BAB II
TINJAUAN PUSTAKA

2. 1 Tinjauan Pustaka

Penelitian yang di lakukan oleh (Bidou, 2014) dengan judul "Konsep dan Implementasi Security Operation Centre", peneliti menjelaskan bahwa Security Operation Centre (SOC) terdiri dari lima modul berbeda: acara generator, pengumpul acara, basis data pesan, mesin analisis, dan reaksi perangkat lunak manajemen. Masalah utama yang dihadapi ketika membangun SOC adalah Integrasi semua modul ini, biasanya dibangun sebagai bagian otonom, sementara kesesuaian ketersediaan, integritas, dan keamanan data dan transmisi mereka saluran. Dalam tulisan ini kita akan membahas arsitektur fungsional yang dibutuhkan untuk mengintegrasikan modul-modul tersebut. Bab satu akan memperkenalkan konsep di belakang setiap modul dan jelaskan secara singkat masalah umum yang dihadapi dengan masing-masing mereka. Dalam bab dua kita akan merancang arsitektur global SOC. Kita kemudian akan fokus pada pengumpulan & analisis data yang dihasilkan oleh sensor di bab tiga dan empat. Kesimpulan singkat akan menjelaskan penelitian lebih lanjut &analisis yang akan dilakukan di bidang desain SOC.

Penelitian yang dilakukan oleh (Anif, Hws, & Huri, 2015; Nugroho, Affandi, & Rahardjo, 2014) dengan judul "Penerapan Intrusion Detection System (IDS) dengan Metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang", peneliti mendefinisikan bahwa hal yang ditakuti oleh pengguna sistem komputer dan jaringan yaitu terkena virus dan dinyusup oleh peretas jaringan

atau *hacker*. Hampir setiap komputer memiliki anti virus dan sistem perangkat lunak *firewall* sistem-sistem tersebut mungkin bisa menahan serangan – serangan dari host tetapi kita tetap memerlukan sebuah sistem sebagai pemantauan jaringan agar kita tau permasalah dari jaringan tersebut. Teknik yang digunakan oleh peneliti yaitu *Intrusion Detection System* (IDS). Sistem IDS memeriksa setiap kejadian pada jaringan baik pada trafik jaringan maupun sistem operasi sehingga jaringan tersebut akan terdeteksi jika ada penyusup jaringan dengan cara menjalankan sistem *portsentry* dan di integrasikan dengan *syslog-notify* sebagai *alert* .

Kesimpulan dari penelitian ini yaitu bahwa keamanan jaringan merupakan sebuah isu yang sangat penting , karena banyak informasi yang penting yang tertinggal di dalam jaringan sehingga sebuah jaringan sangat membutuh sistem pemantauan sehingga kita akan tahu apa permasalahan dari jaringan tersebut. Sistem *portsentry* merupakan penangkalan dari *portscanning* tetapi tidak dapat memblokir serangan jenis *sniffer, IP Spoffing dan DOS*.

Menurut (Wijayanto & Waspada, 2016) dengan judul "Aplikasi Monitoring Perangkat dan Aktivitas Pengguna Pada Jaringan Menggunakan Protokol SNMP", peneliti tersebut mengatakan bahwa latar belakang dibuatnya sebuah sistem monitoring atau pemantauan jaringan ini agar dapat digunakan sebagai pemantauan dan mengontrol perangkat jaringan yang kompleks terhadap fungsi dan kinerja jaringan yang meliputi antara lain *traffic, bandwith,* dan *tracking* sehingga bisa mengetahui kondisi sumber masalah dalam perangkat jaringan tersebut.

Dalam penelitian ini peneliti menggunakan metode *waterfall* dengan sistem *database* MySQL. Metode tersebut sangat efektif dilakukan yang menghasilkan solusi dalam menerapkan aplikasi pemantauan dengan menggunakan protokol SNMP.

Setelah siap melakukan analisa penelitian ini menghasilkan sebuah kesimpulan, bahwa aplikasi-aplikasi seperti ini juga dapat membuahkan hasil sebuah data dan infomasi perangkat termasuk status antarmuka perangkat, status *up/down*, status *traffic in* dan *out*, dan berbagai informasi lainnya yang didapatkan dalam suatu perangkat jaringan sehingga dapat memudahkan *administrator* jaringan dalam memantau dan memonitoring perangkat jaringan tersebut.

Sistem monitoring jaringan adalah alat yang berkemampuan untuk mengawasi suatu jaringan komputer dari posisi yang ditentukan.

Dalam penerapannya, terdapat model konseptual sebagai pendukung untuk metode penelitiannya yaitu, *The International for Standardization* (ISO) yang menjelaskan fungsi monitoring jaringan, antara lain:

1. Monitoring performa

Memperkirakan performa pada suatu jaringan dan sekaligus menganalisa data statistik.

2. Monitoring kesalahan jaringan

Ditujukan untuk admin jaringan agar dapat mengenal suatu masalah pada perangkat sehingga langsung diketahui dan segera untuk mengambil tindakan perbaikan.

3. *Report* (pelaporan)
4. Manajemen keamanan

Mengatur hak akses pengguna ke *resource* jaringan sehingga data dan informasi tidak dapat diperoleh tanpa izin.

Penelitian ini menyimpulkan, bahwa aplikasi monitoring menggunakan protokol SNMP ini supaya berfungsi dengan menjalankan semua fungsi dan modul monitoring sesuai perancangan pada metode yang telah dibuat.

Dalam literatur lain oleh (Sholikatin & Rosyid, 2017) dengan judulnya "*Implementasi Fault Management* (Manajemen Kesalahan) Pada *Network Management System* (NMS) Berbasis SNMP", mengatakan bahwa latar belakang dirancang penelitian tersebut disebabkan adanya temuan masalah-masalah jaringan yang sering ditemui di lapangan diantaranya kerusakan elemen jaringan seperti *hub*, *bridge*, *router*, *server*, bahkan sampai ke *transmission facilities*. Kesalahan jaringan tersebut seringkali tidak dapat diketahui oleh seorang admin jaringan dan penanganan masalah menjadi terlalu lama sehingga berakibat fatal pada penurunan kualitas jaringan. Oleh karena itu, perancangan dan implementasi sebuah aplikasi sistem monitoring jaringan merupakan solusi yang efektif dalam mencari dan

menemukan kesalahan (*fault*) yang terdapat pada suatu jaringan, sehingga dapat dilakukan penanganan secepat mungkin.

Kesimpulan yang didapat dari penelitian bahwa Aplikasi NMS yang dirancang dapat membantu seorang admin jaringan dalam mengelola dan memelihara infrastruktur jaringan dan juga merupakan solusi yang efektif dalam mencari dan menemukan kesalahan (*fault*) yang terdapat pada suatu jaringan. Efektif yang dimaksud di sini adalah dalam hal penyampaian kejadian *error* yang bersifat *real time* sehingga dapat dilakukan penanganan sedini mungkin agar masalah tersebut tidak berakibat pada penurunan kualitas jaringan.

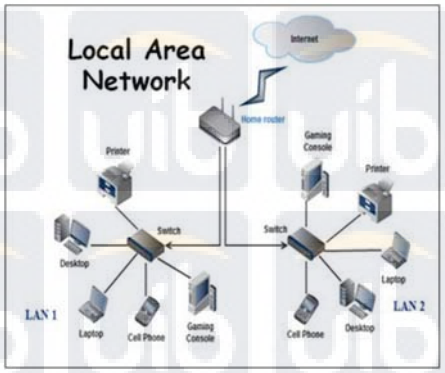
2.2 Landasan Teori

Dalam melakukan penelitian tentang keamanan jaringan *wireless* ini, penulis membuat sebuah landasan teori. Landasan teori adalah kumpulan dari teori – teori yang dipakai dalam penelitian penulis, dimana teori – teori ini nantinya akan berguna untuk memperkuat pengertian dan deskripsi dari studi terkait. Landasan teori yang penulis gunakan dalam penelitian ini yaitu:

2.2.1 Jaringan Komputer

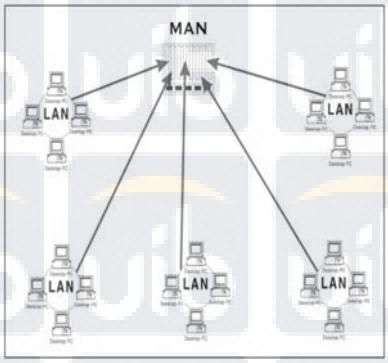
Jaringan komputer merupakan teknologi yang melingkupi *hardware*, *software*, dan perangkat jaringan lainnya serta bertujuan untuk dapat saling berkomunikasi atau saling berbagi data dengan konsep data tersebut dibawa oleh pengirim ke penerima dengan menggunakan media *wired* maupun *wireless* (Saputra, Irawan, & Ilhamsyah, 2014). Secara umum jaringan komputer terdapat LAN, MAN, dan WAN.

Local Area Network (LAN) merupakan salah satu jenis jaringan komputer yang mencakup wilayah kecil yang tidak begitu besar dan luas, seperti jaringan yang digunakan dalam kampus, gedung, kantor dengan dengan kecepatan pengiriman data hingga 1000 Mbit/s. (Varianto & Badrul, 2015). Berikut dapat dilihat pada Gambar 2.1:



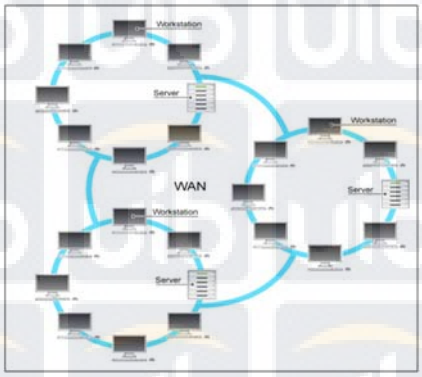
Gambar 2. 1 *Local Area Network* (LAN)

Metropolitan Area Network (MAN) merupakan topologi jaringan yang menggabungkan dari beberapa jaringan LAN sehingga jaringan ini mencakup ruang lingkup area yang lebih luas dan besar seperti suatu kota dengan pengiriman data dengan kecepatan kiriman yang lumayan tinggi, yang dapat menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Dari segi jangkauan, MAN ini dapat mencapai antara 10 km sampai 50 km (Lukman, 2016). Berikut dapat dilihat pada Gambar 2.2:



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

Wide Area Network (WAN) merupakan sebuah jaringan komputer dengan mencakup area jaringan yang lebih luas seperti antar Wilayah, Kabupaten, bahkan Negara, serta dapat digunakan untuk menghubungkan banyak LAN secara geografis terpisah agar dapat menggunakan layanan seperti *leased line, dial-up*, satelit atau layanan *packet carrier* (Chelara & Hermanto, 2014). Berikut dapat dilihat pada Gambar 2.3:

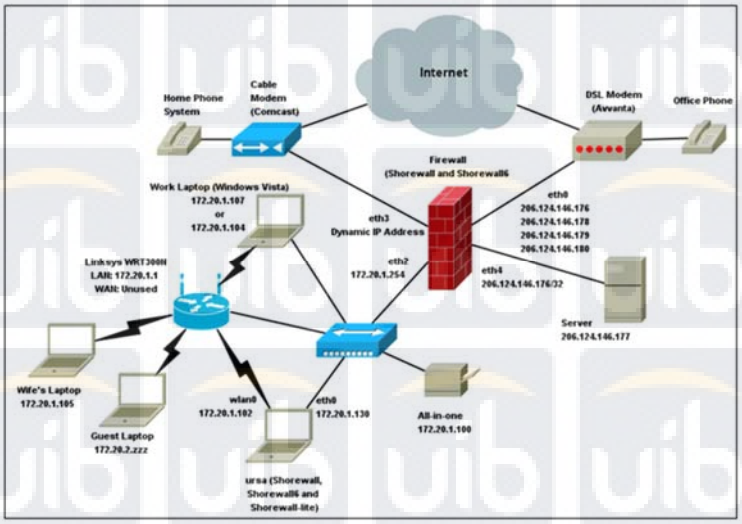


***Gambar 2. 3** Wide Area Network (WAN)*

2.2.2 Internet

Internet merupakan jaringan global dengan konsep dapat menghubungkan satu *host* dengan *host* lainnya baik bersifat pribadi (*stand alone*) maupun *corporate* diseluruh dunia melalui saluran dan *server* dengan menggunakan standar komunikasi pengiriman dan penerimaan data yang telah disepakati bersama dalam

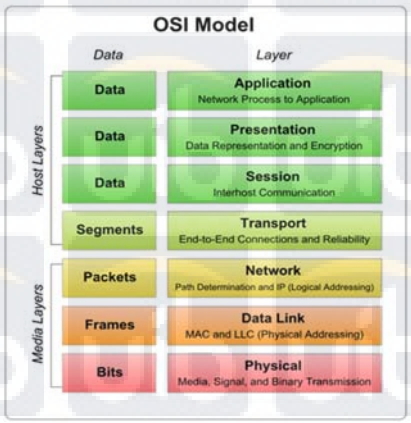
keseragaman pengiriman dan penerimaan data seluruh dunia sehingga tidak terjadi kekacauan dalam dunia Internet (Nurdin Nurdin, 2015). Berikut dapat dilihat pada Gambar 2.4:



Gambar 2. 4 Internet

2.2.3 OSI Layer

Open Systems Interconnection (OSI) layer ini dikembangkan untuk mengkoordinasikan standar pertukaran dan pengembangan data dalam sebuah jaringan. OSI *layer* bukanlah sebuah protokol melainkan sebuah standar dan acuan dalam jaringan komputer (Sujana, 2014). Berikut dapat dilihat pada Gambar 2.5:



Gambar 2. 5 OSI Layer

Model OSI terdiri atas 7 lapisan (*layer*), diantaranya:

1. *Physical Layer*

Physical layer adalah lapisan atau layer yang paling pertama dan berfungsi untuk mengelola koneksi perangkat-perangkat keras (*hardware*), layer ini biasanya menangani pengiriman dan penerimaan sinyal biner dan menangani penyandian bit. Contohnya topologi jaringan dan pengkabelan.

2. *Data Link Layer*

Data link layer adalah lapisan ini merupakan lapisan yang menyediakan alamat untuk sebuah pengiriman data dengan memaketkannya atau menggabungkannya menjadi sebuah *frame* yang berhubungan dengan *hardware* kemudian dibawa melalui media komunikasinya dengan kartu jaringan.

3. *Network Layer*

Network layer adalah lapisan ini merupakan lapisan yang berfungsi dalam menentukan alamat pada sebuah jaringan, dan mengalurkan atau menentukan rute untuk melaksanan pengiriman dalam perjalanan untuk tujuan sekaligus menjaga antrian trafik di jaringan. Data pada *layer* ini berbentuk paket yang berguna sebagai penerjemah IP *address*.

4. *Transport Layer*

Transport layer adalah lapisan yang berperan untuk memastikan pengiriman data, pembagian data per segmen, menangani pengurutan dan balasan, serta menyediakan tahapan kontrol. Unit protokol data pada lapisan ini disebut segmen.

5. *Session Layer*

Session layer merupakan lapisan yang memastikan proses dua terminal saling mengelola dan mengendalikan *connection*. Unit protokol pada lapisan ini disebut data.

6. *Presentation Layer*

Presentation layer merupakan lapisan yang berperan terhadap konversi data dan format untuk pengiriman data. Protokol yang berada dalam level ini berupa *redictor software*. Seperti layanan *Virtual Network Computing* (VNC).

7. *Application Layer*

Application layer merupakan lapisan yang bertanggung jawab sebagai *interface* terhadap fungsionalitas jaringan seperti mengontrol akses aplikasi ke jaringan, dan kemudian membuat pesan-pesan *error*. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

2.2.4 *Internet Protocol* (IP)

IP *Address* merupakan prosedur pengalamatan dengan memberikan sebaris *numeric* pada perangkat jaringan yang diterapkan di *interface* dari perangkat tersebut.

Pada umumnya, alamat IP berfungsi untuk mendeteksi *problem* disaat pengiriman paket data namun, dalam proses komunikasi antar data, alamat IP ini menerapkan dua peranan aturan yakni, *addressing* dan *fragmentation* (Wardoyo, Ryadi, & Fahrizal, 2014).

2.2.5 *Internet Protocol Version* 4 (IPV4)

IPv4 dalam model pengalamatan menggunakan 32 bit bilangan biner namun, untuk mempermudah penulisannya setiap delapan bit biner diwakili oleh satu segmen bilangan oktet, sehingga setiap alamat akan memiliki empat buah segmen dari 0.0.0.0 sampai dengan 255.255.255.255 misalnya 202.152.254.254 sehingga total alamat sebesar 232.

Alamat IPv4 dibagi menjadi dua bagian yaitu alamat jaringan (*network address*) dan alamat komputer (*host address*). *Network address* digunakan untuk

menunjukkan keberadaan pada komputer, sedangkan *host address* menunjukkan keberadaan komputer dalam jaringannya (Warman, Yudhistira, & Nugraha, 2017).

2.2.6 *Media Access Control* (MAC)

MAC *Address* adalah suatu alamat jaringan yang diimplementasikan pada lapisan *data-link* OSI *Layer*. Pada jaringan berbasis *ethernet*, MAC *address* merupakan alamat yang unik yang memiliki panjang 48-bit (6 *byte*) yang dapat mengidentifikasikan komputer, *interface router*, atau *node* lainnya sehingga sering disebut sebagai *Ethernet address*, *Physical address*, atau *Hardware address* (Susianto & Yulianti, 2015).

2.2.7 Linux

Linux adalah program yang menggunakan kernel sebagai sistem operasi berupa *script* yang tersedia di Internet pada tahun 1991. Setelah itu, banyak *user* berperan penting dalam mengembangkan dan memperluas Linux di berbagai belahan dunia. Sistem, peralatan maupun pustakanya secara umum berasal dari sistem operasi berbasis *General Public License* (GPL) yang diumumkan pada tahun 1983 oleh Richard Stallman. Kontribusi GNU adalah dasar dari munculnya nama alternatif GNU/Linux (Harjono, 2016).

2.2.8 Security Onions

Security Onions merupakan sebuah sistem yang berguna untuk mengetahui suatu permasalahan dalam sebuah jaringan, dalam security onions kita menjalankan satu tools lagi yaitu Sguil tools inilah yang berperan untuk memonitoring jaringan kita, dengan menggunakan tools ini kita mengecek dimana terjadi masalah jaringan tersebut, kita dapat melihat IP apa yang masuk ke jaringan kita dan berasal dari

mana IP tersebut dan apa yang dilakukan IP tersebut, sehingga kita dapat menganalisa permasalahannya dan bisa mengatasi masalah tersebut. Setelah kita mendapatkan IP tersebut kita akan menganalisa apa yang dilakukan IP tersebut.

2.2.8 Virtual Box

Menurut (Saefulloh, Supriyono, & Sc, 2014), Virutal Box merupakan sebuah sistem atau tools yang berguna pada saat kita melakukan sebuah virtualisasi.Tools ini digunakan untuk menjalankan virtualisasi seperti kita mengeksekusi sebuah perangkat lunak atau sistem operasi di dalam sistem operasi utama. Sehingga orang dapat melakukan sebuah pengujian atau menjalankan sistem operasi yang lain tanpa mengganggu sistem operasi utama. Tetapi pada saat kita menjalankan virtualisasi dibutuhkan speksifikasi yang mendukung karena dalam satu komputer kita menjalankan lebih dari satu sistem operasi, sehingga jika komputer atau laptop kita tidak memiliki speksifikasi yang mendukung pada saat kita menjalankan virtualisasi akan lebih lambat dalam prosesnya sistem tersebut. Biasa virtualisasi ini dijalankan untuk melakukan sebuah pengujian dan kita tidak perlu lagi menggunakan perangkat tambahan atau komputer tambahan untuk menjalankan sebuah sistem operasi yang akan kita gunakan untuk pengujian. Penguji sendiri juga menggunakan virtualisasi untuk melakukan pengujian ini, sistem operasi utama menggunakan windows 10 dan menjalankan dua sistem operasi dalam virtualisasi, yaitu security onions berbasis Ubuntu dan satu lagi Ubuntu server.

2.2.9 Security Operation Centre

Menurut (Bidou, 2014) Security Operation Centre (SOC) merupakan suatu manajemen yang berfungsi untuk menggambarkan sebagian atau seluruh sebuah platform yang bertujuan untuk menyediakan layanan deteksi dan reaksi insiden

keamanan. Security Operation Centre (SOC) terdiri dari lima modul berbeda: acara generator, pengumpul acara, basis data pesan, mesin analisis, dan reaksi perangkat lunak manajemen. Masalah utama yang dihadapi ketika membangun SOC adalah Integrasi semua modul ini, biasanya dibangun sebagai bagian otonom, sementara kesesuaian ketersediaan, integritas, dan keamanan data dan transmisi mereka saluran. Dalam tulisan ini kita akan membahas arsitektur fungsional yang dibutuhkan untuk mengintegrasikan modul-modul tersebut.

Komponen inti dalam membangun Security Operation Centre (SOC), terdiri dari 3 komponen yaitu,

1. People

   Tantangannya adalah ketersediaan security profesional yang masih sedikit, effort yang besar untuk merekrut, melatih, dan maintain tenaga ahli SOC, hingga tenaga ahli tersebut memiliki skill dan experience yang cukup untuk memonitor, menganalisa dan memberikan rekomendasi terhadap jaringan terkait dengan incident security yang akan dan sedang terjadi.

2. Technology

   Tantangan yang akan dihadapi adalah kompleksitas infrastuktur, dimana untuk membangunnya akan memerlukan waktu yang lama, modal yang besar, dan sarana yang mendukung.

3. Process

   Tingkat kompleksitas dalam membangun dan menerapkan prosedur, bagaimana cara meningkatkan supaya proses tersebut dapat efektif, waktu dan uang untuk merekrut tenaga ahli untuk membangun proses

SOC, dan belum tentu proses tersebut dapat berjalan dengan baik dan tepat.