BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Rujukan penelitian yang pertama yaitu jurnal Oris Krianto Sulaiman Mahasiswa Universitas Islam Sumatera Utara dengan judul Analisis Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security*. Dalam jurnal nya, peneliti melakukan analisis terhadap masing masing jenis *switch port security* untuk menentukan kehandalan, kegunaan dan pemanfaatannya dilapangan. Peneliti menggunakan aplikasi simulasi program Cisco Packet Tracer 6.2 (CPT).

Rujukan penelitian kedua yaitu jurnal Ridatu Ocanitra dan Muhammad Ryansyah mahasiswa Fakultas Teknik, Universitas Bina Sarana Informatika dengan judul Implementasi Sistem Keamanan Jaringan Menggunakan *Firewall Security Port* pada Vitaa Multi Oxygen. Dalam jurnal nya, peneliti melakukan analisis bagaimana memblok akses jaringan pada karyawan yang tidak melaporkan perpindahan tempat kerja dan dapat mencegah terjadinya pencurian data oleh orang asing atau bukan karyawan perusahaan tersebut.Dengan penelitian ini, peneliti menyimpulkan bahwa dengan menggunakan *Firewall Security port* maka pihak *IT* dapat memanajemen setiap pengguna jaringan dan mendapatkan informasi jika terdapat perpindahan, karena perangkat yang tidak didaftarkan hak aksesnya akan diblok untuk terkoneksi ke jaringan tersebut.

Rujukan penelitian ketiga yaitu jurnal Sudaryanto mahasiswa Sekolah Tinggi Teknologi Adisutjipto dengan judul *Implementation Port Security For Security Systems Network At The Computing Laboratory Of Adisutjipto Technology College*. Dalam jurnalnya, peneliti melakukan analisis dengan permasalahan bagaimana dengan keamanan *port* yang diimplementasikan di Laboratorium Komputasi STTA pencurian atau penggunaan *bandwith* yang berlebihan dapat dikurangi 70,19% dan penggunaan kabel *Unshielded twisted-pair* (UTP) dengan perangkat komputer yang tidak terdaftar dapat dicegah. Dengan penelitian ini, peneliti menyimpulkan bahwa implementasi keamanan jaringan dengan

menggunakan *port security* dapat memaksimalkan penggunaan *bandwith* di Lab Komputasi sebesar 95,4% dan implementasi *port security* dapat digunakan untuk mencegah penggunaan kabel *UTP* yang tidak bertanggung jawab.

Sedangkan penelitian yang dilakukan oleh peneliti tidak jauh berbeda dengan penelitian sebelumnya yaitu mengimplementasikan sistem keamanan *port switch* di lab jurusan teknik komputer dengan menggunakan metode *static port security*. Untuk memudahkan *administrator* jaringan dalam meningkatkan keamanan pada perangkat yang ada di laboratorium jaringan, maka perlu melakukan pengamanan jaringan lokal yaitu salah satunya dengan menerapkan sistem keamanan *security port* pada Cisco *switch*.

Untuk lebih jelas dan detail terhadap penelitian terdahulu dapat dilihat pada table berikut:

Tabel 2.1 Perbandingan Penelitian Terdahulu dengan Penelitian Sekarang

No	Penelitian	Persamaan	Perbedaan
1.	Oris Krianto Sulaiman. Analisis Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security*.	Menguji kegunaan *switch port security* dan manfaatnya.	-Penerapan *switch port security* ini hanya digunakan di lab jaringan jurusan Teknik Komputer Politeknik Negeri Sriwijaya. -Penulis menggunakan aplikasi Putty untuk melakukan *setting port security* sedangkan peneliti menggunakan Cisco Packet Tracer sebagai aplikasi simulasi.

2.	Ridatu Ocanitra dan Muhammad Ryansyah. Implementasi Sistem Keamanan Jaringan Menggunakan *Firewall Security Port* pada Vitaa Multi Oxygen.	Memanajemen setiap pengguna jaringan, karena perangkat yang tidak terdaftarkan hak aksesnya akan diblok untuk terkoneksi ke jaringan tersebut.	-Penerapan *switch port security* ini hanya digunakan di lab jaringan jurusan Teknik Komputer Politeknik Negeri Sriwijaya -Penulis menggunakan aplikasi Putty untuk melakukan *setting port security*.
3.	Sudaryanto. *Implementation Port Security For Security Systems Network At The Computing Laboratory Of Adisutjipto Technology College*.	Penggunaan kabel *Unshielded twisted-pair* (UTP) dengan perangkat komputer yang tidak terdaftar dapat dicegah	-Penerapan *switch port security* ini hanya digunakan di lab jaringan jurusan Teknik Komputer Politeknik Negeri Sriwijaya -Penulis menggunakan aplikasi Putty untuk melakukan *setting port security*.

2.2 Putty

Aplikasi ini adalah aplikasi kondang yang digunakan untuk masuk ke *server* target dan melakukan segala hal, seperti layaknya sebagai *root*. Ketika hak akses yang didapat sudah sebagai *root* maka analoginya seperti hak *administrator* pada sebuah sistem operasi Windows, sehingga dapat melakukan apa saja.Putty ini juga sebagai *software remote console*/terminal yang digunakan untuk me-*remote* komputer menggunakan *port SSH*. Bentuk akses *remote* dapat berupa mode teks

ataupun mode grafis, tergantung pada konfigurasi yang diizinkan.Putty ini dapat digunakan untuk versi Windows dan Linux . Dan aplikasi Putty ini tidak perlu diinstal, namun hanya langsung dengan eksekusi pada file *executable* saja. (Winarno dkk,2015)

2.3 Pengertian Internet

Internet sebetulnya singkatan dari kata *Interconnected Networking.Networking* artinya jaringan, sedang *Interconnected* berarti saling berkaitan/terkoneksi. Sehingga *internet* adalah jaringan komputer yang saling terkoneksi.(Winarno dkk,2015)

2.4 Pengertian Jaringan Komputer

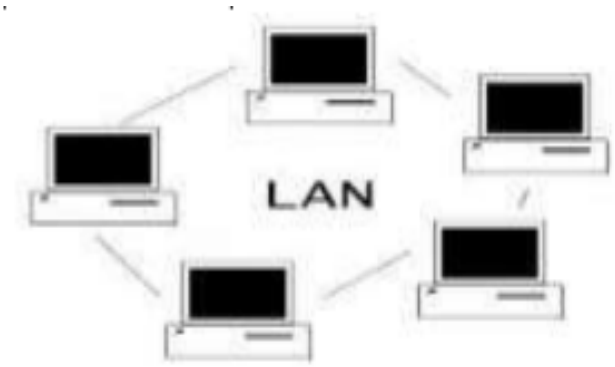
Jaringan komputer adalah sekumpulan komputer yang terhubung dan membentuk sebuah jaring-jaring yang dapat saling berhubung satu sama lain. Tidak hanya saling terhubung, tetapi dapat dimanfaatkan untuk berbagi sumber daya (printer, *CPU*), berkomunikasi (pesan instan, surel), dan dapat mengakses informasi (*browsing web*). (Ariawal & Onno,2016)

2.5 Jenis-Jenis Jaringan Komputer

Setiap jaringan komputer tentu memiliki kelebihan dan kekurangan masing-masing. Setiap jenis jaringan yang dipilih untuk digunakan tentunya berdasarkan biaya dan tujuan yang dimiliki oleh penggunanya. Ariawal dan Onno (2016) menyatakan bahwa secara umum jaringan komputer terbagi menjadi 3 jenis, yaitu :

2.5.1 Lokal Area Network (LAN)

Sebuah *LAN* adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan, seperti sebuah kantor pada sebuah gedung, atau tiap-tiap ruangan pada sebuah sekolah. Biasanya jarak antar *node* tidak lebih jauh dari sekitar 200 m.



Gambar 2.1 Jaringan Local Area Network (LAN)

(*Sumber: Sitanggang R, 2019*)

2.5.2 Metropolitan Area Network (MAN)

Sebuah *MAN* biasanya meliputi area yang lebih besar dari *LAN*, misalnya antar gedung dalam suatu daerah (wilayah seperti provinsi atau negara bagian). Dalam hal ini jaringan menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar. Sebagai contoh, jaringan beberapa kantor cabang sebuah bank di dalam sebuah kota besar yang dihubungkan antara satu dengan lainnya.

Gambar 2.2 Jaringan Metropolitan Area Network (MAN)

(*Sumber: Sitanggang R, 2019*)

2.5.3 Wide Area Network (WAN)

Wide Area Network (WAN) adalah jaringan yang biasanya sudah menggunakan media *wireless*, sarana satelit, ataupun kabel serat *optic*, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antar kota dalam suatu wilayah, tetapi mulai menjangkau area/wilayah otoritas negara lain.

Gambar 2.3 Jaringan Wide Area Network (WAN)

(*Sumber: Sitanggang R, 2019*)

2.6 Perangkat Jaringan Komputer

Jaringan komputer merupakan sekumpulan perangkat jaringan yang dihubungkan melalui media transmisi. Beberapa perangkat jaringan yang biasa digunakan adalah *Repeater, Hub, NIC, Bridge, Switch* dan sebagainya.(Irawati dkk,2018)

2.6.1 Repeater

Repeater merupakan perangkat jaringan yang bekerja pada lapis fisik *OSI*. *Repeater* berfungsi menguatkan sinyal pada saat ditransmisikan. Dalam perjalanannya, sinyal akan mengalami pelemahan/attenuasi. Pelemahan meningkat disebabkan oleh peningkatan panjang kabel yang digunakan serta peningkatan jumlah *node* dalam jaringan. (Irawati dkk,2018)

Gambar 2.4 Repeater

(*Sumber: www.cisco.com*)

2.6.2 Hub

Hub merupakan *multiport repeater* yang berfungsi untuk menghubungkan beberapa perangkat yang menggunakan *ethernet* 10Base-T atau 10Base-F sehingga menjadikannya dalam satu segmen jaringan. *Hub* disebut juga sebagai konsentrator dan bekerja pada lapisan fisik (layer 1) pada model OSI. Cara kerja hub sebagai berikut : ketika sebuah sinyal tiba di salah satu *port* pada hub, maka sinyal tersebut akan dikuatkan dan kemudian diteruskan ke *port-port* yang lain. Hal ini akan menyebabkan kinerja jaringan menjadi lambat jika banyak sinyal yang dikirimkan oleh tiap *port* pada hub. (Irawati dkk,2018)

Gambar 2.5 Hub

(*Sumber: www.cisco.com*)

2.6.3 Kartu Jaringan (Network Interface Card/ NIC)

Kartu jaringan atau LAN *Card*, NIC *card* atau Ethernet *card* merupakan antarmuka yang menghubungkan antara PC dengan sebuah jaringan. Pertukaran data antar komputer dalam jaringan dapat terjadi melalui media NIC *card*. NIC juga berfungsi mengontrol aliran data antara komputer dan sistem kabel, serta menerjemahkannya ke dalam *bit* yang bisa dimengerti oleh komputer. (Irawati dkk,2018)

Gambar 2.6 Network Interface Card (NIC)
(*Sumber: www.asus.com*)

2.6.4 Bridge

Bridge merupakan perangkat jaringan yang terdiri dari 2 *port* dan berfungsi membagi segmen di dalam *LAN*. *Bridge* bekerja berdasarkan alamat *MAC*. Setiap *frame* yang melewati *port* pada *bridge*, akan dibaca alamat *MAC* beserta nomor *port* kemudian disimpan dalam tabel *bridge*. *Bridge* dapat mengambil keputusan apakah sebuah *frame* akan diteruskan atau ditolak. (Irawati dkk,2018)

Gambar 2.7 Bridge
(*Sumber: www.linksys.com)*

2.6.5 Switch

Switch adalah perangkat keras komputer yang berfungsi untuk melakukan *bridging* transparan atau menghubungkan beberapa segmentasi jaringan dan meneruskan *frame* berdasarkan alamat fisik perangkat atau alamat *MAC*. *Switch* identik dengan *hub* tetapi *switch* lebih cerdas dan memiliki performa lebih tinggi dibandingkan dengan *hub*. *Switch* disebut juga *multiport bridge*. (Irawati dkk,2018)

Gambar 2.8 Switch

(*Sumber: www.cisco.com*)

2.6.6 Console Cable

Kabel Konsol adalah kabel yang biasanya digunakan untuk mengkonfigurasi sebuah perangkat jaringan secara langsung. Biasanya tidak digunakan dalam menghubungkan jaringan, hanya untuk mengkonfigurasi sebuah perangkat jaringan secara langsung. (Ariawal dan Purbo,2016)

Gambar 2.9 Console Cable

(*Sumber: www.tp-link.com*)

2.6.7 Router

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui proses yang dikenal sebagai *routing*.Proses *routing* terjadi pada lapisan 3 (Lapisan jaringan seperti *Internet Protocol*) dari *stack* protokol tujuh-lapis *OSI*. (Ryan, 2018)

Gambar 2.10 Router

(*Sumber: www.cisco.com*)

2.6.8 Personal Computer (PC)

Personal Computer adalah komputer yang dirancang untuk menyelesaikan bermacam-macam masalah dengan menggunakan program yang bermacam-macam untuk menyelesaikan jenis permasalahan-permasalahan yang berbeda seperti pengolahan kata, grafis, permainan, multimedia.Komputer jenis ini biasa digunakan di rumah, kantor atau sekolah. (Iskandar,2018)

2.7 Domain Name System (DNS)

Domain Name System (DNS) *server* merupakan sebuah layanan, pada *layer* aplikasi (model *OSI*), yang dipakai untuk menerjemahkan nama *domain* ke alamat *IP*. (Yahya dkk,2019)

2.8 Protocol

Protokol adalah suatu aturan formal dan kesepakatan yang menentukan bagaimana komputer bertukar informasi melewati sebuah media jaringan. Sebuah protokol mengimplementasikan salah satu atau lebih dari lapisan-lapisan *OSI*. (Abdullah,2015)

2.8.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP merupakan hal sangat penting bagi sistem operasi. *TCP/IP* merupakan protokol pilihan bagi sistem operasi karena peranannya sangat penting tersebut. Linux menjadikan protokol ini sebagai *default* atau pilihan. Protokol *TCP/IP* terdiri dari *TCP* yang terletak pada laporan *transport* model lapisan OSI (*Open System Interconnection*), sedangkan *IP* terletak pada lapisan *Network* model *OSI*. (Mukhtar,2019)

2.8.1.1 Physical Layer

Fungsi dari layer fisik adalah mendefinisikan media fisik dari transmisi paket data. (Ariawal dan Purbo,2016)

2.8.1.2 Link Layer

Fungsi dari *layer data link* adalah bagaimana paket *data* didistribusikan melalui media tertentu (*ethernet, hub, switch*), menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut *frame*, dan menentukan bagaimana perangkat jaringan *seperti hub, bridge, repeater* dan *switch* beroperasi. (Ariawal dan Purbo,2016)

2.8.1.3 Network Layer

Fungsi *layer network* adalah untuk mendefinisikan akhir dari pengiriman paket data, mendefinisikan *IP Address* mana yang harus dituju, dan untuk siapa pengirim paket tersebut, kemudian melakukan *routing via internetworking* melalui *router*. (Ariawal dan Purbo,2016)

2.8.1.4 Transport Layer

Fungsi dari *layer transport* adalah untuk memecah data ke dalam paket-paket data serta memeberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali di sisi tujuan setelah diterima. (Ariawal dan Purbo,2016)

2.8.1.5 Session Layer

Fungsi dari *layer session* adalah mendefinisikan bagaimana koneksi dapat dimulai, dikontrol, dan dihentikan dalam komunikasi antar-mesin. (Ariawal dan Purbo,2016)

2.8.1.6 Presentation Layer

Fungsi dari *layer* ini adalah mendefinisikan format (*JPEG,HTML*) data yang akan dikirimkan dari aplikasi menuju jaringan.Format data ini dimanipulasi sehingga dapat bisa dimengerti oleh penerima. (Ariawal dan Purbo,2016)

2.8.1.7 Application Layer

Fungsi dari *layer applications* adalah sebagai penghubung antarmuka yang mengatur bagaimana aplikasi pada komputer terhubung dengan fungsional jaringan. Protokol dalam lapisan ini adalah *HTTP, FTP, SMTP,POP3,* dan *NFS*. (Ariawal dan Purbo,2016)

2.8.2 IP Address

Protokol yang memberikan alamat atau identitas untuk peralatan di dalam jaringan.*IP Address* disebut sebagai *IP Private* dan *IP* Publik.*IP Private* adalah *IP* yang hanya bisa diakses dari jaringan lokal saja dan tidak bisa diakses melalui jaringan *internet* secara langsung tanpa bantuan *Router* (*NAT*).*IP private* digunakan untuk jaringan lokal (*LAN*) agar sesama komputer dapat saling berkomunikasi. (Alam dkk,2020)

2.9 Keamanan Jaringan

Keamanan jaringan komputer saat ini telah menjadi isu utama di dunia. Hal ini dikarenakan dunia telah semakin sempit dengan terkoneksikannya dalam sebuah *internet* sebagai *open system interconnection*. Dengan *internet* kita dapat mengakses dan berkomunikasi dengan orang lain yang letaknya sangat jauh, kita pun dapat masuk ke alamat situs orang lain dan banyak hal lainnya. Hal tersebut memang memudahkan *transfer* informasi akan tetapi juga membawa efek negatif dengan keamanan informasi kita.Berbagai macam kejadian berkaitan dengan keamanan jaringan telah terjadi dan beberapa diantaranya membawa efek negatif semisal pencurian data, pemalsuan data ataupun penghapusan data seseorang atau pun instansi. Oleh sebab itu sangatlah penting bagi seorang *administrator* untuk memahami dan mengerti tentang konsep keamanan jaringan. Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya terhadap upaya perubahan dan perusakan oleh seseorang yang tidak diizinkan. Dan tidak ada jaringan yang dapat sempurna melindungi dirinya dari bahaya pengrusakan atau intrusi orang lain. Hal tersebut disadari betul bahkan beberapa ahli di bidang jaringan komputer menyampaikan bahwa untuk melindungi komputer atau jaringan anda dengan sempurna hanya ada satu cara yakni memberikan pemisah antara komputer dan jaringan selebar 1 inchi artinya tidak ada keamanan jaringan komputer yang sempurna. (Yuliandoko, 2018)

2.9.1 Firewall

Firewall adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. (Ryan, 2018)

2.9.2 Security Port

Banyak teknik yang dapat diupayakan dalam memperkecil tingkat kejahatan dalam jaringan, salah satu teknik yang banyak digunakan untuk pengamanan jaringan lokal adalah dengan menggunakan *port security*.*Security port* merupakan teknik yang akan mengizinkan siapa saja yang berhak

menggunakan akses jaringan melalui *port* yang tersedia di *switch*. (Sulaiman, 2016)

2.9.2.1 Metode Pendaftaran MAC Address

Sulaiman (2016) menyatakan bahwa Sebuah kemampuan *switch manageable* untuk meningkatkan keamanan jaringan dengan menggunakan *port-port* yang tersedia pada *switch* tersebut. Ada 3 metode yang digunakan untuk mendaftarkan *mac-address* dari *end devices* ke dalam *switch*, yaitu :

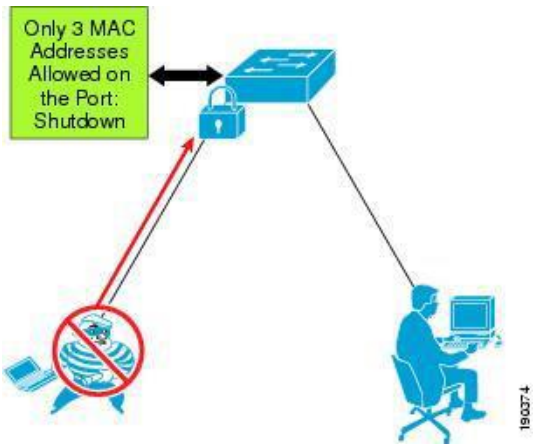
1. *Default / static port security*
2. *Port security dynamic learning*
3. *Sticky port security*

1) *Default / static port security*

Ketika *port security* ini di fungsikan maka *mac-address port security* akan diaktifkan pada *port switch*, sehingga *port* tidak akan mem-*forward packets* jika *source address* bukanlah *address* yang telah kita defenisikan/tentukan sebelumnya. menentukan alamat *mac* tertentu yang di perbolehkan untuk terhubung ke *port* tersebut secara manual.

2) *Port security dynamic learning*

MAC address di pelajari secara dinamis ketika perangkat terhubung ke *switch*, *mac-address* tersebut di simpan di *mac address table*.



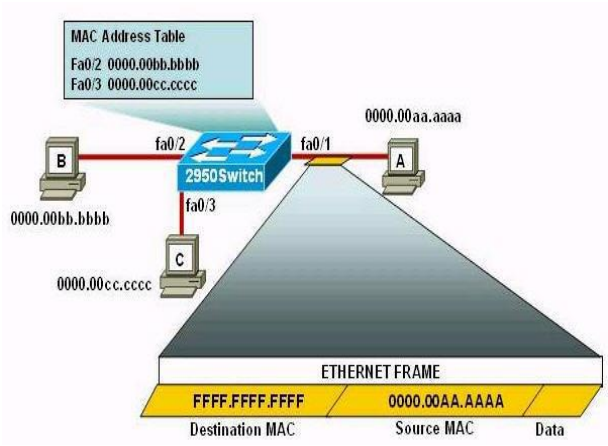
Gambar 2.11 Contoh Switch Port Security

(*Sumber: Sulaiman, 2016*)

Pada gambar tersebut terlihat bahwa pengguna jaringan menggunakan media *switch* untuk berbagi sumber daya namun *switch* tersebut mempunyai kemampuan untuk mengamankan jaringannya, pada *switch* hanya di perbolehkan 3 *MAC address* yang terhubung di *port* tersebut selain itu jika *MAC* tidak terdaftar di *MAC address table* maka tidak diizinkan untuk masuk ke jaringan tersebut.

3) Sticky Port Security

Sebuah kemampuan *switch* dalam mengenal *mac address* tiap tiap perangkat yang terhubung dan akan memblok setiap *mac* yang melebihi dari *mac* yang telah terdaftar.



Gambar 2.12 Switch Port Security

(*Sumber: Sulaiman, 2016*)

Pada gambar tersebut terlihat *switch* akan membaca *mac address* dari tiap perangkat yang terhubung dengannya, dengan menggunakan *sticky port security* maka dapat didaftarkan jumlah pemakaian perangkat yang terhubung di *switch* tersebut. Contohnya jika didaftar hanya 2 *mac* maka ketika ada perangkat yang ketiga dengan otomatis *sticky port security* akan mencegah (*blok*) *mac* tersebut , sehingga perangkat yang terhubung tetap 2 yang pertama.