Analisis Keamanan Jaringan Wifi Menggunakan Wireshark

Fitria Rizqi Nurdiana[a*], Indra Gunawan[b*], Rena Cahya Viollita[c], M.Arip Faizal[d], Deniva Nurcahyadi[e]

[abcde] Teknik informatika;Sekolah Tinggi Teknologi Ronggolawe Cepu

[b] Penulis Korenspondensi, Alamat Email: igunsttr@gmail.com

Abstrak

Menurut Committee on National Security Systems (sebuah departemen di negara Amerika yang bertanggung jawab terhadap sistem keamanan dunia maya), information security atau keamanan sistem informasi adalah perlindungan informasi dan elemen elemennya termasuk sistem dan perangkat kerasnya. Saat ini permasalahan keamanan informasi menjadi penting, khususnya proses penyadapan informasi (Sniffing) pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang bersifat positif maupun yang bersifat sebaliknya. Dalam penelitian ini, proses sniffing digunakan untuk mendapatkan informasi username dan password. Proses sniffing dilakukan menggunakan perangkat lunak Wireshark. Software 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 data yang dilakukan pada jaringan komputer, hal ini mengakibatkan hilangnya salah satu sifat keamanan yaitu privacy dan confidentiality.

Kata kunci: analisis keamanan, keamanan Informasi, sniffing, wireshark, wifi

Abstract

According to the Committee on National Security Systems (a department in the United States responsible for cybersecurity systems), information security or information system security is the protection of information and its elements, including systems and hardware. The problem of the information situation becomes important, especially the process of tapping information (sniffing) on computer networks, which is increasingly being carried out, both for positive and otherwise. In this study, the sniffing process was used to obtain username and password information. The sniffing process is carried out using the Wireshark software. Wireshark software performs the capturing process of data on the Wireless interface, then peering the captured results containing POST data containing username and password on HTTP. From the results of the research conducted, it was found that using Wireshark could do data tapping on a computer network, this shows one of the characteristics of security, namely privacy and confidentiality.

Keywords: information security, information security, sniffing, wireshark

1. Pendahuluan

WiFi merupakan singkatan dari Wireless Fidelity. WiFi dapat dikatakan sebuah teknologi untuk saling bertukar data dengan memanfaatkan gelombang radio (nirkabel) yang dapat digunakan oleh beberapa perangkat elektronik seperti komputer, smartphone, tablet, dan sebagainya . WiFi memiliiki berbagai kelebihan yang menjadikan teknologi ini menjadi primadona bagi masyarakat. Pada jaringan komputer dikenal istilah protokol, yaitu sekumpulan aturan / prosedur atau standar yang digunakan untuk mengirimkan data antara perangkat elektronik. Protokol mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih computer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya.

Beberapa kelebihan WiFi diantaranya adalah bahwa teknologi ini lebih fleksibel atau pengguna bisa berpindah tempat, jaringan internet dapat diakses lebih mudah, juga penggunaan listrik yang lebih efisien. Namun dengan kelebihan yang dimiliki teknologi ini tak dapat dihindari kekurangan yang ada, seperti jaringan yang kurang aman dan bisa di sadap, perangkat yang cukup mahal, kualitas sinyal yang tidak baik pada kondisi tertentu. Hal ini sesuai dengan pendapat bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Keamanan jaringan menjadi hal yang menarik untuk dibahas mengingat hal diatas. Kemanan jaringan penting dilakukan oleh administrator jaringan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Keamanan jaringan komputer (computer network security) harus menjadi perhatian yang besar pada saat kita akan membangun sebuah infrastruktur jaringan.

Selama data itu tidaklah penting seperti berkomunikasi data menggunakan email, pesan ke “wall” facebook, tidak masalah menggunakan koneksi HTTP. Karena mungkin dampak maupun resiko yang terjadi apabila ada yang mengintipnya tidak akan berpengaruh. Namun bagaimana jika data yang kirimkan adalah password email, komunikasi bisnis yang sifatnya rahasia dan lain sebagainya. Untuk penelitiaan ini menggunakan tools sniffer yang sudah sangat terkenal Wireshark. Selain itu bertujuan untuk memahami bagaimana cara kerja sniffing.

2. Metodologi

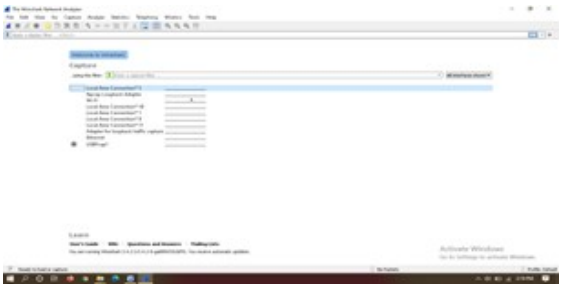
Penelitian ini mencoba melakukan metode sniffing pada jaringan WiFi yang berbasis protokol untuk mendapatkan hasil capture traffic dan mendapatkan username dan password sebuah station. Aplikasi yang digunakan pada proses sniffing adalah Wireshark.

3. Hasil dan Pembahasan

Proses awal penelitian ini adalah membangun jaringan WiFi berbasis protokol 802.1X. Setelah jaringan WiFi terbentuk dan di uji coba selanjutnya menginstall aplikasi Wireshark untuk kemudian di gunakan untuk melakukan proses capturing traffic internet yang berlangsung. Setelah station meminta otentikasi dan memastikan dapat menikmati layanan internet lalu hasil capture traffic yang di dapatkan dilakukan analisa untuk mencari kode otentikasi yang berupa username dan password station.

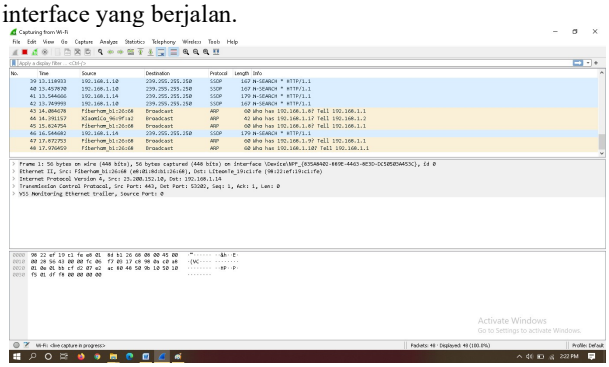
3.1 Wireshark

Wireshark adalah sebuah Network Packet Analyzer. Network Packet Analyzer akan mencoba menangkap paket-paket jaringan dan berusaha unutk menampilkan semua informasi di pakey tersebut sedetail mungkin . Wireshark dapat menganalisis paket data secara real time. Artinya aplikasi Wireshark ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah di tentukan oleh user sebelumnya untuk kemudian menampilkannya. Wireshark dapat diunduh dari web secara gratis untuk selanjutnya dilakukan instalasi pada perangkat laptop / computer dan menjalankannya. erikut adalah gambar antar muka aplikasi Wireshark yang telah berhasil di instal :



Gambar.1 Antar muka aplikasi Wireshark

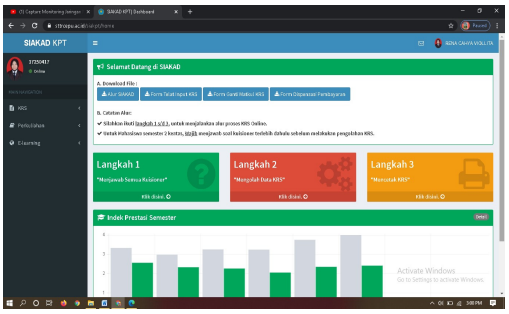
Saat aplikasi Wireshark di jalankan, akan tampak interface yang tersedia, berikut interface yang sedang bekerja dengan penanda terdapat traffic berupa grafik pada interface yang berjalan.



Gambar.2 Proses Sniffing dan Analisis Hasil Capture

Aplikasi Wireshark yang telah di install dalam laptop di jalankan (running) dengan klik dua kali pada interface WiFi, karena pada penelitian ini fokus pada jaringan nirkabel / WiFi. Selanjutnya berperan sebagai seorang user yang akan menikmati koneksi internet dengan kode otentikasi yang telah dibuat sebelumnya. Setelah berhasil login dan mencoba / memastikan koneksi internet dapat dinikmati, proses capturing Wireshark dihentikan untuk kemudian hasil capture traffic tersebut di simpan dan dianalisis, apakah kode otentikasi yang berupa username dan password user tersebut dapat tertangkap di file hasil capturing Wireshark.Berikut adalah gambar proses login sebuah station pada jaringan WiFi berbasis 802.1X.

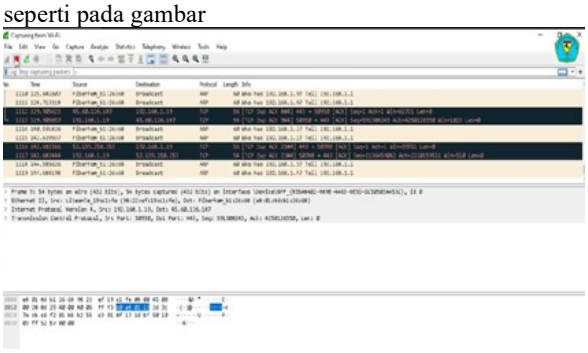
Gambar.3 Proses login pada sebuah station



Gambar.4 Proses login berhasil

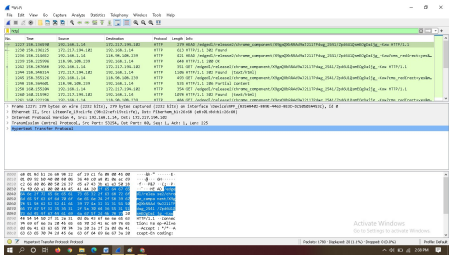
Selanjutnya hasil capture traffic data pada Wireshark diakhiri dan di simpan untuk dianalisis. Hasil analisis yang dilakukan diperoleh bukti bahwa kode otentikasi yang berupa username dan password pada jaringan WiFi berbasis protocol 802.1X .berhasil di peroleh seperti ditunjukan pada gambar berikut :

Dari hasil percobaan diatas didapatkan hasil capture-an seperti pada gambar



Gambar.5 Hasil Capture

Hasil capture-an seperti pada gambar diatas belum dilakukan pemfilteran, sehingga semua data yang lewat pada jaringan tersebut direkam sehingga menyulitkan dilakukan analisa. Disini penulis akan melakukan pemfilteran pada protokol HTTP seperti yang ditunjukkan pada gambar dibawah ini.

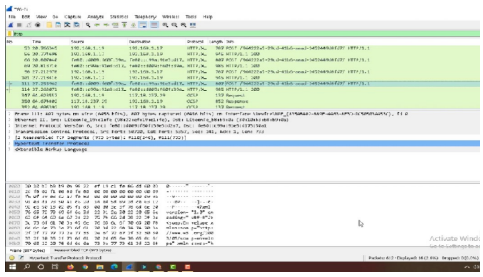


Gambar. 6 Filteran paket HTTP

Setelah melakukan capture pada protokol HTTP, selanjutnya lakukan analisa pada paket yang berisikan data POST seperti pada gambar

Gambar.7 Paket yang berisi data POST

Lalu terdapat informasi HTTP yang berisi POST, host, connection, content-length, origin, user-agent, dan yang paling penting HTML form URL yang berisi username dan password seperti pada gambar .



Gambar .8 Hypertex transfer protocol

Sniffing username dan password menggunakan Wireshark berhasil. Dengan hasil capture yang di analisa melalui jaringan pada jaringan terpilih bisa diketahui username dan password pada paket data POST.

5. Kesimpulan

Kesimpulan dan Saran Dengan menggunakan Wireshark memudahkan proses capture paket data secara langsung dari sebuah network interface, mampu menampilkan informasi yang sangat detail mengenai hasil informasi penting dan rahasia seperti username dan password. Dari percobaan diatas, Sniffing merupakan suatu yang cukup sulit untuk dicegah. Untuk sekarang ini sudah ada beberapa cara penangguhan sniffing seperti menggunakan enkripsi pada data rahasia (username, password), HTTPS (Hypertext Transport Protocol Secure) pada port 443. Saran lebih ditujukan pada asas kehati-hatian ketika melakukan aktifitas seperti mengakses halaman web email, e-banking, social media, pada jaringan internet yang belum dikenal seperti walaupun itu menawarkan secara gratis

Daftar Pustaka

Ethical Hacking, Chris. (2016). How to sniff password using Wireshark Review https://codingsec.net/2016/04/how-sniff-password-using wireshark/. Tanggal Akses : 19 Desember 2020.

Gunawan; Indra. (2021). *Keamanan Data: Teori dan Implementasi*. Jejak Publisher: Sukabumi. Diunduh dari https://www.researchgate.net/publication/338598999_Keamanan_Data_Teori_dan_Implementasi

Gunawan; Indra, Ferriyan; Andrey. (2016). Analisis Keamanan Jaringan Wifi Pendekatan Blackbox dan Whitebox. *Seminar Nasional Sistem Informasi & Teknologi Informasi (SENSITIF)*. Diunduh dari https://www.researchgate.net/publication/316464159_Analisis_Keamanan_Jaringan_Wifi_Pendekatan_Blackbox_dan_Whitebox_Studi_Kasus_Ibnu_Sina_Batam

Primartha, R.,. (2021). “Manajemen Jaringan Komputer”, Penerbit INFORMATIKA, Tanggal Akses 1 januari.

Search Security. (2008). Wireshark tutorial: How to sniff network traffic. Review http://searchsecurity.techtarget.com/tip/Wireshark-tutorial-How-to-sniff-network-traffic. Tanggal Akses : 3 januari 2021.

Triawan (2020). menggunakan wireshark. Review https://triawan.gitbooks.io/modulkeamanan-komputer/bab2.html. Tanggal Akses : 18 Desember 2020.

Tonapa, O., Pauline R., Debora K., (2020) “Analisis Performansi Konektifitas Pada Jaringan Wireless Broadband di Bandung”, Jurnal ELKOMIKA Institut Teknologi Nasional Bandung, Vol. 2, No. 2, Juli – Desember 2020.