BAB II
TINJAUAN PUSTAKA

2. 1 Tinjauan Pustaka

Penelitian oleh Anif et al., (2015) dengan judul "Penerapan *Intrusion Detection System* (IDS) dengan *Metode Deteksi Port Scanning* pada Jaringan Komputer di Politeknik Negeri Semarang". Pada penelitian ini peniliti membuat suatu keamanan jaringan yang ringan, mudah dianalisis serta mudah diatur oleh *networking administrator,* dengan merancang sebuah sistem yang memakai *portsentry* serlaku *Intrusion Detection System* (IDS) yang diintegrasi *syslog-notify* untuk memberitahukan ke *networking administrator,* yang kemudian sistem men-*drop* IP yang dicuragai telah melakukan serangan *port scanning* ke sistem kita. Namun sistem yang menggunakan *portsentry* akan bekerja dalam mendeteksi serangan *port scanning* saja dan tidak dapat men-*drop* serangan, seperti *IP spoofing*, *Denial of Service* (DoS) dan *sniffer* karena bersifat tertutup serta tidak dianggap sebagai sebuah serangan yang dapat membahayakan sistem.

Penelitian oleh Idrus, (2016) dengan judul "Sistem Monitoring Jaringan PT. Exhibition Network Indonesia Dengan *The Dude* Berbasis Mikrotik". Penelitian ini memanfaatkan *tools* miktrotik untuk membuat sebuah sistem keamanan monitoring jaringan diperusahaannya. *The dude* ialah *software* yang dapat memonitoring jaringan yang terdapat di mikrotik, *the dude* mempunyai *service* yang dapat melihat *host* mana yang hidup didalam sebuah jaringan serta dapat menyajikan gambaran *host* berserta jaringannya.

Penelitian oleh Rinaldo, (2016) dengan judul "Implementasi Sistem Monitoring Jaringan Menggunakan Mikrotik RouterOs Di Universitas Islam Batik Surakarta". Penelitian ini menggunakan mikrotik *router* dan aplikasi *the dude* yang terdapat didalam *router* mikrotik untuk menciptakan sistem monitoring jaringan. Aplikasi *the dude* akan mengatur sistem notifikasi yang telah terhubung dengan *router* mikrotik kemudian akan mengirimkan pesan melalui *media sosial short message service* (SMS), *email,* ataupun *telegram* kepada administrasi jaringan apabila *device* mati, rusak, ataupun putus koneksi yang ditandai dengan ping mengalami *timeout,* maka *device* akan berubah menjadi *down* dan akan

mengirimkan pesan notifikasi secara otomatis kepada administrasi jaringan yang berisi informasi *device*.

Penelitian oleh Arta et al., (2018) dengan judul "Simulasi Implementasi *Intrusion Prevention System* (IPS) Pada *Router* Mikrotik". Penelitian ini menggunakan mikrotik *router* untuk membuat sistem keamanan jaringan guna membantu *network administrator* untuk melakukan monitoring trafik jaringan dengan *instrusion prevention system* (IPS) yang merupakan kombinasi antara fasilitas *blocking capabilities* dari *firewall*.

Tabel 2.1 Tinjauan Pustaka

No	Nama	Tahun	Judul	Kesimpulan
1	Anif et al	2015	Penerapan *Intrusion Detection System* (IDS) dengan *Metode Deteksi Port Scanning* pada Jaringan Komputer di Politeknik Negeri Semarang	Sistem ini menggunakan *portsentry* serlaku *Intrusion Detection System* (IDS) untuk mendeteksi dan mencatat serangan *port scanning*.
2	Idrus	2016	Sistem Monitoring Jaringan PT. Exhibition Network Indonesia Dengan *The Dude* Berbasis Mikrotik	Penelitian ini menggunakan mikrotik untuk keamanan jaringan nya, serta menggunakan *the dude* untuk melihat *host* jaringan mana yang hidup.
3	Rinaldo	2016	Implementasi Sistem Monitoring Jaringan Menggunakan Mikrotik RouterOs Di Universitas Islam Batik Surakarta	Penelitian ini menggunakan mikrotik *router* dan aplikasi *the dude* yang terdapat didalam *router* mikrotik untuk menciptakan

No	Nama	Tahun	Judul	Kesimpulan
				sistem monitoring jaringan.
4	Arta et al	2018	Simulasi Implementasi *Intrusion Prevention System* (IPS) Pada *Router* Mikrotik	Sistem ini melakukan monitoring trafik jaringan dengan *instrusion prevention system* (IPS) dengan kombinasi antara fasilitas *blocking capabilities* dari *firewall*

Penulis menganalisis kelima jurnal tersebut dapat disimpulkan penilitian, penelitian Anif et al., (2015) dengan memakai *portsentry* sebagai *Intrusion Detection System* (IDS), penelitian Idrus, (2016) yang menggunakan router mikrotik dalam membuat sistem jaringan, penelitian Rinaldo, (2016) yang menggunakan aplikasi *The dude* yang terdapat pada router mikrotik untuk mengirimkan notifikasi pada *networking administration*, dan penelitian Arta et al., (2018) melakukan monitoring trafik jaringan dengan *instrusion prevention system* (IPS) dengan kombinasi antara fasilitas *blocking capabilities* dari *firewall* dengan bantuan *router* mikrotik.

2.2 Landasan Teori

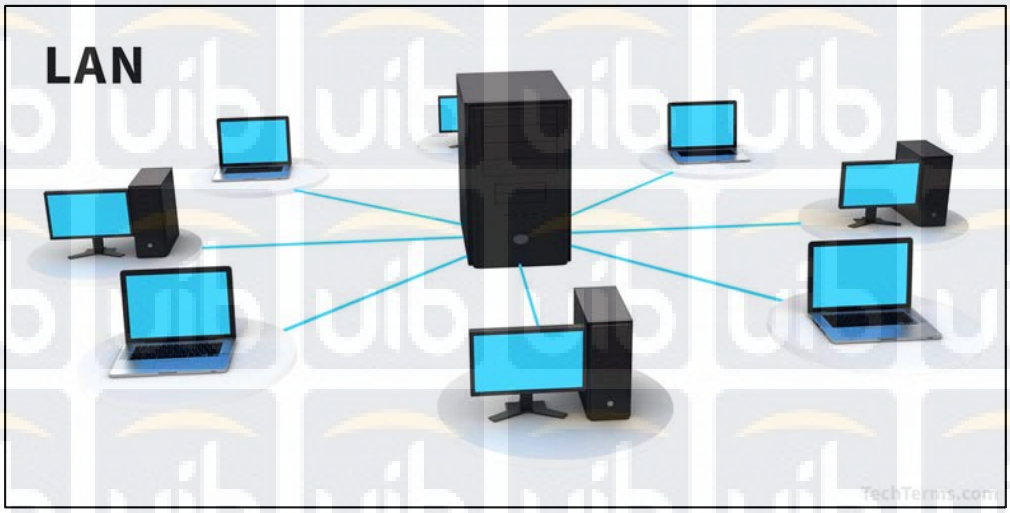
Untuk membuat sebuah penelitian mengenai *networking security* membutuhkan landasan teori, dimana teori tersebut nantinya akan digunakan untuk penelitian penulis yang berfungsi untuk menguatkan pengertian pada studi yang penulis lakukan. Adapun teori - teori yang penulis pakai pada penelitian ini yaitu:

2.2.1 Jaringan Komputer

Menurut Afrianto & Setiawan, (2015) Jaringan komputer merupakan sebuah sistem yang tersusun dari beraneka macam komputer berserta *resource* nya yang dibuat agar bisa memakai sumber daya yang ada seperti *monitor, printer, mouse, cpu, keyboard* sehingga bisa mengakses informasi yang diinginkan. Jaringan komputer mencakup *software, hardware* serta perangkat jaringan komputer lainnya yang disatukan dengan tujuan untuk bisa saling melakukan komunikasi serta saling berbagi data dengan konsep bahwa data akan dibawa melalui pengirim ke penerima memakai media *wired* ataupun *wireless* (Saputra et al., 2014). Dengan menggunakan jaringan pada komputer, informasi juga bisa diakses dikomputer lain, contohnya menggunakan *Local Area Network*.

2.2.2 Local Area Network (LAN)

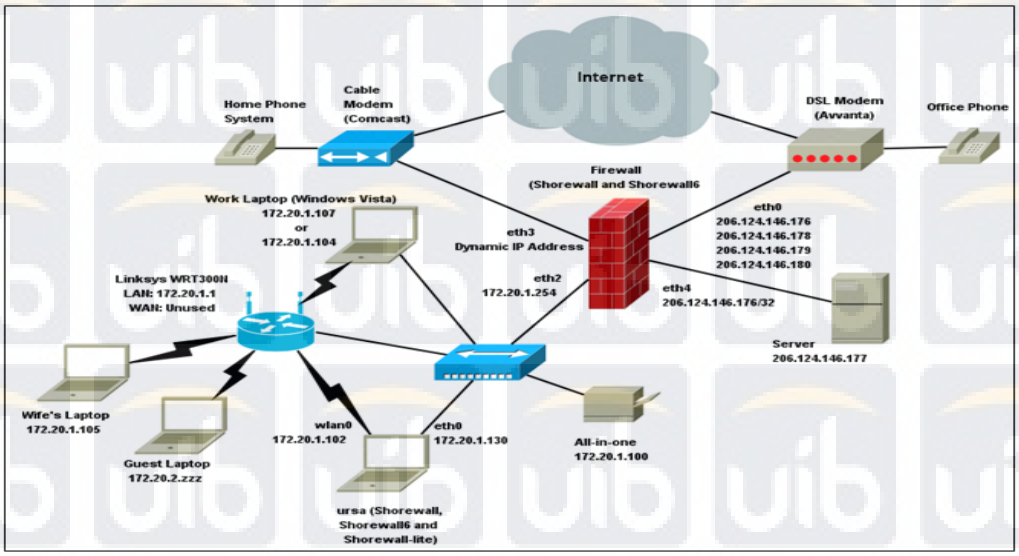
Local Area Network (LAN) merupakan jaringan yang menyatukan 1 atau lebih komputer didalam sebuah *local area*. LAN memiliki skala yang lebih kecil disbanding MAN maupun WAN, yang menyebabkan durasi transmisi saat kondisi terburuknya dibatasin dan kita hanya dapat mengetahui sebelumnya (Hariyadi, 2016). Wilayah cakupan *Local Area Network* (LAN) tidak begitu besar dan luas, LAN hanya dapat mencakup wilayah kecil seperti jaringan yang digunakan didalam rumah, kantor, sekolah, dan perusahaan dengan kecepatan pengiriman data sampai batas 1000 Mbit/s. (Varianto & Badrul, 2015). Gambar 2.1 adalah topologi jaringan LAN.



Gambar 2.1 Jaringan *Local Area Network*

2.2.3 Internet

Internet ialah sebuah jaringan computer terhubung dengan memakai *standart global transmission control protocol* / *internet protocol* (TCP/IP) sebagai dasar perpindahan paket data agar dapat melayanin *user* yang berada dari seluruh dunia (Afrianto & Setiawan, 2015). Konsep internet yaitu bisa menyambungkan suatu *host* dengan *host* lainnya baik itu bersifat *stand alone* ataupun *corporate* ke penjuru dunia dengan menggunakan saluran serta *server* dengan standart komunikasi penerimaan dan pengiriman paket data yang telah disetujui oleh kedua pihak pada keseragaman penerimaan dan pengiriman data ke seluruh dunia agar tidak menimbulkan kekacauan pada dunia Internet (Nurdin Nurdin, 2015). Gambar 2.2 merupakan topologi jaringan internet.



Gambar 2.2 Topologi *Internet*

2.2.4 *Internet Protocol* (IP)

IP *Address* merupakan indetifikasi unik dari sebuah komputer, yang berupa *logical number address*. IP *address* sendiri berisikan alamat informasi berharga yang dikodekan dan juga menyediakan kompleksitas *routing* (Dasmen, 2018).

Pada dasarnya IP *address* berfungsi sebagai pendeteksi masalah pada saat pengiriman paket data. tetapi pada saat proses komunikasi antar data, alamat IP memakai dua peranan aturan yang berbeda yaitu, *fragmentation* dan *addressing* (Wardoyo et al., 2014).

2.2.5 *Internet Protocol Version* 4 (IPV4)

Internet Protocol Version 4 merupakan sebuah jaringan diamana pengalamatan jaringan yang dipakai pada *protocol* jaringan TCP/IP yang menggunkan *protocol IP version 4* dengan total panjangnya ialah 32-*bit* yang secara teoritis bias mengalamati 4 milliar *host* komputer dengan angka pastinya 4,294,967,296 host yang berada diseluruh dunia.

IPv4 *Internet Protocol Version 4* terdapat dua komponen yaitu alamat komputer (*host address*) dan satunya lagi adalah alamat jaringan (*network address*). *host address* berfungsi untuk menentukan keberadaan komputer didalam jaringan, sedangkan fungsi *Network address* untuk menunjukan keberadaan pada komputer.

2.2.6 *Media Access Control* (MAC)

MAC *Address* merupakan sebuah nomor indetifikasi pada sebuah perangkat yang terletak pada lapisan *data-link* pada OSI *Layer*. MAC *address* sendiri memiliki alamat unik yang panjangnya 48-bit yang berfungsi untuk mengidentifikasikan sebuah perangkat komputer, *node, interface router* lainnya oleh sebab itu sering disebut sebagai *Hardware address, Ethernet address, Physical address* (Susianto & Yulianti, 2015).

2.2.7 *Intrusion Detection System* (IDS)

Intrusion detection system merupakan sebuah sistem yang mendeteksi aktivitas yang mencurigakan kemudian mencatatnya ke dalam sebuah sistem ataupun jaringan. Apabila ditemukan aktivitas yang mencurigakan yang berhubungan dengan *traffic* jaringan maka *intrusion detection system* akan memberikan peringatan kepada *administration* jaringan Sutarti et al., (2018).

2.2.8 *Intrusion Prevention System* (IPS)

Intrusion Prevention System merupakan sistem keamanan yang dapat menggabungkan teknik firewall dan metode *intrusion detection system* untuk mencegah serangan yang ke dalam jaringan dengan memeriksa dan mencatat semua paket data yang masuk kemudian memblok paket data yang dianggap melakukan serangan kedalam jaringan.

2.2.7 Linux

Linux ialah sebuah system operasi open source gratis dibawah lisensi Gnu Not Unix (GNU). Linux OS memungkinkan pengguna untuk memperoleh software yang lengkap beserta source code-nya, sehingga pengguna mengubah memodifikasi source code-nya, dan itu legal dilakukan tentunya tetap dibawah lisence GNU. Sistem, *tools* ataupun teori sebagian besar berasal disistem operasi yang berbasis *General Public License* (GPL) diumumkan oleh Richard Stallman pada tahun 1983. Kontribusi GNU merupakan awal mula munculnya nama alternatif GNU/Linux (Harjono, 2016).

2.2.8 Mikrotik

Menurut Lubis, Raharjo, & Sutanta, (2014) Mikrotik mempunyai kelebihan-kelebihan antara lain satu *account user* hanya dapat digunakan untuk satu user, dapat mencatat *MAC address* dan *IP address user,* manajemen *bandwidth* bisa dilakukan sesuai keinginan *user*, serta memilki tampilan grafis penuh. Sedangkan kelemahan mikrotik dinilai tidak memiliki halaman *logout* yang dapat muncul secara otomatis, *router* dapat mencatat *cookies* pada *account user* yang telah melakukan *login*, serta sistem *billing hotspot* dilakukan secara *default*. Menurut Murtomaa & Letto, (2017) Mikrotik merupakan perusahaan yang berpusat di Latvia. Dibangun oleh John Trully dan Arnis Riekstins pada tahun 1996. John dan Arnis sendiri memulai *routing* dunia pada tahun 1996. Berawal dari sistem operasi *MS-DOS* dan *Linux* yang kemudian dikemas menggunakan teknologi *Wireless* LAN (WLAN) *Aeronet* dengan kecepatan 2 *Mbps* di Moldova yang merupakan negara tetangga Latvia, lalu dimulai dengan melayani lima *costumer* pertamanya diLatvia. Berdasarkan Supendar & Siregar, (2018) *router* mempunyai fungsi berupa sebuah aplikasi manajement bandwidth, *vlan, virtual private network, routing*, sistem *hotspot*, aplikasi *wireless access point*, aplikasi *firewall*, dan aplikasi *backhaul link*.

2.2.9 Winbox

Winbox merupakan sebuah perangkat lunak yang digunakan untuk memudahkan *user* mengakses serta melakukan konfigurasi dengan menggunakan mikrotik baik itu menggunakan cara *mode Graphical User Interface* (GUI)

maupun *mode Command Line Interface* (CLI) (Dwiyatno et al., 2015). Dengan menggunakan *winbox* kita bisa menghubungkan computer kita ke dalam mikrotik *router* baik dengan memakai alamat IP *address* maupun dengan *MAC address* sebuah perangkat komputer. Menurut Fitriastuti & Utomo, (2012) *winbox* mempunyai beberapa kelebihan, kelebihan *winbox* ini sendiri yaitu dapat memudahkan *user* untuk melakukan *remote* ke *router* karena berbasis GUI.

2.2.10 Virtual Machine

Menurut (Nursalam, 2016, 2013), Mesin Virtual sering disebut sebagai *virtual machine* merupakan penerapan perangkat lunak ke sebuah mesin komputer yang bisa menjalankan program yang serupa layaknya kayak sebuah komputer asli (Aditya et al., 2015). *Virutal machine* berupa sistem atau *tools* yang kita gunakan saat kita ingin melakukan virtualisasi. *Tools* ini berfungsi sebagai virtualisasi pada saat kita ingin mengeksekusi sistem operasi dari dalam sistem operasi utamanya sehingga kita bisa membuat sebuah percobaan serta mengoperasikan sistem operasi kita di *virtual machine* tersebut tanpa mengganggu sistem operasi yang sebenarnya.

2.2.11 Security Operation Centre

Security Operation Centre (SOC) adalah suatu sistem manajemen yang berfungsi untuk menggambarkan sebagian maupun keseluruhan sebuah platform yang bertujuan sebagai menyedia layanan pendeteksi dan reaksi didalam insiden keamanan (Bidou, 2014). *Security Operation Centre* (SOC) sendiri terdiri dari 5 modul yang berbeda diantaranya: acara generator, pengumpul acara, basis data pesan, mesin analisis, dan reaksi perangkat lunak manajemen. Masalah yang sering dihadapi saat membangun *Security Operation Centre* (SOC) ialah integrasi dari semua modul ini, SOC biasanya dibangun sebagai bagian dari otonom, sementara itu kesesuaian, ketersediaan, integritas, keamanan data dan transmisi mereka saluran. Pada laporan ini kita akan menjelaskan arsitektur fungsional yang dibutuhkan untuk mengintegrasikan modul-modul tersebut.

Komponen inti dalam membangun *Security Operation Centre* (SOC) yaitu terdiri dari 3 komponen diantaranya:

1. *People*

   Komponen pertama yang hatus dimiliki yaitu seorang *networking administration* yang handal. Akan sangat membutuhkan waktu dan usaha yang keras agar bisa merekrut, *training*, dan *maintenance* tenaga ahli untuk menjadi *Security Operation Centre* (SOC) yang handal. Seorang *networking administration* dapat dikatakan handal apabila tenaga ahli dinilai mempunyai skill dan *experience* yang baik dalam menganalisa, memonitor, serta memberikan rekomendasi pada jaringan yang terkait seperti *incident security* yang sering dialami.

2. *Technology*

   Komponen kedua yaitu *technology*, masalah yang biasa dihadapi ialah kompleksitas infrastuktur jaringan, disebabkan untuk membangun, merancang sangat membutuhkan modal yang besar, sarana yang mendukung serta membutuhkan waktu yang lama.

3. *Process*

   Komponen terakhirnya adalah *process*, *process* yang dimaksud yaitu tahap kompleksitas dalam membangun, merancang, menerapkan prosedur, serta berusaha meningkatkan efesiensi dan efektifitas agar proses dapat diselesaikan dalam waktu singkat.