Analisis Keamanan Data Pada Website Dengan Wireshark

Fahrik Huzaeni[a*], Indra Gunawan[b*], Dentaruni Cahya Purnomo[c], Muntri Yanti[d], Novi Krisdayanti[e]

[abcde]Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe Cepu

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

Abstrak

Era teknologi terus berkembang pesat dari waktu ke waktu, terutama di perangkat komputer. Komputer saat ini memfasilitasi semua pekerjaan manusia. Dalam hal menjalankan operasinya, komputer memiliki perangkat lunak pendukung yang berjalan pada sistem operasi dan memainkan peran yang sangat penting dalam melaksanakan tugas yang dilakukan oleh pengguna. Dari penelitian tentang analisis keamanan data pada situs web dengan Wireshark, dapat disimpulkan bahwa protokol HTTP sangat berbahaya ketika digunakan untuk menulis informasi pribadi rahasia, terutama nama pengguna dan kata sandi. Dari kesimpulan di atas, penelitian ini memiliki kelemahan dalam bentuk tidak ada perbandingan informasi yang diperoleh dengan analisis paket jaringan lain selain Wireshark.

Kata Kunci : Data security, Website, Wireshark.

Abstract

The technological era continues to develop rapidly from time to time, especially in computer devices. Today's computers facilitate all human work. In terms of running its operations, the computer has supporting software that runs on the operating system and plays a very important role in carrying out the tasks performed by the user. From research on data security analysis on websites with wireshark, it can be concluded that the HTTP protocol is very dangerous when it is used to write confidential personal information, especially user names and passwords. From the above conclusions, this study has drawbacks in the form of no comparison of the information obtained with other network packet analyzers besides Wireshark.

Keywords : Data security, Website, Wireshark.

1. Pendahuluan

Era teknologi terus berkembang pesat seiring berjalannya waktu, terutama pada peralatan computer. Computer saat ini memudahkan seluruh pekerjaan manusia. Dalam hal menjalankan operasinya, computer memiliki software pendukung yang berjalan diatas sistem operasi dan berperan sangat penting untuk melaksanakan tugas-tugas yang dikerjakan oleh user. Melalui software, komputer bisa menjalankan perintah sehingga dapat membantu user dalam mengatasi pekerjaannya. Tetapi tidak semua software bisa mendukung dan melancarkan manusia dalam mengatasi pekerjaannya, ada juga jenis software yang dibentuk untuk melaksanakan kerusakan atau tindak kejahatan yang bisa merugikan user lain.

Selain software-software yang berjalan diatas sistem operasi computer juga memiliki protocol pada internet berupa HTTP dan HTTPS yang biasanya digunakan untuk mengakses sebuah website atau platform yang berbasis web. Teknologi ini tidak pernah tergerus oleh waktu karena website bisa diakses dengan cepat melalui hamper semua perangkat teknologi seperti handphone, laptop, tablet, dan lain-lain.

Karena kemudahan tersebut maka semakin banyak juga celah keamanan yang ada dilalamnya dan tidak jarang user yang menjadi korban karena kurangnya pengetahuan tentang protocol website yang aman. Data yang biasanya dicuri adalah username dan password dari akun korban untuk dimanfaatkan demi kepentingan yang tidak baik. Oleh karena itu penulis melakukan penelitian ini dengan tujuan untuk memberikan gambaran tentang cara mendapatkan username dan password yang sering bocor kepada pihak kektiga dengan menggunakn aplikasi wireshark sehingga user bisa lebih berhati-hati dalam mengetikan informasi-informasi pribadi yang penting.

2. Kerangka Teori

2.1. HTTP

Hypertext Transfer Protocol (HTTP) merupakan sebuah protokol jaringan aplikasi yang digunakan untuk mendistribusikan informasi antara komputer server dengan komputer client. Server disini yang dimaksud adalah jenis web server denan bentuk fisik jaringan komputer yang memiliki sekala besar. Sedangkan client adalah web browser yang dapat mengakses, menerima dan menampilkan konten melalui browser (Interen, 2020).

Pada protokol HTTP tidak ada jaminan data antara client dan server akan aman. Hal ini menyebabkan banyak isu kejahatan berupa kebocoran data-data pribadi yang di masukan kedalam web dengan protokol HTTP. Pada dasarnya setiap protokol komunikasi antara client dan server selalu menggunakan konsep HTTP. Namun jika ingin menerapkan protokol yang lebih aman dibutuhkan sertifikat SSL (Secure Soket Layers). Halaman web dengan protokol HTTP akan lebih sulit diakses bahkan tidak akan terbuka dan dialihkan ke halaman yang lain.

2.2. HTTPS

Hypertext Transfer Protocol Secure (HTTPS) merupakan pengembangan dari versi HTTP sebelumnya. HTTPS memiliki tingkat keamanan yang lebih baik dibandingkan dengan HTTP sehingga dapat membuat client merasa lebih aman dalam mengakses konten-konten web.

Protokol HTTPS dikembangkan oleh perusahaan berbasis IT yaitu Netscape Communication Corp. HTTPS memiliki protokol kolaboratif berupa keamanan data yang ditransmisikan hal ini menyebabkan HTTPS lebih banyak digunakan oleh web developer. Tiga prosedur yang digunakan oleh HTTPS untuk security data adalah autentikasi server, kerahasiaan data, dan integritas data.

2.3. Sniffing

Sniffing merupakan proses yang dilakukan untuk mendapatkan aket data yang dikirimkan melalui jaringan komputer. Sniffing bisa digunakan untuk memamtau dan menangkap semua lalulintas yang terjadi di dalamnya tanpa pengecualian darimana dan untuk siapa paket-paket tersebut dikirimkan. Dampak negatif dari sniffing adalah seseorang bisa melihat informasi rahasia milik orang lain yang terhubung ke jaringan contohnya adalah username dan password (Isparmo, 2008).

Dampak baik dari sniffing jaringan adalah untuk mengaanalisa paket data yang melewati jaringan sehingga jaringan dapat lebih optimal, menganalisa data apakah mempengaruhi performa jaringan atau tidak, dan dapat mengetahui bila ada pihak asing yang menyusup kedalam jaringan.

2.4. Wireshark

Wiresharek merupakan aplikasi yang dijadikan tool untuk menganalisis paket data jaringan yang sedang berlangsung (Kurniawan, 2012). Wireshark disebut juga sebagai network packet analyzer yang berfungsi untuk menampilkan semua informasi pada paket tersebut secara lengkap dan menangkap paket-paket yang dikirimkan maupun diterima.

Network packet analyzer bisa digunakan untuk memantau berbagai macam jaringan mulai dari jaringan berkabel maupun wireless. Dengan adanya wireshark ini admin akan lebih mudah mengawasi jaringan karena data yang tertangkap pada wireshark dapat disimpan dan dibuka kembali untuk dianalisis (Adriant et al, 2015).

3. Metodologi

3.1. Pengumpulan Data

Dalam penelitian ini penulis mengunakan data yang dikumpulkan melalui penangkapan paket-paket data dengan menggunakan aplikasi wireshark. Data tersebut diambil dengan cara mengakses website sistem informasi akademik dari STTR Cepu yaitu www.sttrcepu.ac.id dengan menggunakan dua protocol yang berbeda, protocol pertama adalah HTTP dan protocol kedua adalah HTTPS. Proses ini dilakukan kurang lebih lima menit untuk setiap protokol.

3.2. Perancangan Alur Penelitian

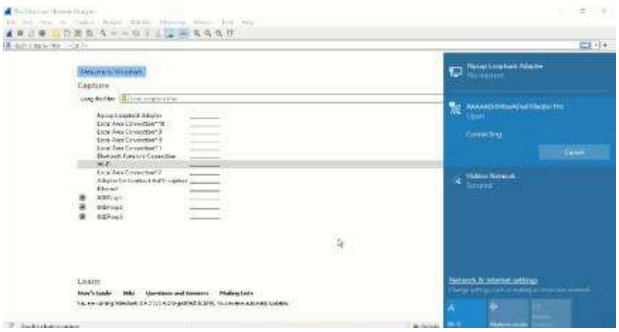
Perancangan alur penelitian untuk analisis keamanan data pada website dengan wireshrk adalah seperti pada gambar 1. Proses pertama yang harus dilakukan adalah mengaktifkan aplikasi wireshark dengan memilih jaringan wifi kemudian kita harus mengakses alamat website yang akan dijadikan contoh melalui btowser setelah itu tunggu sampai paket-paket data tersebut ditangkap oleh wireshark. Pada saat paket sudah tertangkap matikan atau stop penangkapan paket pada wireshark agar lebih mudah untuk melakukan analisis paket-paket tersebut. Lakukan filtering menggunakan HTTP kemudian temukan paket dengan metode post dan mulailah untuk menganalisa isi dari paket tersebut.

Gambar 1. Alur Penelitian.

4. Hasil dan Pembahasan

Hasil analisis keamanan data pada website dengan wireshark, pertama akan melakukan analisis dengan website yang menggunakan http untuk melakukan sniffing menggunakan wireshark agar mendapatkan username dan password, Dengan melakukan beberapa langkah dibawah ini :

1. Jalankan Aplikasi Wireshark

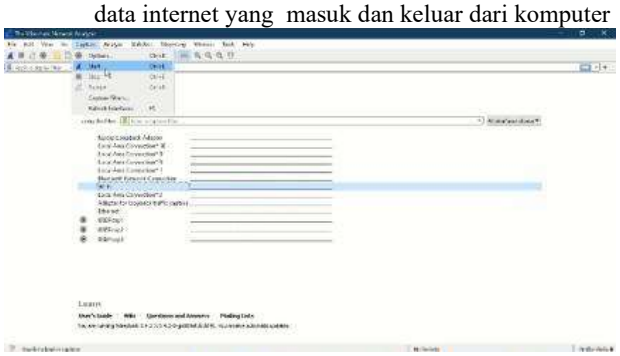


Gambar 2. Tampilan Wireshark.

2. Tentukan alamat HTTP
   Disini kami menggunakan alamat http://sttrcepu.ac.id/siakapt/login untuk melakukan proses snifing untuk mendapatkan username dan password

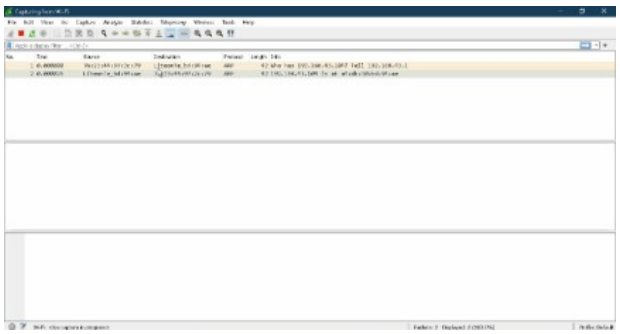
.Gambar 3. website HTTP.

3. Kemudian pilih wifi sebagai interfacenya dan klik capture dan pilih start untuk memulai perekaman data internet yang masuk dan keluar dari komputer



Gambar 4. Capture.

4. Setelah itu Wireshark akan melakukan proses capture data yang masuk dankeluar

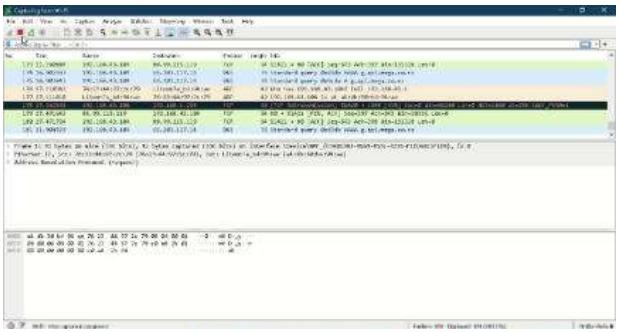


Gambar 5. proses Capture.

5. Selanjutnya buka websitenya dan masukan username dan password dalam website tersebut

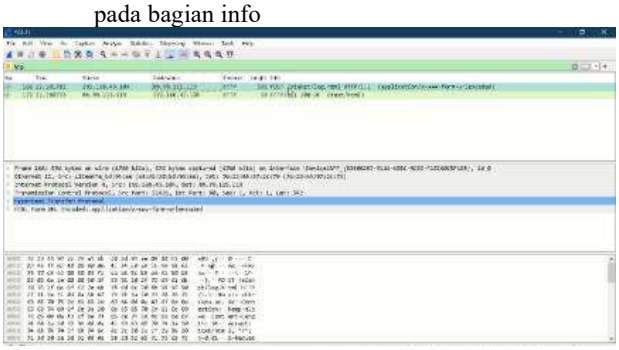
Gambar 6. username dan password.

6. Kembali ke wireshark dan stop capture yang sedang berjalan



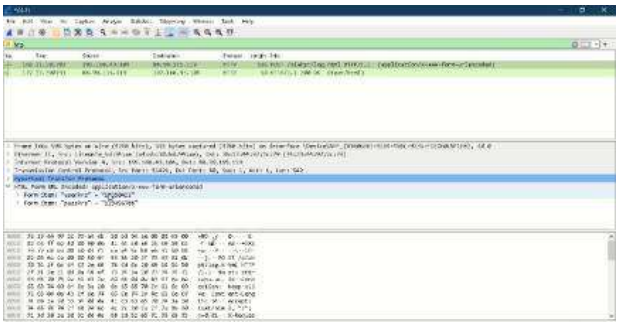
Gambar 7. stop capture.

7. Ketikan perintah HTTP pada filter dan pilih POST pada bagian info



Gambar 8. filter http.

8. Pada data POST terdapat informasi seperti alamat IP192.168.43.104 source dan 88.99.115.119 destination, kemudian didalam HTTP terdapat berbagai informasi kemudian pilih HTML form untuk mengetahui username dan password yang telah dimasukan tadi



Gambar 9. HTML form.

9. 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.

Gambar 10. username dan password.

Setelah melakukan snifing pada HTTP selanjutnya kita menggunakan HTTPS, untuk perintahnya seperti dibawah ini :

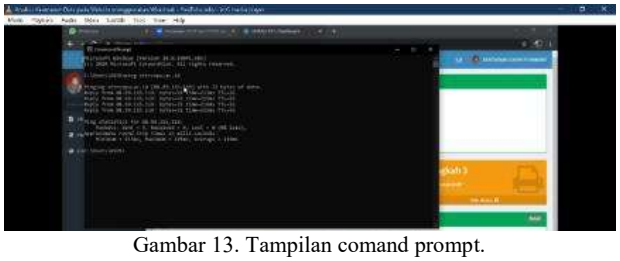
1. Buka wireshark dan akan muncul jendela sofware wireshark,kemudian sambungkan dengan wifi dan lakukan proses capture seperti HTTP.

Gambar 11. Jendela wireshark.

2. Selanjutnya buka websitenya, untuk https yaitu https://sttrcepu.ac.id/siakapt/home kemudian masuk dengan memasukan username dan password pada form yang ada dan lakukan login

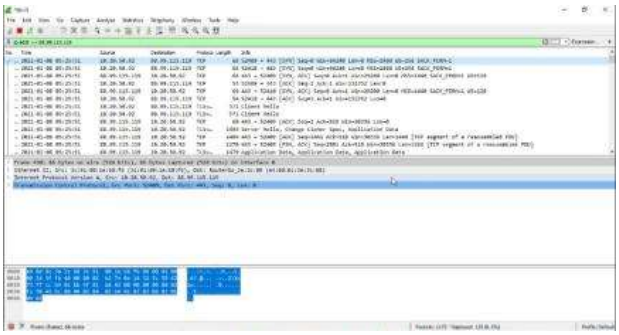
Gambar 12. Tampilan sudah login.

3. Kemudian untuk mengecek website yang diakses lakukan ping pada command prompt untuk mengetahui Ip websitenya.



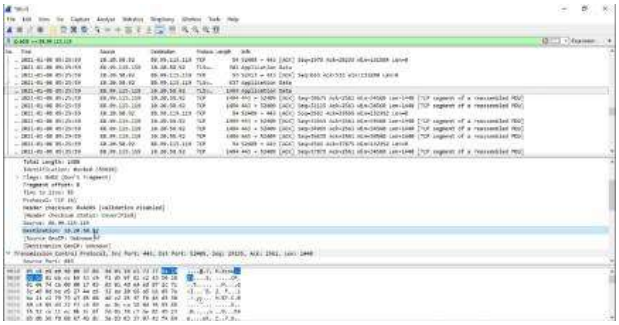
Gambar 13. Tampilan comand prompt.

4. Setelah melakukan ping sttrcepu.ac.id dan didapati ipnya yaitu 88.99.115.119, Selanjutnya cari dengan sofware wireshark pada bagian filter tulis ip.ddr == 88.99.115.119



Gambar 14. mencari ip.

5. Maka akan terlihat ip dari website https://sttrcepu.ac.id pada sofware wireshark



Gambar 15. Analisis paket.

5. Kesimpulan

Dari penelitian tentang analisis keamanan data pada website dengan wireshark dapat ditarik kesimpulan bahwa protocol HTTP sangat berbahaya saat digunakan untuk menulis informasi pribadi yang bersifat rahasia khususnya username dan password. Pada gambar (berapa) sudah terlihat halisnya pada metode post yang tertangkap wireshark apa yang dimasukan oleh user dapat terbaja jelas tanpa enkripsi. Sedangkan protocol HTTPS lebih aman karena saat kita mengakses situs dengan protocol HTTPS tidak ada protocol HTTPS yang dapat tertangkap oleh aplikasi ini. Informasi yang disajikan lewat pelacakan IP halaman yang dikunjungi hanya berupa IP asal dan tujuan atau server dan port yang digunakan untuk melakukan komunikasi, paket data yang melewati hanya bisa diketahui jumlahnya saja dan ketika dilihat paket tersebut tidak bisa terbaca atau telah ter enskripsi oleh enkripsi yang digunakan oleh masing-masing situs web. Dari kesimpulan diatas penelitian ini memiliki kekurang berupa tidak adanya perbandingan informasi yang didapatkan dengan network packet analyzer yang lain selain wireshark.

Daftar Pustaka

Adriant et al, F. (2015). Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan. *Seminar Nasional Cendekiawan 2015*.

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

Interen, D. (2020). *Apa perbedaan HTTP dan HTTPS? lengkap beserta penjelasannya*. Dicoding.

Isparmo. (2008). *Mengenal Dunia Hacking : SNIFFING*. http://isparmo.web.id/2008/06/06/mengenal-dunia-hacking-sniffing/

Kurniawan, A. (2012). *Network forensics : panduan analisis dan investigasi paket data jaringan menggunakan Wireshark*. Andi Offset.