Jurnal TIMES , Vol. IV No 2 : 20-23 , 2015
ISSN : 2337 - 3601

# ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN MENGGUNAKAN WIRESHARK

Tengku Mohd Diansyah
Jurusan Teknik Informatika
Sekolah Tinggi Teknik Harapan Medan
Jl. H.M. Joni No. 70C Medan 20215 Indonesia
Email :dian_22_88@yahoo.co.id

**Abstrak**

Faktor kemanan jaringan computer merupakan satu hal yang mutlak dalam membangun suatu jaringan. Pada dasarnya system keamanan yang dimiliki oleh system operasi tidaklah cukup untuk mengamankan jaringan komputer. Oleh karena itu untuk mendapatkan sebuah keamanan jaringan computer maka diperlukan suatu tools yang dapat mendeteksi adanya suatu mekanisme serangan dari jaringan. Jenis serangan yang terjadi bias *flood*ing ataupun syn *flood*. Dimana tujuan serangan ini adalah untuk membuat komputer yang mengakses tidak bisa berjalan dengan normal sehingga wireshark ini dapat membantu untuk mendeteksi serangan yang akan terjadi sehingga pengguna jaringan internet tidak khawatir dengan serangan tersebut.

Kata Kunci : Wireshark, Jaringan Komputer

## 1. Pendahuluan

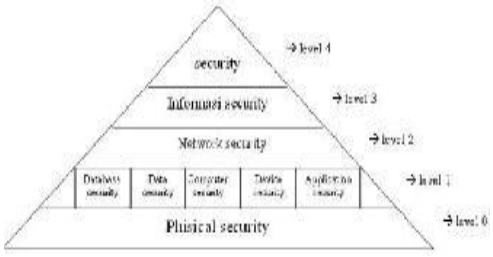
Keamanan jaringan komputer merupakan hal yang sangat penting dalam priotitas keberadaannya. Dalam hal ini keamanan jaringan komputer dibagi menjadi 2 bagian yaitu keamanan secara fisik (hardware) dan keamanan secara non-fisik(*software*). Gangguan tersebut dapat berupa gangguan dari dalam (internal) ataupun gangguan dari luar (eksternal). Gangguan internal merupakan gangguan yang berasal dari lingkup dalam jaringan infrastruktur tersebut. Dalam hal ini adalah gangguan dari pihak-pihak yang telah mengetahui kondisi keamanan dan kelemahan jaringan tersebut. Gangguan eksternal adalah gangguan yang memang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin menembus keamanan yang telah ada[1]. Gangguan eksternal biasanya lebih sering terjadi pada jaringan eksternal, seperti web *server*, telnet, FTP, SSH *server*.

Pada dasarnya pengamanan jaringan dibagi menjadi dua jenis yaitu *rule based* dan *adaptive system*. Sistem *rule based* mendeteksi suatu serangan berdasarkan aturan- aturan yang sudah di definisikan pada kumpulan data aturan sedangkan *adaptive-system* dapat mengenali jenis serangan baru dengan cara membandingkan kondisi saat ini dengan kondisi normal suatu sistem.

Wireshark merupakan *software* untuk melakukan analisa aktivitas jaringan komputer yang memiliki fungsi-fungsi yang berguna bagi profesional jaringan,administrator,peneliti, hingga pengembang piranti lunak jaringan. Tools dapat bekerja secara real time dalam menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa[2].

## 2. Keamanan Jaringan

Keamanan jaringan secara umum adalah komputer yang terhubung ke *network*, mempunyai ancaman kemanan lebih besar dari pada komputer yang berdiri sendiri (*standalone*). Dengan pengendalian yang teliti, resiko tersebutdapat dikurangi. Namun *network security* biasanya bertentangan dengan *network a ccess* semakin mudah, maka *network security* semakin rawan dan bila *network security* semakin baik, *network access* semakin tidak nyaman. Suatu *network* didesain sebagai komunikasi data *highway* dengan tujuan meningkatkan akses kesistem komputer, sementara *security* didesain untuk mengontrol akses. Penyediaan *network security* adalah sebagai aksi penyeimbang atara open *access* dengan *security.*




Gambar 1. Security Methodology

Menurut Garfinkel, seorang pakar keamanan komputer atau *computer security*, mencakup empat aspek yaitu yang pertama adah *privacy*, dimana aspek ini berhubungan dengan kerahasian informasi. Inti utama aspek *privacy* adalah bagaimana menjaga informasi ini dari orang yang tidak berhak mengaksesnya. Sebagai contoh, *e-mail* seorang pemakai tidak boleh dibaca oleh orang lain, bahkan oleh seorang administrator untuk melindungi aspek privacy ini dibutuhkan pengamanan menggunakan enkripsi. Aspek yang kedua adalah *integrity* berhubungan dengan keutuhan informasi. Inti utama

aspek *integrity* ini adalah bagaimana menjaga informasi agar tidak diubah tanpa izin pemilik informasi. Aspek yang ketiga adalah aspek authentication, aspek ini berhubungan dengan identitas atau jati diri atau kepemilikan yang sah. Sistem harus mengetahui bahwa informasi dibuat atau di akses oleh pemilik yang sah. Ada dua masalah yang terkait dengan aspek ini, yang pertama pembuktian keaslian informasi atau dokumen, yang kedua adalah *access control*.

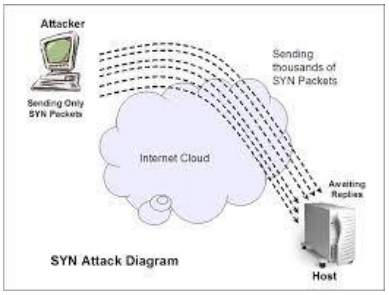
Salah satu usaha untuk memenuhi masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking dan digital signature Watermarking dapat digunakan untuk menjaga intellectual property, dengan menandai dokumen atau hasil karya dengan tanda tangan pembuat. Masalah kedua, yaitu accsess control, berkaitan dengan pembatasan hak akses orang yang dapat mengakses informasi. Cara standar yang digunakan untuk *access control* yaitu dengan login dan password

Aspek yang ke empat berupa aspek availa bility berhubungan dengan ketersediaan informasi. Contoh serangan terhadap aspek ini yaitu denial of service dimana *server* dikirimi permintaan palsu yang bertubi-tubi sehingga tidak dapat melayani permintaan yang lain. Kondisi ini menyebabkan informasi tidak dapat diakses.

### 2.1. Penyalahgunaan Protokol TCP

TCP (*Transmision Control Protocol*) adalah sebuah protokol yang menyediakan layanan pengiriman data, TCP merupakan protokol yang bersifat *connection-oriented*, *reliable*, *byte stream service*[3].

Connection oriented berarti dua aplikasi pengguna TCP harus melakukan pembentukan hubungan dalam bentuk pertukaran kontrol informasi (handshaking), sebelum, transmisi data terjadi. Realiable merupakan proses deteksi kesalahan paket TCP dan mentransmisikan kembali. *Byte stream service* merupakan paket yang dikirimkan dan sampai ketempat tujuan secara berurutan. Pada dasarnya jenis protkol TCP sulit untuk di salah gunakan. Kecuali penyusup mengontrol suatu router diantara dua system, penyusup itu dapat selalu dilacak keberadaannya serta penggunaan seperti penggunakan *syn attack*. Penyalahgunaan yang sering dilakukan dalam *protocol* ini adalah *syn attack*, *syn attack* adalah jenis serangan yang memnafaatkan kelemahan koneksi TCP, penyerang mengirimkan paket TCP SYN secara acak ke host tujuan akan mengim kembali paket SYN ACK. Serangan yang berjenis ini cukup sulit untuk di deteksi alamat pengumannya karena alamat *IP* dari pengirim tersebut telah disamarkan dengan menyeleksi paket router yang menghubungkan jaringan internet, terlihat seperti gambar 2.



Gambar 2. SYN TCP Attack

Gambar diatas menjelaskan bahwa paket SYN dengan alamat pengirim yang telah disamarkan, ketika paket SYN sampai ke *server*, selanjutnya *server* akan mengalokasikan buffer memori yang diperlukan. Lalu apabila pengalokasian memori sudah diberikan kepada host penyerang maka, host penyerang akan terus mengirimkan paket SYN yang telah dimanipulasi oleh penyerang dan alamat IP yang telah disamarkan. Host penyerang akan memaksa *server* untuk mengakumulasi koneksi setengah terbuka "*half open connection*" sehingga pada posisi puncaknya *server* tidak mampu mengakumulasi half open connection sehingga sumber daya yang dimiliki *server* lumpuh total.

Karena serangan SYN dengan alamat IP pengirim yang dipalsukan pada awalnya bukanlah suatu bentuk serangan yang mengonsumsi *bandwidth*, namun lebih kepada serangan yang mengonsumsi sumber daya *server*.

### 2.2. *Flood*ing data

*Traffic* data yang ada dalam suatu jaringan akanmengalami turun naikselama pemakainannya. Pada jam-jam sibuk *traffic* suatu data akan sangat padat sehingga *traffic* data tersebut akan terganggu. Baik data yang dikirm ataupun data yang akan datang akan mengalami antrian data yang mengakibatkan

Kelambatan dalam pengiriman data dan penerimaan data.Tetapi ada kalanya data-data yang berada dalam *traffic* merupakan data yang tidak perlu. Data-data tersebut memang sengaja dikirim oleh sesorang untuk merusak jaringan data yang ada. Pengiriman data tersebut dapat mengakibatkan lambatnya jalur *traffic* yang ada dalam jaringan, dan juga bisa mengakibatkan kerugian lain yang cukup berarti, misalnya kerusakan alat ataupun kerusakan program karena adanya intruder yang masuk ke dalam jaringan. Pengiriman data yang berlebihan baik dari besar paket maupun jumlah paket kedalam suatu jaringan dan umumnya merupakan data yang tidak berguna biasa disebut *flood*.

### 2.3. Wireshark

Wireshark banyak digunakan dalam memecahkan *troubleshooting* dijaringan untuk memeriksa keamanan jaringan, men-debug implementasi protocol jaringan dalam software mereka, melakukan *debugging* implementasi paket

protocol, serta belajar[4].

protocol dan banyak juga digunakan untuk sniffer atau mengendus data-data privasi dijaringan. Wireshark ini diibaratkan sebagai media atau tool yang dapat dipakai oleh user untuk penggunaanya, apakah untuk kebaikan atau kejahatan. Hal ini karena wireshark dapat digunakan untuk mencari informasi yang sensitif yang berkeliaran pada jaringan, contoh nya kata sandi, cookie dan lain sebagainnya.

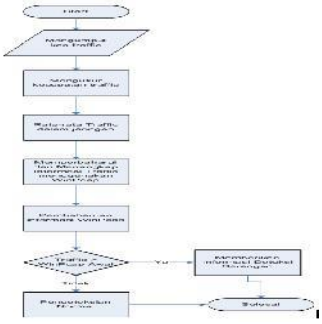
Wireshark dapat menganalisis paket data secara real time. Artinya aplikasi wireshark ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah di tentukan oleh user sebelumnya. Wireshark dapat menganalisa paket data secara real time artinya, aplikasi wireshark akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya.

Jika Komputer terhubung dengan jaringan kecepatan tinggi dan pada computer sedang digunakan aplikasi berbasis jaringan, aplikasi wireshark akan menampilakan banyak sekali paket data dan menimbulkan kebingungan karena ada begitu banyak paket data jaringan yang muncul. Aplikasi wireshark dapat memfilter jenis protocol tertentu yang ingin ditampilkan[5].

## 3. Analisa dan Perancangan

### 3.1. Analisa Sistem aktivitas illegal di dalam jaringan

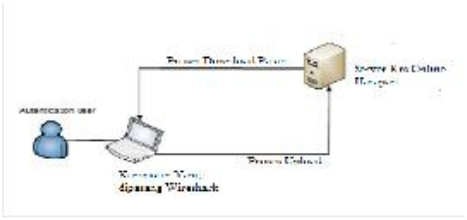
Analisa yang digunakan, yaitu analisa pengembangan sistem. Penelitian dengan pendekatan pengembangan, adalah suatu penelitian yang berusaha mencari pengaruh variabel tertentu, terhadap variabel yang lain dalam kondisi yang terkontrol. Metode penelitan yang dilakukan dengan menggunakan eksperimen secara langsung, dibawah ini adalah flowchart untuk proses aktivitas illegal di dalam jaringan.



Gambar 3. flowchart pendeteksian aktivitas illegal

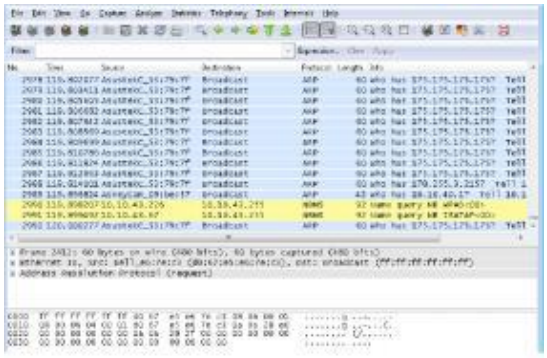
### 3.2. Perancangan Sistem jaringan untuk aktivitas ilegal

Pada bagian ini wireshark yang diuji coba menggunakan sistem operasi windows akan dijelaskan pada gambar 4 dimana pada gambar tersebut akan menjelaskan proses penangkapan aktivitas illegal yang terjadi di jaringan komputer



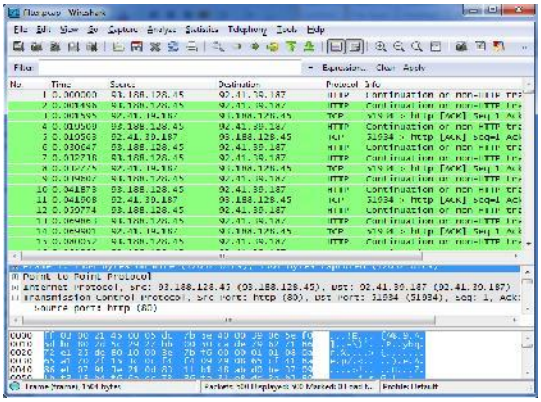
Gambar 4. penangkapan aktivitas illegal

Gambar diatas menjelaskan user diberikan hak akses berupa proses upload maka pada sistem yang akan dibangun menggunakan pembatas harddisk dengan menggunakan disk quota, jadi user tidak bisa melakukan upload secara sembarang karena telah dibatasi quota untuk melakuakan proses upload. Proses yang dilakukan tersebut diawasi oleh wireshark agar *user* dapat dengan aman meng-*upload* data tanpa perlu mengkawatirkan ada yang menyusupi pada saat melakukan *upload* data tersebut. Untuk melakukan *capture packet* sesuai dengan keinginan dari *user* dimana setelah memilih salah satu *interface* yang akan dipantau aktivitas jaringan secara *online* maka akan muncul seperti gambar dibawah ini



Gambar 5. *capture packet*

Dalam proses analisa aktivitas illegal di dalam jaringan, wireshark mampu untuk melihat atau menganalisis paket secara offline seperti ditunjukkan gambar 6, dimana penulis menyimpan file terlebih dahulu kedalam filter *.pcap. Dalam melakukan perancangan ini penulis memperoleh 500 aktivitas data dalam file ini.



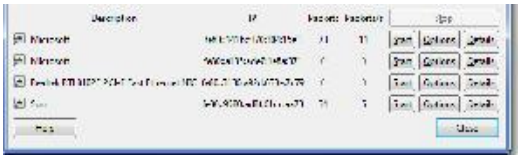
Gambar 6. Penangkapan paket secara offline

## 4. Hasil Pengujian

Hasil pengujian dibawah ini adalah pengujian aktivitas yang berhasil di-*capture* oleh wireshark terhadap informasi sumber, tujuan *protocol* dan waktu *capture*-nya.

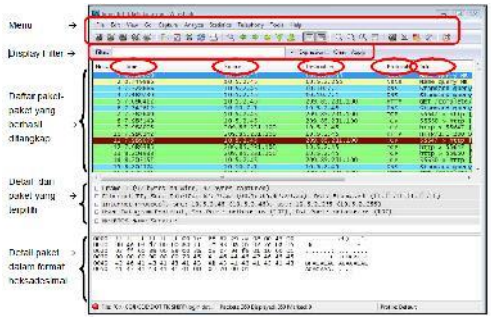
### 4.1. Pemfilteran Aktivitas Jaringan Secara Langsung

Apabila ingin memfilter aktivitas paket data jaringan secara langsung, kita dapat melakukannya ketika membuka *interface* yang ingin digunakan seperti terlihat gambar dibawah ini.



Gambar 7. *Interface* untuk pemfilteran paket

Gambar 7 menjelaskan bagaimana wireshark dapat menangkap aktivitas illegal di dalam jaringan setelah memillih *interface* yang akan ditangkap untuk dianalisa, apabila dalam proses tersebut sudah selesai maka klik tombol start untuk memulai proses *capture* packet kemudian aplikasi wireshark akan melakukan pemfilteran dan hasilnya akan di tampilkan pada layar wireshark untuk pengujian, penulis memfilter dan menganalisa paket HTTP tcp port 80 maka hasil penangkapan paket tersebut seperti gambar dibawah ini.




Gambar 8. Paket yang dianalisis

## 5. Kesimpulan

Dari data yang didapatkan mengenai protocol jaringan hasil dari pemfilteran paket data menggunakan wireshark adalah pada wireshark untuk memfilter paket caranya cukup mudah dibandingkan dengan aplikasi seperti *forensic tools snort* karena memerlukan penyetingan pada snort.conf sementara pada wireshark hanya cukup memilih filter paket pada kolom filter. Sehingga *administrator* jaringan dapat menganalisa paket jaringan yang sedang berlangsung.

## 6. Daftar Pustaka

[1] Ariyus, D. 2007. Intrusion Detection System. Penerbit Andi: Yogyakarta.

[2] Ariyus, D. 2006. Computer Security. Penerbit Andi: Yogyakarta.

[3] Pratama, A. J. 2010 Design And Implementation Of Data *Flood*ing Prevention On Computer Network dalam Undergraduate Theses Teknik Informatika ITS Surabaya (ict.binus.edu/metamorph/file/research/MA ID_JOURv2.0.pdf diakses tanggal9 November 2015)

[4] Kurniawan, A. 2010. Network Forensics Wireshark. Penerbit Andi: Yogyakarta

[5] Ramadhani, K. B. 2011. Pengamanan Jaringan Komputer Pascasarjana UPN "Veteran" Jatim menggunakan metode "IDS (Intrusion Detection System)" Dari Aktifitas dalam tesis Pasca sarjana UPN Veteran Jatim