Nama : Agus Salim (1410651169)

Kelas : A

1. Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

Jawab :

In this CISSP Essentials Security School lesson, Domain 4, Software Development Security, expert CISSP exam trainer Shon Harris details how applications and systems are structured, what security mechanisms and strategies are commonly used to secure data during access, processing and storage; it also presents some of the common threats and countermeasures. Before watching the special Domain 4, Software Development Security video below, students are encouraged to read the Domain 4 spotlight article, which provides an overview of the concepts presented in the video, including system development processes, namely the models, methods life cycle phases, and management of the development process; database systems and their components, models, management systems, query languages, data warehousing and mining, schema and security measures; application development methodology, covering software architecture, programming languages and concepts, change control methods, improvement models, data modeling and structures, data interface and exchange methods, artificial neural networks and expert systems; and security threats and countermeasures, the common threats to applications and systems and how expert techniques and artificial neural networks can be applied to mitigate threats.

2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

Jawab :

Analisa Jaringan dengan Menggunakan Program Wireshark

Wireshark adalah sebuah program analisa paket jaringan yang akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket sedetail mungkin. Sangat mudah dipakai karena meggunakan GUI dan merupakan freeware (software gratis). Sering digunakan oleh analisis jaringan komputer, untuk menganalisa protokol seperti SNMP, ARP, ICMP, HTTP. Dapat melogikakan atau memikirkan sebuah packet analyzer jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan. Wireshark adalah mungkin salah satu analisa terbaik paket open source yang tersedia saat ini.

Beberapa tujuan penggunaan wireshark :

- administrator jaringan menggunakannya untuk memecahkan masalah jaringan
- insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan
- pengembang menggunakannya untuk men-debug implementasi protocol
- beberapa orang menggunakannya untuk mempelajari protokol jaringan internal

Beberapa fitur yang terdapat pada wireshark :

- Tersedia untuk UNIX dan Windows.
- Capture paket data langsung dari antarmuka jaringan.
- Menampilkan paket dengan informasi protokol yang sangat rinci.
- Buka dan Simpan data paket yang diambil.
- Impor dan Ekspor paket data dari dan ke banyak program capture lainnya.

- Menyaring paket pada banyak kriteria.
- Pencarian untuk paket pada banyak kriteria.
- Colorize menampilkan paket berdasarkan filter.

Bagian-bagian pada wireshark

- Packet List Pane menampilkan ringkasan dari paket-paket yang tertangkap oleh Wireshark.
- Packet Detail Pane menampilkan detail dari paket yang dipiliha pada Packet List Pane.
- Packet Byte Pane menunjukkan isi data dari sebuah paket dalam heksadesimal serta menunjukkan detail dari field yang dipilih pada Packet Detail Pane.

Wireshark sebagai salah satu packet sniffer dapat diartikan sebagai sebuah program atau tool yang memiliki kemampuan untuk “mencegat” dan melakukan pencatatan terhadap traffic data dalam jaringan. Selama terjadi aliran data dalam jaringan, packet sniffer dapat menangkan protocol data unit (DPU), melakukan dokoding serta analisis terhadap isi paket berdasarkan spesifikasi RFC atu spesifikasi-spesifikasi yang lain.

Wireshark memiliki dua bahasa penyaringan : Satu digunakan saat menangkap paket-paket, dan satu digunakan ketika menampilkan paket- paket, adn satu digunakan ketika menampilkan paket. Pada bagian ini dapat mengeksplorasi jenis kedua filter yaitu filter tampilan.

Filter tampilan memungkinkan untuk berkonsentrasi pada paket anda tertarik ketika bersembunyi yang saat ini tidak menarika. Mereka memungkinkan untuk memilih paket oleh protokol, kehadiran lapangan, nilai lahan dan perbandingan antara bidang.

- Enkapsulasi

Enkapsulasi merupakan proses yang membuat satu jenis paket data jaringan menjadi jenis data lainnya. Enkapsulasi terjadi ketika sebuah protokol yang berada pada lapisan yang lebih rendah menerima data dari protokol yang berada pada lapisan yang lebih tinggi dan

meletakkan data ke format data yang dipahami oleh protokol tersebut. Beberapa jenis enkapsulasi lainnya antara lain:

- Frame Ethernet yang melakukan enkapsulasi terhadap datagram yang dibentuk oleh Internet Protocol (IP), yang dalam datagram tersebut juga melakukan enkapsulasi terhadap paket data yang dibuat oleh protokol TCP atau UDP. Data yang dienkapsulasi oleh protokol TCP atau UDP tersebut sendiri merupakan data aktual yang ditransmisikan melalui jaringan.

- Frame Ethernet yang dienkapsulasi ke dalam bentuk frame Asynchronous Transfer Mode (ATM) agar dapat ditransmisikan melalui backbone ATM.

• Protokol Data Unit TCP

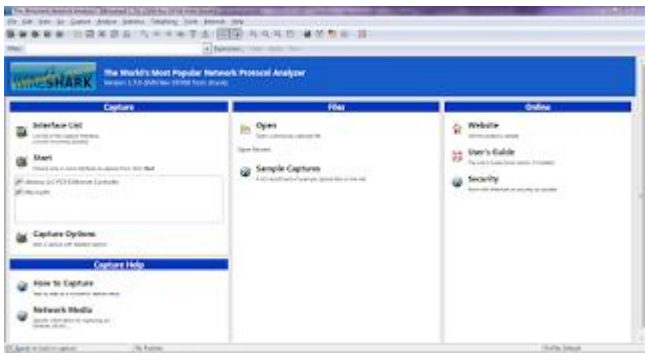
TCP harus berkomunikasi dengan IP pada lapisan di bawahnya (dengan menggunakan metode IP) dan aplikasi pada layer di atasnya (menggunakan ULP TCP). TCP juga harus berkomunikasi dengan implementasi TCP lain dalam jaringan. Oleh karena itu, untuk melakukan ini, digunakan protocol data unit (PDU).

• Protokol Data Unit UDP

UDP atau User Datagram Protocol adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP.

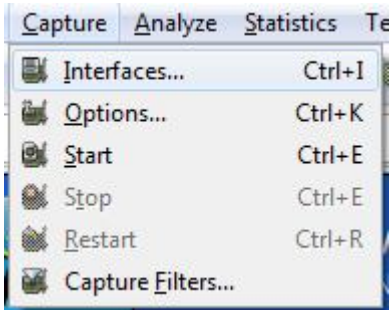
Cara Kerja Pelaksanaan

1. Instal program Wireshark dan buka programnya



2. Sambungkan koneksi ke jaringan wifi

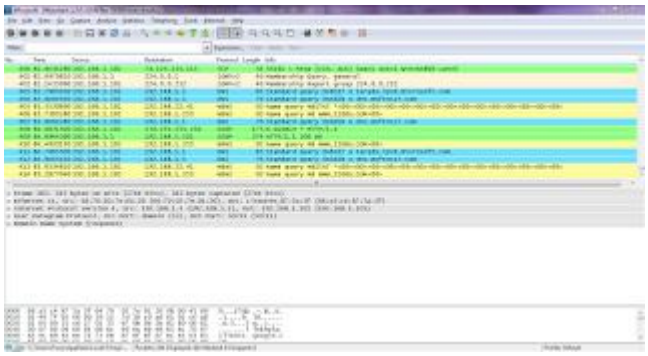
3. Klik menu Capture dan pilih Interfaces



4. Centang alamt IP address yang aktif dan klik Start

5. Akan muncul layar kosong, masuk ke web browser dan ketik alamat URL yahoo.co.id

6. Masuk ke program Wireshark dan awalnya layar kosong, akan terlihat komunikasi data pada layar



7. Amati pada Hypertext Transfer Protocol

a. Server : YTS/1.20.20\r\n

b. Content Type : text/plain, charset = utf-8\r\n

c. Date : Tue, 12 Februari 2013 06:05:33 GMT\r\n

- Pada box Transmission control protocol :

Source Port : http (80)

Destination Port : 53693(53693)

Header Length : 20 bytes

- Pada box Internet protocol :

Version : 4 ->

Header Length : 20 bytes ->

Source : 180.233.119.143 (180.233.119.143)

Destination : 192.168.137.54 (192.168.137.54) ->

- Pada box Ethernet II :

Src : LiteonTe_c4:aa:60(70:f1:a1:c4:aa:60),
Dst:LiteonTe_87:5a:3f(68:a3:c4:87:5a:3f)

Header Lenghth

- Pada box Frame :

Arrival Time : Feb 12, 2013 13:05:33:416319000 SE Asia Strandard Time

[Time delta from previous captured frame : 0.010630000 seconds]

[Time delta from previous displayed frame : 0.02025700 seconds]

[Time since reference of first frame : 10.299044000 seconds]

Frame number : 397

Frame length : 401 bytes (3208 bits)

Protocols in frame : eth:ip:tcp:http:data:data:data-text-lines

- Pada box Compurserve gif :

Version :

Screen width : screen height

Background_color index

Image position