari perusahaan kecil hingga perusahaan terbesar, memerlukan keamanan jaringan untuk mencegah serangan yang berkembang pesat yang merusak infrastruktur dan aset penting. Menyesuaikan properti berbagi jaringan pada komputer memungkinkan pengontrolan keamanan jaringan; ini membatasi folder dan file yang hanya dapat dilihat oleh pengguna tertentu, sehingga pengguna yang tidak terdaftar tidak dapat melihat folder atau file tersebut [22].

2.5 *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) adalah proses yang memantau trafik jaringan sistem untuk menemukan pola dan aktivitas yang mencurigakan yang memungkinkan serangan sistem. Ada dua jenis deteksi intrusi: deteksi intrusi berbasis anomaly dan deteksi intrusi berbasis. Karena perkembangan teknologi komputer semakin cepat, kedua metode ini mengalami perubahan. Salah satu keunggulan komputer adalah kemudahan pengoprasian data karena informasi disimpan dalam satu komputer. Salah satu komponen penting dalam teknologi informasi adalah keamanan jaringan komputer, yang melindungi informasi dan data yang dianggap penting oleh suatu lembaga atau Perusahaan [23]. Berikut adalah tiga bentuk Sistem Deteksi Intrusi (IDS):

1. *Network-Intrusion Detection System* (NIDS) berbasis jaringan adalah bagian dari jaringan komputer yang dapat dilihat oleh komputer atau jaringan. Bagian ini dapat digunakan untuk lebih baik mengetahui grafik keluar atau masuk yang dihosting dalam grafik atau segmen antara lokal

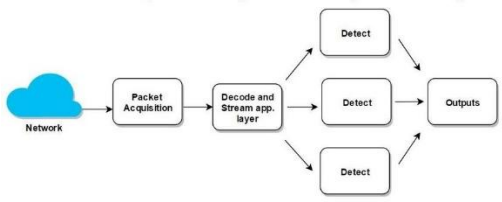
jaringan. Sistem deteksi serangan berbasis jaringan dapat dibangun di belakang atau di depan VPN getways atau firewall untuk mengukur seberapa baik perangkat lunak melindungi jaringan.

2. Aplikasi perangkat lunak khusus yang disebut "sistem deteksi serangan berbasis *host intrusion*" dapat diinstal pada server, yang memungkinkan untuk memantau semua komunikasi keluar atau masuk dari server dan memantau perubahan dalam sistem data.
3. Sistem deteksi intrusi tersebar terdiri dari sensor yang terhubung satu sama lain dan dapat bekerja dengan sensor jarak jauh untuk menyampaikan laporan ke sistem pusat [1].

2.6 Suricata

Suricata, yang dikembangkan oleh Open Information Security Foundation (OISF) pada tahun 2009, adalah mesin pendeteksi ancaman jaringan yang multithreaded, cepat, andal, dan gratis. Deteksi intrusi real-time, pencegahan intrusi inline, pemantauan keamanan jaringan, dan pemrosesan pcap offline adalah semua kemampuan Suricata. Suricata menggunakan aturan untuk memeriksa lalu lintas jaringan dan mendukung skrip Lua yang kuat untuk menemukan ancaman yang kompleks [24].

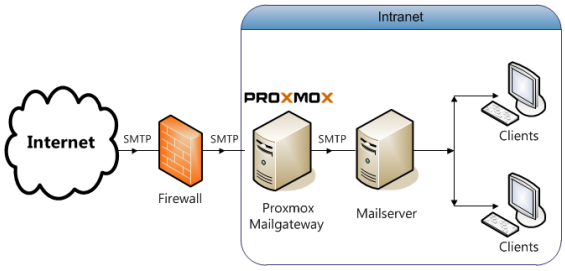
Suricata juga sebuah sistem pendeteksian dan pencegahan intrusi adalah perangkat lunak *open source* yang merupakan generasi berikutnya dari perangkat IDS/IPS yang ada saat ini. Suricata adalah aplikasi IDS/IPS yang berbasis tanda tangan yang mendeteksi serangan atau gangguan melalui metode tanda tangan. Menurut aturan yang dimilikinya, Suricata mengeluarkan peringatan apabila terdapat paket yang dianggap sebagai jenis serangan. Selanjutnya, administrator akan melacak paket serangan untuk menghentikannya [2].



Gambar 2.6.10 Arsitektur Suricata [2]

2.7 Proxmox

Proxmox adalah platform virtualisasi open*source* yang memungkinkan pengoperasian *Virtual Appliance* dan *Virtual Machine*. Proxmox VE adalah distro khusus yang dirancang untuk berfungsi sebagai mesin host virtualisasi sistem dan memiliki dukungan untuk dua teknologi virtualisasi, yaitu KVM dan OpenVZ [25].



Gambar 2.71 Arsitektur Proxmox [26]

Container Virtualization dan *Full Virtualization* digunakan oleh Proxmox VE.

1. *Container Virtualization*, juga dikenal sebagai OpenVZ, adalah teknologi yang direkomendasikan untuk menjalankan server linux karena membuat sejumlah *container* yang aman dan terisolasi (juga dikenal sebagai CT, VE, atau VPS). Setiap *container* beroperasi dan mengeksekusi sama dengan sebuah server terpisah. *Container* dapat di-*reboot* secara mandiri dan memiliki akses super user, alamat IP, memori, proses, file, aplikasi, library sistem, dan konfigurasi unik.
2. KVM adalah solusi virtualisasi penuh untuk *hardware* berbasis x86 yang memiliki ekstensi virtualisasi (Intel VT datau AMDV CPU). Setiap komputer virtual memiliki *hardware* virtual sendiri, seperti kartu jaringan, disk, adapter grafis, dan sebagainya.KVM dan XEN mirip, tetapi KVM adalah bagian dari Linux dan menggunakan sistem jadwal dan manajemen memori standar Linux [26].