IMPLEMENTASI WIRESHARK UNTUK PENYADAPAN (*SNIFFING*) PAKET DATA JARINGAN

M. Ferdy Adriant, Is Mardianto
Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Trisakti

Abstrak

Saat ini perkembangan teknologi informasi berkembang dengan sangat pesat, yang menyebabkan isu keamanan informasi menjadi penting. Proses penyadapan informasi (Sniffing) pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang bersifat positif maupun yang bersifat sebaliknya. Keamanan Informasi adalah segala usaha perlindungan informasi, terhadap akses atau modifikasi data dan informasi yang tidak sah yang dapat terjadi pada media penyimpanan atau pada saat transmisi data. Dalam penelitian ini, proses *sniffing* digunakan untuk mendapatkan informasi *username* dan *password*. Proses *sniffing* dilakukan menggunakan perangkat lunak Wireshark. So*ftware* 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 atau pengendusan data yang lewat pada jaringan komputer, hal ini mengakibatkan hilangnya salah satu sifat keamanan yaitu *privacy* dan *confidentiality*.

Kata kunci: Keamanan Informasi, *sniffing, WireShark.*

Pendahuluan

Perkembangan teknologi informasi yang begitu cepat dan memberi banyak kemudahan pada hidup masyarakat menimbulkan beberapa masalah, terutama munculnya kejahatan komputer seperti penyadapan/pengendusan(sniffing) data dan informasi yang lewat pada sistem jaringan komputer. Proses S*niffing* sendiri berlaku seperti bermata dua, disatu sisi memiliki dampak positif dan disisi lain dapat berdampak negatif, tergantung bagaimana, siapa dan apa tujuan kegunaannya

Dalam penelitian ini dilakukan proses s*niffing* menggunakan *software* Wireshark. Dengan memanfaatkan tools yang ada pada Wireshark kita dapat mengetahui username dan password. Dan juga bertujuan untuk memahami bagaimana cara kerja *sniffing.*

Teori Dasar

Sniffing

Sniffing merupakan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu di kirimkan. Contoh dampak negatif *sniffing*, seseorang dapat melihat paket data informasi seperti *username* dan *password* yang lewat pada jaringan komputer. Contoh dampak positif *sniffing*. Seorang admin dapat menganalisa paket-paket data yang lewat pada jaringan untuk keperluan optimasi jaringan, seperti dengan melakukan penganalisaan paket data, dapat diketahui dapat membahayakan performa jaringan atau tidak, dan dapat mengetahui adanya penyusup atau tidak.

Bahaya yang mengancam dari proses sniffing yaitu hilangnya sifat privacy dan confidentiality seperti tercurinya informasi penting dan rahasia seperti *username* dan *password*. (Parmo, 2008).

Wireshark

Wireshark adalah tool yang ditujukan untuk penganalisaan paket data jaringan (Kurniawan, 2012). Wireshark disebut juga *Network packet analyzer* yang berfungsi menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi dipaket tersebut sedetail mungkin.

Sebenarnya *network packet analyzer* sebagai alat untuk memeriksa apa yang sebenarnya terjadi di dalam jaringan baik kabel maupun *wireless*. Dengan adanya wireshark ini semua sangat dimudahkan dalam hal memonitoring dan menganalisa paket yang lewat di jaringan.

Ada beberapa contoh penggunaan Wireshark :

1. Admin sebuah jaringan menggunakan untuk troubleshooting masalah di jaringan.
2. Admin menggunakan Wireshark untuk mengamankan jaringannya.

Beberapa fitur kelebihan Wireshark, diantaranya :

1. Berjalan pada sistem operasi Linux dan Windows.
2. Menangkap paket (*Capturing Packet*) langsung dari *network interface*.
3. Mampu menampilkan hasil tangkapan dengan detail.
4. Dapat melakukan pemfilteran paket
5. Hasil tangkapan dapat di *save*, di *import* dan di *export*.

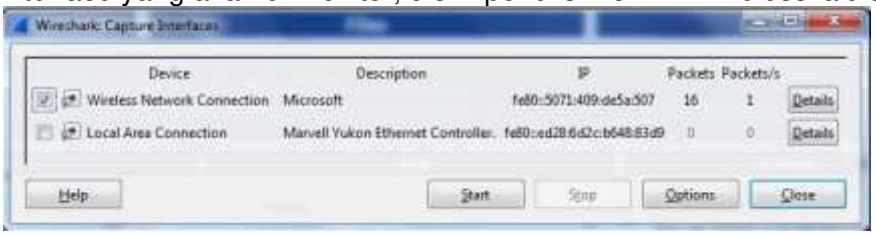
Percobaan

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

1. membuka program Wireshark

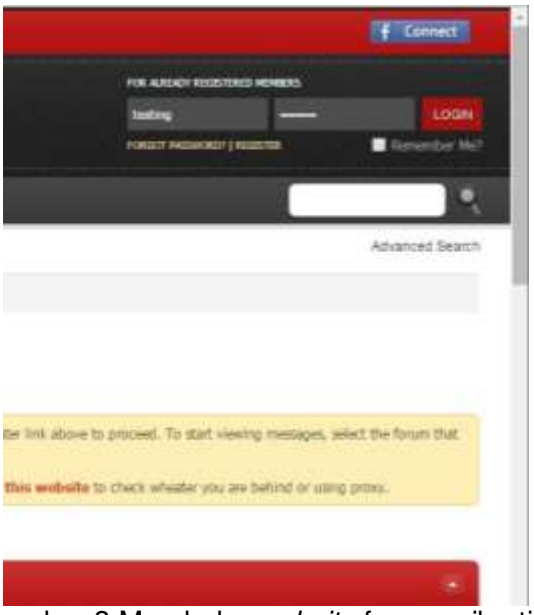
Gambar 1 Tampilan Wireshark

2. Memilih *interface* yang akan di monitor, disini penulis memilih *Wireless* lalu tekan start



Gambar 2 *Interface Wireless*

3. Membuka *website* , masukkan *username* dan *password*

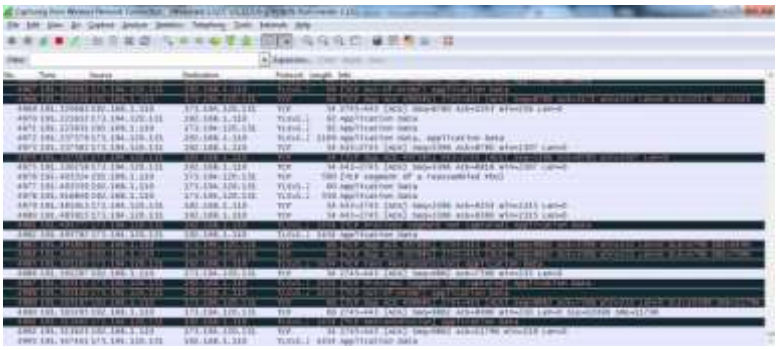


Gambar 3 Membuka *website* forum mikrotik

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

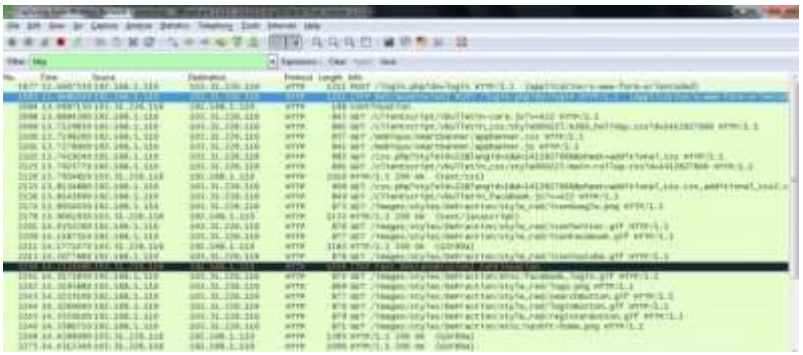
Pembahasan

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



Gambar 4 Hasil *capture*-an

Hasil pen-capture-an diatas belum dilakukan pemfilteran, sehingga semua data yang lewat pada jaringan tersebut terrekam yang menyulitkan untuk dilakukan analisa. Disini penulis akan melakukan pemfilteran pada protokol HTTP seperti yang ditunjukkan pada gambar 5 di bawah ini.

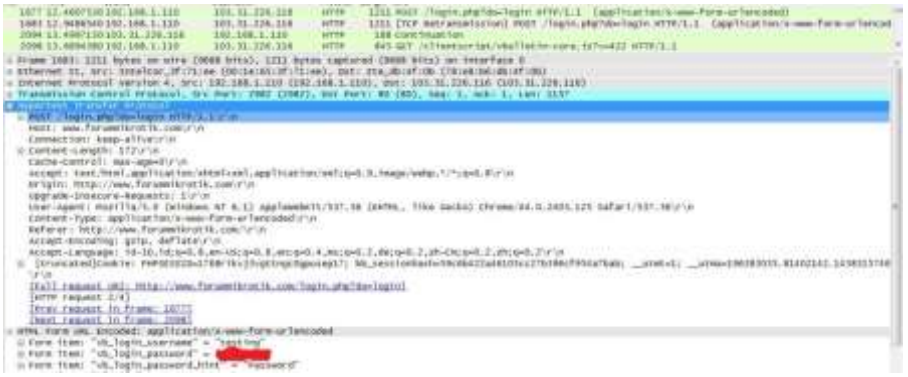


Gambar 5 Pemfilteran paket HTTP

Setelah dilakukan pen-capture-an pada protokol HTTP, lakukan analisa pada paket yang berisikan data POST seperti pada gambar 6.

Gambar 6 Paket yang berisi data *POST*

Pada data POST tersebut beberapa informasi seperti, alamat IP 192.168.1.110 source dan 103.31.226.116 destination, port TCP yang digunakan yaitu port 2982 source dan port 80 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* telah berhasil. Dengan hasil *capture*-an yang telah di analisa, yang lewat di jaringan bisa diketahui *username* dan *password* pada paket data POST.

Kesimpulan dan Saran

Dengan menggunakan Wireshark penyadapan atau pengendusan data dan informasi dapat dilakukan pada paket yang lewat di jaringan yang mengakibatkan tercurinya 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 protokol jaringan lapisan aplikasi. 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 warnet, kantor, kafe.

Daftar Pustaka

Kurniawan, A. (2012). *Network Forensic.* Yogyakarta: Andi Offset.

Parmo, I. (2008, juni 6). *Mengenal Dunia Hacking : Sniffing*. Retrieved from isparmo.web.id: http://isparmo.web.id/2008/06/06/mengenal-dunia-hacking-sniffing/

Singh, A. (2013). *Wireshark Starter.* Birmingham: Packt Publishing.