ANALISA MONITORING UNTUK PENCEGAHAN AKSES ILEGAL DI DALAM JARINGAN DEPARTEMENT TI PT.PUSRI

MONITORING ANALYSIS FOR THE PREVENTION OF ILLEGAL ACCESS WITHIN THE NETWORK OF THE IT DEPARTMENT OF PT. PUSRI

M.Alzi Ikrar Agamuri[1], Tamsir Ariyadi M.Kom[2],
[1,2,3]Universitas Bina Darma Palembang
E-mail: [1]Alziikrar@gmail.com, [2]penulis.2@email.ac.id,

Abstrak

Teknologi memegang peranan penting kelangsungan hidup manusia dalam aktivitas sehari-hari tidak lepas dari teknologi. Teknologi informasi memudahkan manusia berbagi informasi atau mencari informasi.Serangan siber seperti serangan *malware* atau upaya peretasan merupakan ancaman serius bagi jaringan TI. Tujuan dari keamanan jaringan adalah untuk mengantisipasi resiko ancaman jaringan yang dapat mengganggu operasional jaringan komputer sehari-hari. Dalam penelitian kali ini penulis menggunakan metode *Action Research*.Davison, ini di bertujuan untuk pengujian dan pengembangan, menemukan dan merancang. Jaringan pada Departement TI PT. Pupuk Srwidjaja Palembang sudah cukup aman di karenakan pada saat di lakukannya monitoring jaringan selama 10 hari pada tanngal 6 juni 2023 sampai dengan 22 juni 2023 tidak ada terjadinya akses illegal.

Kata Kunci : Wireshark, Monitoring, Teknologi, PT.Pusri

Abstract

Technology plays an important role in human survival in daily activities cannot be separated from technology. Information technology makes it easy for humans to share information or find information. Cyberattacks such as malware attacks or hacking attempts pose a serious threat to IT networks. The purpose of network security is to anticipate the risk of network threats that can disrupt daily computer network operations. In this study, the author used the Action Research method. Davison, this in aimed at testing and development, invented and designed. Network at the IT Department of PT. Pupuk Srwidjaja Palembang is quite safe because at the time of network monitoring for 10 days from June 6, 2023 to June 22, 2023 there was no illegal access..

Keywords : Wireshark, Monitoring, Technology, PT. Pusri

1. PENDAHULUAN

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).

2. METODE PENELITIAN

2.1 Monitoring

Monitoring merupakan aktivitas mengumpulkan dan menganalisis data berdasarkan faktor yang ditetapkan secara teratur kemudian berlanjutan pada aktivitas program sehingga bisa melakukan tindakan koreksi untuk menyempurnakan aktivitas program tersebut

2.2 Analisis

Analisis adalah kegiatan untuk mencari pola, atau cara berpikir yang berkaitan dengan pengujian secara sistematis terhadap sesuatu untuk menentukan bagian, hubungan antar bagian, serta hubungannya dengan keseluruhan.

2.3 Pengertian mencegah

Menurut Kamus Besar Bahasa Indonesia (KBBI), kata mencegah /me•cegah/ dapat didefinisikan sebagai berikut.

1) Mengikhtiarkan supaya jangan terjadi
2) Merintangi; melarang
3) Menahan agar sesuatu tidak terjadi; menegahkan; tidak menurutkan

2.4 Wireless

Wireless atau yang dikenal dengan jaringan nirkabel wireless atau wireless Network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Teknologi wireless adalah salah satu pilihan yang tepat untuk menggantikan teknologi jaringan yang terdiri dari banyak kabel dan merupakan sebuah solusi akibat jarak antar jaringan yang tidak mungkin dihubungkan melalui kabel. Keuntungan terbesar dari wireless yaitu sangat praktis, dimana komputer dapat terhubung ke jaringan tanpa membutuhkan kabel.

2.5 Web Traffic

Traffic pada website merupakan jumlah orang yang mengunjungi website, membuka halaman website, dan durasi saat pengunjung membuka dan membaca halaman pada website kamu. Jadi, saat seseorang mengunjungi website kamu, kunjungan serta semua link yang mereka klik dan follow akan direkam oleh domain kamu. Nantinya angka-angka akan memberi ide tentang seberapa populernya website kamu.

2.6 Cyber Crime

Cyber Crime merupakan aktivitas individu maupun kelompok yang mengguakan jaringan komputer sebagai media untuk melakukan tindakan kriminal, atau menjadikan komputer sebagai sasaran kejahatan

2.7 Jaringan Komputer

Jaringan Komputer merupakan hubungan dengan beberapa perangkat yang bisa saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup komputer desktop, samrthphone, tablet, router, switch, dan hub

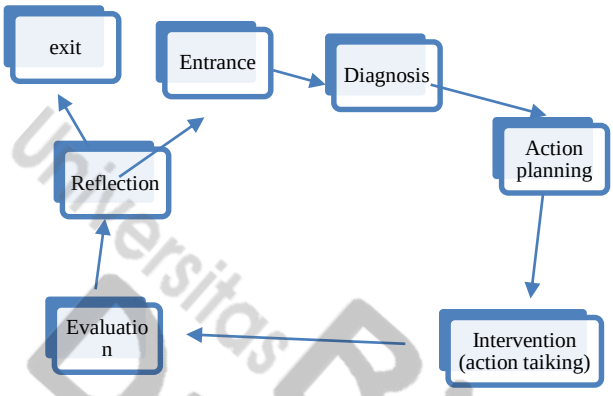
2.8 Keamanan Jaringan

Keamanan jaringan yang terkendalinya atas akses penggunaan jaringannya dimana seseorang dapat mengakses jaringan dan dikendalikan oleh siapapun yang berhak juga bisa menghalangi subjek maupun orang asing yang tidak memilki hak untuk masuk ke dalam jaringan.

2.9 Wireshark

Wireshark merupakan tool yang ditunjukan untuk menganalisa paket data jaringan, Wireshark juga disebut Network Packet Analyzer yang memilki fungsi untuk menangkap paket data dalam jaringan dan berusaha memperlihatkan informasi dipaket tersebut secara rinci.

2.10 Dalam penelitian kali ini penulis menggunakan metode Action Research



Gambar 1. Metode *Action Research*

Davison, et al (2004)Metode *Reaction Research* ini di bertujuan untuk pengujian dan pengembangan, menemukan dan merancang, langkah-langkah ini diterapkan di tempat kerja (Objek), Dengan menggunakan metode ini pekerjaan akan menjadi lebih muda, lebih cepat dan hasilnya lebih baik dan lenih berkualitas.

2.11 Diagnose (Diagnosis)

Setelah melaksanakan magang di PT Pupuk Sriwidjaja Palembamg, Peneliti Melakukan diagnosis setelah melihat beberapa karyawan mencoba masuk ke situs *web* yang mungkin belum memiliki standar keamanan, sehingga informasi pribadi seperti *Pasword* atau *email* dapat di kenali, Jika informasi penting seperti alamat email pengguna internet dapat di dideteksi meskipun email tersebut di tautkan ke banyak akun lain, ini dapat lebih berbahaya bagi pengguna unternet dan memungkinkan orang lain untuk menyalahgunakan.

2.12 Alat Alat yang Digunakan Topologi Pada PT. Pupuk Srwiridjaja

a. Router

Router merupakan salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau internet menuju sasaran,melalui sebuah proses yang di kenal sebagai routing, Router berfungsi sebagai penghubung antar 2 (dua) atau lebih jaringan untuk meneruskan daa dari satu jaringan ke jaringan lainnya (Mhd. Dicky Syahpura LUBIS, dkk, 2020).

b. Proxy

Proxy adalah sistem yang menengahi pengguna dan internet untuk menyembunyikan identitas asli pengguna, sehingga data yang dikirim ke website tujuan akan menggunakan alamat IP dari proxy server, bukan alamat IP pengguna. (HeruKurniawan, dkk, 2020).

c. Hub

Hub adalah perangkat jaringan yang memungkinkan Anda menghubungkan beberapa PC ke satu jaringan. Perangkat ini digunakan untuk menghubungkan segmen

LAN. Sebuah hub memiliki berbagai macam port, jadi ketika sebuah paket tiba di satu port, itu disalin ke berbagai port lainnya. (Rizky Amanda, dkk, 2020).

d. Switch

switch adalah sebuah komponen jaringan yang tugasnya untuk menghubungkan beberapa perangkat, untuk bisa melakukan pertukaran paket data, baik dalam proses penerimaan, serta meneruskan data ke perangkat lain.(Desmira, dkk, 2020).

e. Kabel UTP

UTP merupakan singkatan dari Unshield Twisted Pair. Sesuai namanya "Unshield", yang berarti kabel ini tidak dilengkapi dengan pelindung aluminium sehingga jenis kabel ini kurang tahan dengan interferensi elektromagnetik, berbeda dengan saudaranya STP (Shield Twisted Pair).(Bobi Agustian, Muhammad Yasser Arafat,2020).

f. Kabel Fiber Optic

Fiber Optik adalah saluran transmisi atau sejenis kabel yang terbuat dari kaca atau plastik yang sangat halus dan lebih kecil dari sehelai rambut, dan dapat digunakan untuk mentransmisikan sinyal cahaya dari suatu tempat ke tempat lain. Sumber cahaya yang digunakan biasanya adalah laser atau LED.(Amalia Rizqi Utami, dkk, 2020).

g. Kabel Koaksil

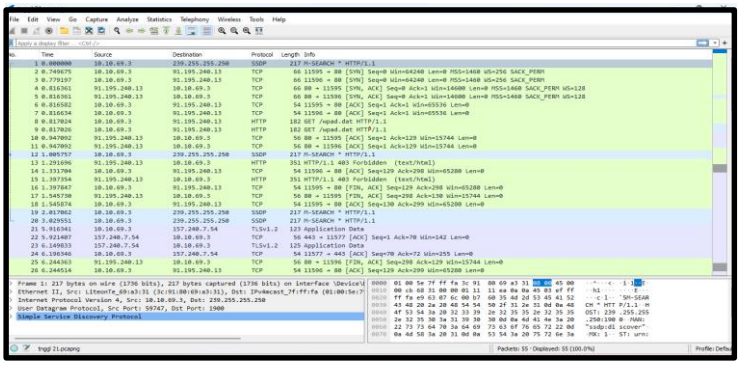
Kabel coaxial merupakan kabel yang mempunyai 2 konduktor yakni copper pada bagian tengahnya atau pusat inti yang terbuat dari tembaga bertekstur keras dan dilapisi dengan isolator. Sementara konduktor kedua adalah yang melingkar pada bagian luar isolator pertama serta tertutup dengan insulator luar.(Anisa Yulia Haryanti, dkk, 2021)

3. HASIL DAN PEMBAHASAN

3.1 Filtering Protokol HTTP

Disini penulis akan mmelakukan filtering paket data yang melewati protokol http pada beberapa jaringan yang ada di PT.Pupuk Sriwidjaja Palembang, selanjutnya ketikkan http pada kolom addres filter.

1. capturing filtering pada jaringan pusri.id new



Gambar 2.filtering protocol http

Bisa di analisis user-agent yang di pakai pada jaringan Pusri.id New menggunkan Mozilla/5.0 (windows NT 10.0; WIN 64; x64) AppleWebKit/537.36 (KHTML, Like gecko) Chrome/115.0.0.0 Safari /537/36 Dan Host mysql - phi – intergration.com, Selain itu dapat di ketahui date yaitu 22 juni 2023 01:32 41 GMT DAN Full Request Get Uri Http, Disini bisa di

lihat bahwa adanya aktivitas yang sedang mengakses laman web Gambar Capture TCP Stream Wireshark dibahwa ini dapat melihat info get yang sedang di buka

Gambar 3. *Tcp Stream*

Tabel 1. Website yang di akses pengguna pada jaringan PT.Pusri

NO	Website Yang Di Aksses	Jenis Brwoser
1	http.//mysql-phi-integration	Google Mozila
2	Blog.spot.com	Google Mozila
3	www.msftconnecttest.com,	Google Mozila
4	ocsp,pki.goog	Google Mozila

Tabel 2. data ip akses *protocol http*

TIME	SOURCE	DESTNATION	PROTOCOL
0.069188	10.10.69.3	91.195.240.13	HTTP
650.037090	103.121.18.202	192.168.11.17	HTTP
86.281421	10.10.70.97	142.251.12.94	HTTP
72.863219	10.10.69.3	204.79.197.203	HTTP

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Adapun penelitian pada jaringan di Departement TI PT. Pupuk Sriwidjaja Palembang adalah sebagai berikut.

1. Jaringan pada Departement TI PT. Pupuk Srwidjaja Palembang sudah cukup aman di karenakan pada saat di lakukannya monitoring jaringan selama 10 hari pada tanngal 6 juni 2023 sampai dengan 22 juni 2023 tidak ada terjadinya akses illegal.
2. Wireshark memiliki keunggulan pada bagian *sniffing* di bandingkan software monitoring lainnya dan wiresahrk juga dapat membaca hasil *capture* dari *software monitoring* lainnya.
3. Wireshark adalah sebuah perangkat lunak yang dapat melakukan *Monitoring traffic* jaringan sekaligus *sniffing* , Namun tidak berlaku untuk semua *website* di karenakan beberpa website sudah terenkripsi dengan baik.

Kesimpulan harus mengindikasi secara jelas hasil-hasil yang diperoleh, kelebihan dan kekurangannya, serta kemungkinan pengembangan selanjutnya. Kesimpulan dapat berupa paragraf, namun dapat juga berbentuk poin-poin dengan menggunakan numbering atau bullet. Saran-saran untuk untuk penelitian lebih lanjut untuk menutup kekurangan penelitian.

4.2 Saran

Dari penelitian ini penulis menyarankan beberapa hal yang berkaitan dengan software monitoring, dan sniffing di antaranya:

1. Meskipun wireshark dapat melakukan sniffing, alangkah baiknya jika di gunakan untuk kepentingan yang baik atau positif seperti dengan mengetahui kekurangan dari suatu keamanan tertentu dapat lebih di tingkatkan lagi keamanan jaringannya.
2. Untuk menhindari sniffing dapat dapat menggunakan keamanan firewall yang dapat menutup traffic yang datanf baik incoming network traffic maupunoutgoing network traffic berdasarkan sumber atau tujuan traffic tersebut.
3. Selain itu dapat menggunakan protocol yang memiliki standar aman yangsudah di lengkapi dengan enkripsi data seperti IPSec, HTTPS, SMB Signing, dan sebagainya.

UCAPAN TERIMA KASIH

Terimakasih kepada PT.Pupuk Sriwidjaja Palembang dan Universitas Bina darma yang telah mendukung keterlaksanaannya penelitian ini

DAFTAR PUSTAKA

[1] (Hanipah & Dhika, 2020) Analisa pencegahan aktivitas ilegal didalam jaringan dengan wireshark. *DoubleClick: Journal of Computer and Information Technology*, *4*(1), 11-23.

[2] (Hasbi & Saputra, 2022) Analisis Quality of Service (Qos) Jaringan Internet Kantor Pusat King Bukopin Dengan Menggunakan Wireshark. *JUST IT: Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, *12*(1).

[3] (Febriani & Sahfitri, 2022) MONITORING PENCEGAHAN AKTIVITAS ILEGAL DALAM JARINGAN PADA KANTOR DINAS ESDM PROVINSI SUMATERA SELATAN. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 4, No. 1, pp. 92-99).

[4] (Ubaedila et al., 2022) Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark. *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, *6*(1), 95-104.

[5] (Wulandari & Ariyadi, 2022) ANALISA MONITORING SNIFFING PAKET DATA JARINGAN LOKAL PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA PRABUMULIH. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 3, No. 2, pp. 185-192).

[6] (Sulicdio et al., 2022) Comparative Analysis of Wireshark and Windump Software in Network Security Monitoring. *Jurnal Media Computer Science*, *1*(1), 1-6.

[7] (ALKASAR & Stiawan, 2020). *SISTEM PENCEGAHAN SERANGAN SQL INJECTION PADA WEB PENETRATION TESTING DAMN VULNERABLE WEB ATTACK DVWA MENGGUNAKAN METODE BAYESIAN NETWORK* (Doctoral dissertation, Sriwijaya University).

[8] (Herman et al., 2023) Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration. *JURIKOM (Jurnal Riset Komputer)*, *10*(1), 317-329.

[9] (Setiawan & Zulfikri, 2020) Sistem Keamanan Jaringan Komputer Metode Network Intrusion Detection System Di Kantor Setwan. *Jurnal Intra Tech*, *4*(2), 35-46.

[10] (Ibrahim, 2020)). *Analisis Keamanan Jaringan pada Fasilitas Internet (Wifi) Kantor Pemerintahan Kota Batam terhadap Serangan Packet Sniffing* (Doctoral dissertation, Prodi Teknik Infomatika).

[11] (Tamsir Ariyadi & Ali, 2018). Analisis Paket DHCP Rogue Pada Jaringan Local Area Network (LAN) Menggunakan Wireshark. In *PROSIDING SEMINAR NASIONAL INOVASI, TEKNOLOGI DAN APLIKASI SeNITiA- 2018* (pp. 97-101). FAKULTAS TEKNIK UNIVESITAS BENGKULU.