BAB I
PENDAHULUAN

1.1 Latar Belakang

Spanning Tree Protocol (STP) digunakan pada peralatan *switch manageable* yang menerapkan jalur lebih dari satu untuk hubungan antar switch. Penggunaan jalur yang jumlahnya lebih dari satu ini dimaksudkan agar kecepatan perpindahan data antar switch mencapai kecepatan diatas 100 mbps. Namun akibat dapat menimbulkan *redundancy* sehingga switch melakukan pemblokiran pada jalur tersebut. Pemblokiran ini dapat dihilangkan dengan mengaktifkan STP sehingga kecepatan yang diinginkan dapat tercapai. Selain pada jalur yang lebih dari satu, *redundancy* dapat muncul pada jalur antar switch yang menggunakan VLAN untuk hubungan antar komputer pada jaringan komputer. Menurut Wiguna (2013), jaringan merupakan suatu hal pokok yang harus ada pada sebuah instansi atau perusahaan, karena dengan jaringan dapat mempermudah dalam hal pertukaran data maupun transfer data. Seiring perkembangan teknologi beberapa perusahaan, organisasi menerapkan konsep jaringan VLAN.

Menurut Ali (2015), VLAN merupakan sebuah LAN yang terkonfigurasi secara software bukan menggunakan kabel fisik. Jaringan VLAN mempunyai beberapa kelebihan yaitu dari aspek keamanan, jika suatu departemen memiliki data sensitif terpisah dari jaringan yang ada, maka akan mengurangi peluang pelanggaran hak akses ke informasi rahasia dan penting. Menurut Peniarsih (2018), *Spanning Tree Protocol* (STP) adalah *Protocol* pada jaringan yang menjamin tidak terjadinya *loop* pada *network layer* 2, di mana *loop* tersebut bisa mengakibatkan terjadinya *broadcast* pada *network*. Oleh karena itu perlu adanya *Spanning Tree Protocol* (STP) pada sebuah VLAN.

Pada penelitian Saputra dan Fajar (2017) yang berjudul "Implementasi VLAN dan *Spanning Tree Protocol* Menggunakan GNS3 dan Pengujian Sistem Keamanannya" menjelaskan implementasi jaringan VLAN dan *spanning tree protocol attack* menggunakan aplikasi GNS3 serta menguji dan meningkatkan jaringan VLAN dan *Spanning Tree Protocol* dari segi keamananya dengan teknik

mitigasi yang tepat dari jaringan VLAN dan *spanning tree protocol* apabila terjadi sebuah serangan VLAN *hopping* dan *spanning tree protocol attack*. Menurut Glackin (2015), serangan *Denial of Service* (DoS) telah diidentifikasi sebagai kerentanan yang paling umum untuk *Spanning Tree Protocol*. Selain itu juga menjelaskan *script* dengan bahasa pemograman *phyton* dengan tujuan untuk mengidentifikasi topologi jaringan *Local Area Network* (LAN) serta informasi *Spanning Tree Protocol* (STP).

Pada penelitian Zunaidhi (2012), yang berjudul "Aplikasi Peramalan Penjualan Menggunakan Metode Regresi Linier" menjelaskan cara memprediksi hasil penjualan waktu yang akan datang berdasarkan hasil dari data penjualan yang telah lalu. Salah satu metode yang digunakan dalam penelitian nya adalah metode regresi linier dengan model *time series* dengan menggunakan bahasa pemrograman visual basic 6.0. Regresi linier merupakan teknik atau metode yang banyak digunakan dalam permalan penjualan karena telah teruji ketepatan dalam peramalan.

Selain itu juga pada penelitian Hijriani dkk (2016) menjelaskan "Implementasi Metode Regresi Linier Sederhana Pada Penyajian Hasil Prediksi Pemakaian Air Bersih Pdam Way Rilau Kota Bandar Lampung Dengan Sistem Informasi Geografis*"* menjelaskan banyaknya pelanggan dan pemakaian air bersih di suatu daerah yang masuk dalam zona pelayanan PDAM Way Rilau Kota Bandar Lampung diamati sebagai informasi yang dapat digunakan dalam perencanaan produksi air bersih di masa mendatang. Hasil prediksi jumlah pelanggan dan jumlah pemakaian air bersih akan bermanfaat dalam perencanaan produksi air bersih dan peningkatan layanan kepada pelanggan. Prediksi dapat dilakukan dengan berbagai metode, salah satunya metode regresi linier sederhana. Penelitian ini dilakukan dengan tujuan untuk membangun sistem informasi geografis yang dapat menyajikan hasil prediksi pemakaian air bersih kota Bandar Lampung dalam wilayah pelayanan PDAM Way Rilau Kota Bandar Lampung. Data pada penelitian ini diperoleh dari PDAM Way Rilau Kota Bandar Lampung. Hasil keseluruhan pengujian menunjukkan bahwa sistem informasi geografis penyebaran dan prediksi

jumlah penduduk telah sesuai baik dari segi fungsionalitasnya, maupun dari segi interaksi sistem dengan pengguna.

Penelitian Siti Juairiah, R., (2017) "Analisa Lalu Lintas Jaringan Komputer Menggunakan *Wireshark* Dan *Command Prompt*" menjelaskan proses *capture* menggunakan software *wireshark* pada berita teknologi.com dan live streaming www.video.metrotv.com. Pada penelitian Saputro , W. U (2012) "Analisis Performance Jaringan Nirkabel Menggunakan Aircrack-Ng Dan Wireshark" yang berisi Industri tentang WLAN 802.11 atau WiFi (*Wireless Fidelity*) pada saat ini sedang berkembang dan sedang mendapatkan momentumnya. Berbagai macam toko, rumah sakit, bandara, mall, cafe, kantor dan tempat pendidikan sudah banyak memanfaatkan teknologi WiFi untuk berkomunikasi. Teknologi ini digunakan karena mobilitas dan produktivitas tinggi sehingga memudahkan penggunanya dalam berkomunikasi tanpa koneksi fisik. WLAN memungkinkan client untuk mengakses informasi secara realtime sepanjang masih dalam jangkauan WLAN, sehingga meningkatkan kualitas layanan dan produktivitas. Pengguna bisa melakukan kerja dimanapun berada asal dilokasi tersebut masuk dalam *coverage* area WLAN. Kekuatan sinyal juga sangat berpengaruh dalam hal pertukaran data, karena jika terjadi hal sinyal pada jaringan *hotsport full* tapi kekuatan *download* dan *upload* lemah maka dapat disimpulkan beberapa penyebabnya diantaranya adalah : banyak yang mengunakan jaringan tersebut, alat rusak, atau juga jaringan digunakan oleh pihak itu. *Aircrack-ng* dan *wireshark* adalah salah satu *software* yang berbasis open source. Software ini terbilang baru dan masih jarang digunakan oleh banyak orang.

Penelitian yang dilakukan Diansyah, T. M., (2015) yang berjudul " Analisa pencegahan aktivitas *illegal* didalam jaringan menggunakan *wireshark*" yang berisi Faktor kemanan jaringan komputer merupakan satu hal yang mutlak dalam membangun suatu jaringan. Pada dasarnya sistem keamanan yang dimiliki oleh sistem operasi tidaklah cukup untuk mengamankan jaringan komputer. Oleh karena itu untuk mendapatkan sebuah keamanan jaringan komputer maka diperlukan suatu *tools* yang dapat mendeteksi adanya suatu mekanisme serangan dari jaringan. Jenis serangan yang terjadi bias *flood*ing ataupun syn *flood*. Dimana tujuan serangan ini

adalah untuk membuat komputer yang mengakses tidak bisa berjalan dengan normal sehingga *wireshark* ini dapat membantu untuk mendeteksi serangan yang akan terjadi sehingga pengguna jaringan internet tidak khawatir dengan serangan tersebut.

Selain itu juga pada penelitian Yuvandra dan Zulfin (2013), juga menjelaskan "Analisa Kinerja Trafik Video Chatting Pada System Client-Client Dengan Aplikasi Wireshark. Menjelaskan Teknologi *Video chat* adalah salah satu media komunikasi yang memberikan kemudahan pengguna untuk dapat melihat wajah lawan bicara dalam *chatting* dengan menggunakan kamera yang terdapat di notebook atau perangkat komputer. *Video chat* juga membutuhkan jaringan *internet* sebagai media transmisinya. Salah satu aplikasi untuk *video chat* adalah skype. Skype adalah *software* aplikasi komunikasi suara berbasis IP dengan teknologi P2P (*peer to peer*) melalui *internet* antara sesama pengguna Skype. Paper ini membahas tentang pengaruh lamanya waktu *chatting* antara *client* A dengan *client* B berdasarkan pengujian yang dilakukan. Pengujian dilakukan dengan pengcapturan data menggunakan *software wireshark*. Parameter QoS yang dianalisis berupa *delay*, *packet loss* dan *throughput.* Hasil analisa data dari percobaan yang dilakukan menunjukkan bahwa pada saat melakukan *video chat* diperoleh *delay* rata-rata sebesar 0,72 sec, *packet loss* yang bernilai 0 %, sedangkan nilai *throughput*nya akan semakin turun seiring dengan lamanya waktu *chatting*.

Pada penelitian Saleh, I. A (2018) "Perancangan Jaringan Berbasis *Etherchannel* dan *Spanning Tree Protocol* (STP) Untuk Modul Praktikum Di Laboratorium D3-Elektronika Universitas Muhammadiyah Malang*"* Pertumbuhan kebutuhan layanan jaringan internet dan intranet saat ini telah membuat lalu lintas pertukaran data informasi serta kebutuhan akan kehandalan perangkat jaringan dan infrastruktur yang ada, maka dari itu *frame* yang *looping* tanpa henti didalam network yang menyebabkan terganggunya kinerja network. Topologi *EtherChannel* juga menyediakan bandwidht yang lebih banyak dan topologi *Spanning Tree Protocol* (STP) menyediakan jalur cadangan otomatis sehingga gabungan topologi *EtherChannel* dan *Spanning Tree Protocol* (STP) dapat mengurangi *looping* didalam network. Di dalam perancangan ini ada beberapa

analisa untuk menghitung parameter jaringan yang menggunakan system QOS (*Quality Of Service*). Perhitungan parameter QOS meliputi throughput, packet loss, dan delay untuk mengetahui kinerja jaringan yang telah dibuat. Metode pengumpulan data yang digunakan dengan metode monitoring jaringan dengan *software wireshark.*

Pada penelitian Widodo, S (2012) yang berjudul " Pemantauan Jaringan Komputer dengan DNS Server Berbasis Routing Statis Menggunakan *Wireshark*" menjelaskan tentang beberapa hal yang perlu mendapat perhatian dalam merancang jaringan komputer adalah *collision domain* dan *broadcast domain*, sehingga ketika diimplementasikan tidak muncul permasalahan di kemudian hari. *Colision domain* perlu diatasi dengan pemakaian perangkat seperti switch sehingga hanya memiliki satu *collision domain* saja. Jaringan komputer yang hanya mengandalkan sejumlah switch untuk jaringan yang besar sangat berdampak pada *broadcast domain*, untuk itu perlu sejumlah router untuk memisahkan *broadcast domain*nya, seperti penggunaan routing statis dalam perancangan jaringan komputer yang tidak kompleks. Kinerja jaringan komputer dapat dipantau dengan penganalisis jaringan seperti *wireshark*. *Wireshark* adalah penganalisa paket yang digunakan untuk pemecahan masalah, analisis, dan pengembangan protokol komunikasi. Rancangan jaringan dengan server DNS dibuat dengan routing statis, membuat tabel routing dan mengkonfigurasi router. Menguji koneksi ke DNS dan proses pemantauan jaringan. Pemantauan yang dilakukan dengan menggunakan *wireshark* menunjukkan jaringan komputer bekerja dengan baik.

Penelitian Balogh, Z., dkk (2018), yang berjudul "*LAN security analysis and design"* Jaringan komputer adalah sistem yang sempurna untuk komputer yang terhubung dan bekerja sama. Ini membentuk dasar bagi banyak orang sistem lain. Tujuan dari makalah ini adalah untuk menganalisis dan mengusulkan keamanan untuk jaringan komputer lokal. Tujuan dari analisis ini adalah untuk buat ikhtisar ringkas tentang informasi yang penting bagi memahami potensi risiko dan ancaman di komputer jaringan. Dalam studi kasus, melakukan simulasi serangan. Faktor terpenting yang perlu diperhatikan saat mendefinisikan keamanan LAN menjaga kerahasiaan, integritas, ketersediaan informasi dan keaslian. Cara

melindungi lalu lintas jaringan dengan menggunakan enskripsi SSL atau *Transport Layer Security* (TLS). Sniffer merupakan alat untuk mendiagnosis masalah jaringan. Serangan LAN yaitu *SPOOFING* ARP , ARP *Poison Routing*, ARP *Poison Cache*. Serangan MITM seorang mendapatkan 2 perangkat dalam berkomunikasi kemudian menganalisis, mengubah komunikasi ke penerima.

Pada penelitian Adriant dkk (2016) "Implementasi wireshark untuk penyadapan (*sniffing*) paket data jaringan" Saat ini perkembangan teknologi informasi berkembang dengan sangat pesat, yang menyebabkan isu keamanan informasi menjadi penting. Proses penyadapan informasi (*Sniffing*) pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang bersifat positif maupun yang bersifat sebaliknya. Keamanan Informasi adalah segala usaha perlindungan informasi, terhadap akses atau modifikasi data dan informasi yang tidak sah yang dapat terjadi pada media penyimpanan atau pada saat transmisi data. Dalam penelitian ini, proses *sniffing* digunakan untuk mendapatkan informasi *username* dan *password*. Proses *sniffing* dilakukan menggunakan perangkat lunak Wireshark. So*ftware* Wireshark melakukan proses capturing data pada *interface Wireless*, lalu mengamati hasil *capture*-an yang berisikan data POST yang berisi *username* dan *password* pada HTTP. Dari hasil penelitian yang dilakukan didapatkan bahwa dengan menggunakan Wireshark dapat melakukan penyadapan atau pengendusan data yang lewat pada jaringan komputer, hal ini mengakibatkan hilangnya salah satu sifat keamanan yaitu *privacy* dan *confidentiality*.

Dari aspek keamanan, meskipun jaringan *Spanning Tree Protocol* (STP) memiliki tingkat keamanan yang cukup baik tetapi perlu diuji dengan melakukan serangan dari pihak luar seperti pada penelitian sebelumnya. Dari latar belakang maka dilakukan penelitian dengan judul "Analisis Kinerja Jaringan Komputer Berbasis *Spanning Tree Protocol* (STP) Terhadap Serangan *Config BPDU* dan *Take Over Root Bridge* Menggunakan *Wireshark".*

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dirumuskan permasalahan yaitu bagaimana mengamati, mendapatkan data dan mengelola data dari *wireshark* pada jaringan komputer berbasis *Spanning Tree Protocol* (STP).

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disebutkan, maka dapat didapatkan batasan masalah sebagai berikut:

1. Penelitian ini menggunakan aplikasi *wireshark* sebagai analisis paket data dan Tool *Yersinia* untuk melakukan serangan *Spanning Tree Protocol Attack.*
2. Membahas sistem keamanan jaringan *Spanning Tree Protocol* (STP)
3. Menggunakan metode serangan *Spanning Tree Protocol Attack* yaitu DoS *(Denial of Service) using flood config Bridge Protocol Data Unit (BPDU)* dan *Take over Root bridge* .
4. Menggunakan teknik mitigasi pada jaringan *Spanning Tree Protocol* (STP) untuk mengatasi serangan STP *attack.*
5. Analisis ini menggunakan analisis regresi linier sederhana (*simple linier regression*).
6. Aplikasi analisis STP berbasis website yang dibuat tanpa menggunakan *database*

1.4 Tujuan dan Manfaat Penelitian

Penelitian dengan judul "Analisis Kinerja Jaringan Komputer Berbasis *Spanning Tree Protocol* (STP) Terhadap Serangan *Config BPDU* dan *Take Over Root Bridge* Menggunakan *Wireshark"* mempunyai tujuan untuk membantu *staff engineer* dalam meningkatkan sebuah keamanan jaringan *Spanning Tree Protocol* (STP). Serta manfaatnya untuk meningkatkan sistem keamanan jaringan *Spanning Tree Protocol* (STP) dengan menggunakan teknik mitigasi *Spanning Tree Protocol* (STP).

1.5 Metode Penelitian

Metode penelitian yang digunakan dalam menyelesaikan tugas akhir ini adalah metode penelitian kuantitatif yang dilakukan dengan:

1. Metode Pengumpulan Data

   Metode-motode pengumpulan data yang digunakan dalam penelitian ini yaitu : Metode dokumentasi, Metode kepustakaan, install software wireshark dan packet tracer. Hasil dari pengumpulan data ini akan menjadi data yang akan dianalisis.

2. Pengujian hipotesis

   Pada penelitian ini digunakan untuk mengetahui apakah ada perbedaan yang signifikan antara STP sebelum diserang dengan STP setelah dilakukan serangan.

3. Analisis Hasil

   Berdasarkan dua teknik antisipasi yang dilakukan tidak bisa menghilangkan sebuah serangan sehingga dibutuhkan teknik selanjutnya yang dikaji dan teliti dengan membuat VLAN trunking.