ANALISIS DAN PENYADAPAN TRANSMISI PAKET DATA JARINGAN KOMPUTER MENGGUNAKAN WIRESHARK

Dedi Irawan
Diploma III Manajemen Informatika, Universitas Muhammadiyah Metro
Jl. Gatot Subroto 100 Yosodadi Kota Metro Lampung- Indonesia
e-mail : dedi.mti@gmail.com

Abstrack
According to the Committee on National Security Systems (a department in the United States responsible for cyber security systems), information security or information system security is the protection of information and elements including elements of the system and hardware. Currently the information security problem becomes important, especially the process of tapping the information (Sniffing) on computer networks become increasingly common, both for the use of a positive and the opposite. In this study, the sniffing process is used to obtain username and password information. The sniffing process is done using Wireshark software. The Wireshark software capturing data on the Wireless interface, then observes the capture results containing POST data containing usernames and passwords on HTTP. From the results of research conducted it was found that by using Wireshark can do data tapping performed on computer networks, this resulted in the loss of one of the security properties of privacy and confidentiality.

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: information security, keamanan Informasi, sniffing, wireshark.

PENDAHULUAN

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

Teori Dasar

Sniffing

Menurut wikipedia Indonesia, : “Sniffer Paket (arti tekstual: pengendus paket — dapat pula diartikan ‘penyadap paket’) yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Contoh dampak negatif sniffing, seseorang dapat melihat paket data informasi seperti username dan password yang lewat pada jaringan komputer. Contohnya begini, Anda adalah pemakai komputer yang terhubung dengan suatu jaringan dikantor. Saat Anda mengirimkan email ke teman yang berada diluar kota maka email tersebut akan dikirimkan dari komputer Anda lalu melewati jaringan komputer kantor (mungkin melalui server maupun gateway internet), lalu keluar dari kantor melalui jaringan internet, lalu sampe di inbox email teman. Pada saat email tersebut melalui jaringan komputer kantor itulah aktifitas *sniffing* bisa dilakukan.

Wireshark

Wireshark merupakan sebuah *software* penganalisa jaringan yang paling dikenal. *Software* ini sangat berguna dalam menyediakan jaringan dan protokol serta memberikan informasi tentang data yang tertangkap pada jaringan. Software wireshark dapat menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer. Dapat mengumpamakan sebuah *Network Packet Analyzer* sebagai alat untuk memeriksa apa yang sebenarnya sedang terjadi di dalam kabel jaringan.

Ada beberapa contoh penggunaan Wireshark, yaitu:

- ✓ Admin sebuah jaringan menggunakannya untuk troubleshooting di jaringannya.
- ✓ Teknisi keamanan jaringan menggunakannya untuk memeriksa keamanan jaringan.
- ✓ Pengembang software dapat menggunakannya untuk men-debug implementasi protocol jaringan dalam software mereka.
- ✓ Orang yang memakainya untuk mempelajari protocol jaringan secara detail.
- ✓ Serta digunakan sebagai sniffer atau “pengendus” data-data privasi jaringan.

Beberapa fitur kelebihan Wireshark, diantaranya:

- ✓ Mampu menangkap paket-paket data/informasi yang bertebaran dalam jaringan yang kita “intip”.
- ✓ Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa.
- ✓ Dapat dipakai untuk sniffing (memperoleh informasi penting spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya.

Percobaan

Pada percobaan ini penulis akan melakukan sniffing menggunakan Wireshark untuk mendapatkan username dan password. Berikut-berikut langkah-langkah untuk melakukan sniffing pada Wireshark:

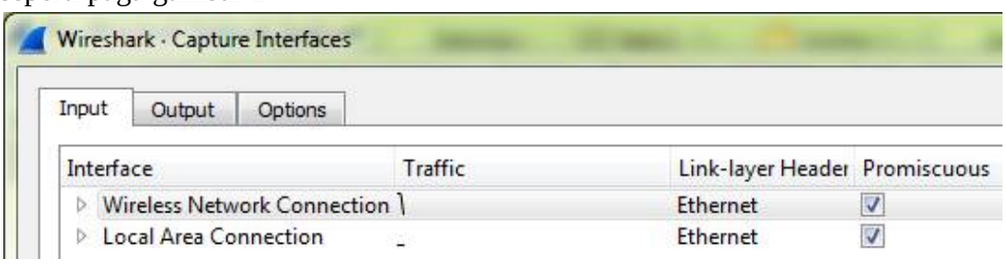
1. Jalankan Wireshark

   Mencoba menggunakan wireshark untuk memantau akses browser yang dijalankan namun mencoba memonitor jaringan wi-fi, seperti pada gambar 1 dibawah ini.

Gambar 1 Tampilan Wireshark

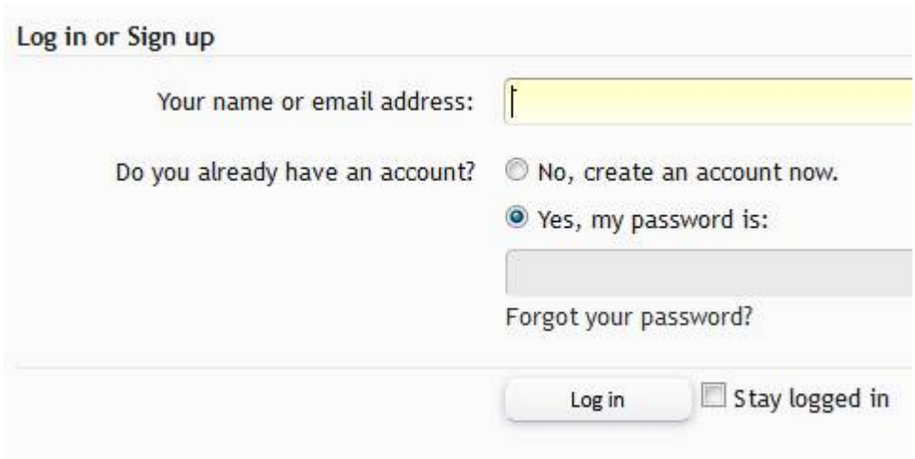
   Langkah pertama untuk memilih driver wireless, saat ditampilan awal kita bisa menenkan tombol Ctrl +K.

2. Memilih interface yang akan dimonitor, disini penulis memilih Wireless lalu tekan start, seperti paga gambar 2



Gambar 2. Memilih interface

3. Membuka website, masukkan username dan password

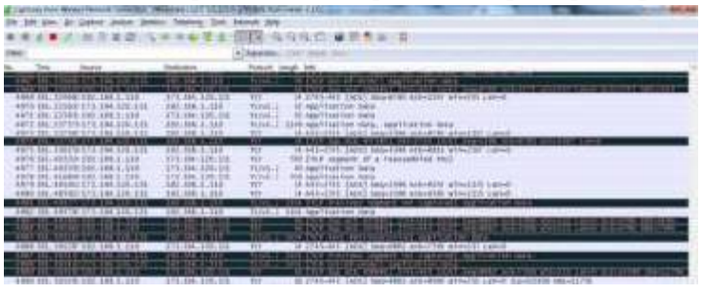


Gambar 3 Membuka website komunitas publisher indonesia

4. Dari percobaan diatas, program Wireshark dijalankan lalu memilih interface device network, disini penulis memilih interface Wireless start lalu membuka web komunitas dan masukkan username dan password lalu log in.

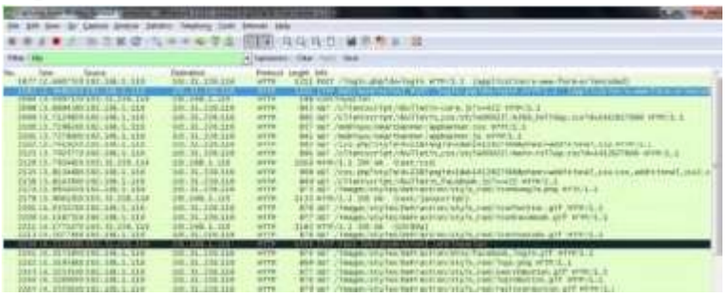
Pembahasan

1. Dari hasil percobaan diatas didapatkan hasil capture-an seperti pada gambar 4.



Gambar 4. Hasil Capture

2. Hasil capture-an seperti pada gambar 4 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 5 dibawah ini.



Gambar 5. Filteran paket HTTP

3. Setelah melakukan capture pada protokol HTTP, selanjutnya lakukan analisa pada paket yang berisikan data POST seperti pada gambar 6.

Gambar 6. Paket yang berisi data POST

4. Pada data POST tersebut beberapa informasi seperti, alamat IP 192.168.43.196 source dan 119.81.17.85 destination, 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 7.

Gambar 7. 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.

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 Oktober 2017.

Triawan.2017. Tutorial menggunakan wireshark. Review https://triawan.gitbooks.io/modul-keamanan-komputer/bab2.html. Tanggal Akses : 18 Oktober 2017.

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 Oktober 2017.