BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digitalisasi saat ini, teknologi memegang peranan penting kelangsungan hidup manusia dalam aktivitas sehari-hari tidak lepas dari teknologi. masalah ini berubah dari cara berpikir menjadi acuan bagi kemajuan peradaban manusia dan menangani dan memecahkan setiap masalah pola pikir yang kompleks agar tidak tersesat dengan perkembangan dan dukungan teknologi informasi didukung oleh berbagai penemuan dan inovasi banyak perubahan dalam hidup seseorang. Itu juga menyebabkan pengembangan bersama pembangunan dan teknologi Perangkat keras, secara langsung atau tidak langsung Informasi telah menjadi bagian penting dalam berbagai aspek kehidupan untuk dukungan sederhana tenaga kerja manusia. Departemen TI seringkali bertanggung jawab untuk mengelola dan menjaga keamanan data sensitif seperti informasi karyawan, informasi pelanggan, atau data bisnis penting lainnya. Monitoring dan pencegahan akses ilegal membantu mencegah upaya pencurian atau pengungkapan data yang tidak sah di PT Pupuk Sriwidjaja (PUSRI).

Teknologi informasi memudahkan manusia berbagi informasi atau mencari informasi. kamu bisa melihatnya Tentang perkembangan teknologi internet dan jaringan. Baru-baru ini *internet* adalah untuk pertukaran informasi dan untuk mencari informasi. Jaringan komputer adalah suatu sistem yang terdiri dari dari beberapa komputer yang dirancang untuk pertukaran data, informasi dan sumber daya. Jaringan

komputer adalah suatu sistem yang terdiri dari dari beberapa komputer yang dirancang untuk pertukaran data, informasi dan sumber daya. Tujuan dari jaringan komputer adalah Setiap bagian dari jaringan komputer dapat meminta dan menyediakan layanan informasi dan data. Pihak yang meminta atau menerima layanan kepada siapa pelanggan merujuk dan siapa yang mengirim atau menyampaikan layanan disebut *server*.

Serangan siber seperti serangan *malware* atau upaya peretasan merupakan ancaman serius bagi jaringan TI. Dengan memantau lalu lintas jaringan dan menerapkan tindakan pencegahan yang tepat, departemen TI dapat mengidentifikasi serangan yang sedang berlangsung dan mengambil tindakan untuk menghentikannya sebelum menjadi sangat merusak bagi perusahaan. Pada pasal 30 ayat 1 UU ITE No 19 Tahun 2016 ,Perbuatan ini dapat dikategorikan yang dinyatakan dalam Pasal 30 ayat (1) UU ITE yaitu setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.

Tujuan dari keamanan jaringan adalah untuk mengantisipasi resiko ancaman jaringan yang dapat mengganggu operasional jaringan komputer sehari-hari. Nirkabel diperlukan di kantor karena nirkabel dapat membantu menyelesaikan pekerjaan. Perkembangan teknologi *Wireless Fidelity* (*WI-FI*) mengalami kemajuan yang sangat pesat untuk memenuhi kebutuhan sistem. Teknologi *WI-FI* banyak digunakan pada *hotspot* komersial, keamanan jaringan Internet *Service Provider* (*ISP*) di sekolah dan perkantoran sangat penting, namun hanya sebagian operator jaringan saja yang memperhatikan keamanan lalu lintas data pada jaringan *WI-FI.* Salah satu ancaman

keamanan jaringan paling umum yang ditimbulkan oleh penjahat dunia maya adalah serangan paket. *Sniffing* paket adalah bentuk serangan yang menangkap data dari paket yang melintasi jaringan. Informasi ini mungkin termasuk nama pengguna, kata sandi, dan informasi penting lainnya yang dikirimkan melalui jaringan dalam bentuk teks. Tidak hanya satu paket yang harus ditangkap, bisa ratusan bahkan ribuan. Hal ini dapat merugikan pengguna jaringan komputer. Sero, R. L. (2022).

Dalam lingkungan TI yang kompleks, penggunaan ilegal atau aktivitas jaringan yang mencurigakan dapat mengganggu ketersediaan sistem. Dengan menggunakan solusi pemantauan yang tepat, departemen TI dapat mengidentifikasi masalah dan kesalahan jaringan dengan lebih cepat dan mengambil tindakan segera untuk menjaga ketersediaan sistem, Serangan yang berhasil dapat mengakibatkan gangguan pada proses bisnis. Mengontrol dan mencegah penggunaan ilegal dapat meminimalkan risiko kerusakan finansial dan reputasi yang mungkin diakibatkan oleh serangan atau pelanggaran keamanan.

Dalam penelitian ini penulis melakukan penelitian dengan menggunakan metode Action Research yang bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara-cara pendekatan baru dan untuk memecahkan masalah dengan cara penerapan langsung pada objek penelitian. Febriani, Y., & Sahfitri, V. (2022, August).

Sehubungan dengan hal tersebut di atas PT. Pupuk Sriwidjaja Palembang di perlukannya melakukan *monitoring* dan pencegahan dari akses illegal pada jaringan menggunakan *wireshark. Administrator* jaringan dapat mengabil tindakan

penaggulangan ketika akses illegal terdeteksi melalui jaringan kompouter akses illegal yang di maksud adalah seperti pengguna atau user membuka situs atau webstie yang berbahaya dan tingkat keamanannya sangat lemah, Oleh karena itu *administrator* memerlukan alat yang tepat untuk memantau jaringan yaitu *wireshark, Software Wireshark* karena alat ini mampu menagkap paket data atau informasi dan sekaligus memantau lalu lintas antara Wlan (*Wireless Local area Network*). Febriani, Y., & Sahfitri, V. (2022, August).

Berdasarkan yang di jelaskan di latar belakang penulis tertarik memonitor dan mencegah akses illegal di dalam jaringan, department TI dapat meningkatkan keamanan jaringan, melindungi data sensitif, mengurangi resiko serangan siber dan menjaga kelangsungan bisnis organisasi yang berjudul ***"Monitoring Dan pencegahan Akses Ilegal Di Dalam Jaringan Pada Departemen TI Di PT Pupuk Sriwidjaja"***

1.2 Rumusan Masalah

Berdasarkan dari latar belakang di atas, dirumuskan masalah pokok penelitian adalah "Bagaimana *Monitoring* jaringan dari akses ilegal pada PT Pupuk sriwidjaja dari akses ilegal Menggunakan *Wireshark*"?.

1.3 Batasan masalah

Dengan rumusan masalah tersebut maka akan di buat dengan batasan masalah sebagai berikut:

1.Monitoring dengan menggunakan wireshark dapat dibatasi hanya pada perangkat yang dapat di akses dari titik wifi tertentu

2. Pada jaringan widi di gedung anex PT.Pupuk Sriwidjaja, monitoring hanya pada jaringan yang diidentifikasi dengan SSID tertentu yang ada di gedung tersebut

3. Waktu yang di gunakan dalam monitoring dari tanggal 6 juni – 21 juni 2023 juga bisa menjadi pertimbangan untuk melakukan monitoring lalu lintas jaringan pada gedung tersebut.

1.4 Tujuan Dan Manfaat Penelitian

1.4.1 Tujuan penelitian

Adapun tujuan penelitian ini adalah untuk memonitoring jaringan di PT Pupuk Sriwidjaja dari akses illegal menggunakan *wireshark*

1.4.2 Manfaat penelitian

Wireshark memungkinkan kita untuk menganalisis lalu lintas jaringan secara mendalam. Dengan melihat paket data yang dikirim dan diterima, Kita dapat mengidentifikasi masalah jaringan seperti kegagalan koneksi, latensi tinggi, atau paket yang hilang.

Wireshark dapat digunakan untuk mendeteksi ancaman keamanan jaringan. Kita dapat melihat aktivitas yang mencurigakan, pencobaan penetrasi, atau serangan

jaringan lainnya. Ini dapat membantu Kita merespons cepat untuk mengatasi ancaman keamanan sebelum mereka menyebabkan kerusakan lebih lanjut.

Kita dapat menggunakan Wireshark untuk menganalisis lalu lintas web yang melintasi jaringan Kita. Ini dapat membantu dalam mendeteksi ancaman keamanan web, memeriksa kinerja situs web, dan mengidentifikasi permintaan atau tanggapan HTTP yang bermasalah.

1. Manfaat Bagi Penulis

   Penulis dapat mengimplementasikan ilmu penegtahuan yang dimilikinya yang di dapat dari perkuliahan.

2. Manfaat Terhadap Lokasi Penelitian

   Di harapkan dengan adanya penelitian ini, maka menjadi bahan referensi bagi lokasi yg di pakai untuk penelitian, agar dapat mengoptimalkan system keamanan jaringan dengan memanfaatkan *tools* bantuan seperti *wireshark* dalam memonitoring lalu lintas jaringan , yang juga dapat di gunakan untuk mengcapture hasil dari *Monitoring* paket data yang keluar dan masuk pada jaringan , Serta biasa memberikan gambaran sebuah system yang berjalan dengan baik, di tinjau dari segi keamanan jaringan itu sendiri.

3. Manfaat Terhadap Dunia Akademis

   Penelitian Ini dapat di jadikan bahan atau *referensi* dalam penelitian selanjutnya tentang sistem keamanan jaringan Komputer.

1.5 Penelitian Terdahulu

Penelitian terdahulu merupakan upaya penelitian untuk mencari pembanding kemudian menemukan inspirasi baru untuk penelitian selanjutnya.Selain itu. Penlitian sebelumnya membantu mempromosikan peneilitian dan menunjukan *orisinalitas* penelitian.

1. Penelitian terdahulu ini di ambil dari jurnal yang di tulis oleh bapak Abdul Majid dan Bapak Timur Dali Purwanto, Pada penelitian ini penulis menggunkan sebuah metode action research, Metedo action research ini memeiliki beberapa tahapan yaitu.

1. Melakukan Diagnosa *(Diagnosing)*
2. Membuat rencana tindakan *(Action planning)*
3. Melakukan tindakan *(Action Tacking)*
4. Melakukan evaluasi *(Evaluating)*
5. Pembelajaran *(learning)*

2. Penelitian terdahulu ini di ambil dari jurnal yang di tulis oleh Yesi Febriani dan Vivi Sahfitri, Dalam penelitian ini penulis melakukan penelitian dengan menggunakan metode Action Research yang bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara-cara pendekatan baru dan untuk memecahkan masalah dengan cara penerapan langsung pada objek penelitian.

1.Melakukan Diagnosa (Diagnosing) Setelah melakukan magang pada Kantor Dinas ESDM Prov. Sumsel, peneliti melakukan diagnosa setelah melihat beberapa pengawai mencoba login pada halaman web yang belum tentu memiliki standar keamanan. Sehingga dapat memungkinkan bila informasi pribadi seperti password atau e-mail dapat terdeksi. Bila info penting seperti e-mail pengguna internet dapat terdeksi bahkan bila e-mail tersebut bersangkutan dengan banyak akun lainya, itu dapat mebahayakan lebih merugikan pengguna internet sehingga dapat disalah gunakanolehoranglain. 2 Membuat Rencana Tindakan (ActionPlanning) Pada tahap ini penulis berencana membuat tindakan pada Kantor Dinas ESDM Sumatera Selatan, berikut ini rencana tindakan meliputi :

1) Memonitoring menggunakan dua software yaitu Wireshark dan Microsft Network Monitor selama 14 hari dimulai pada tanggal 15 Maret sampai 30 Maret(terpotong hari minggu)

2) Menyimpan hasil rekaman traffic data setiap tanggalnya menggunakan Wireshark

3) Mengecek hasil rekaman membaca apakah terdapat sniffing atau tidak dengan cara melalui TCP Stream dan dilihat apakah traffic data terenkripsi atau tidak, dan mencari data penting pengguna internet

4) Membandingkan kedua software yang digunakan, manakah yang lebih baik

5) Menginformasikan bahwa ada data pengguna internet yang telah tersniffing. 3. Melakukan Evaluasi (Evaluating)

Peneliti melakukan evalusi dan penrikan kesimpulan dari monitoring yang telah dilakukan pada Kantor Dinas ESDM Sumatera Selatan. Dapat dilihat dari hasil rekaman traffic data yang merekam banyaknya aktivitas yang saling bercakapan dan juga dapat diketahui pengguna intrnet yang pergi ke suatu halaman web, penulis juga membeda rekaman data mana yang terjadi sniffing dengan cara menganalisis menggunakan menu TCP Stream yang ada pada software Wireshark.