UAS KEAMANAN INFORMASI

RESUME TENTANG

“Operations System”

Oleh :

AHMAT YAVI YULIAN

1310651133

Kelas B

TEKNIK INFORMATIKA

UNIVERSITAS MUHAMMADIYAH JEMBER

Keamanan Informasi

Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. “Keamanan Teknologi Informasi” atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan.

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

1. *Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability (ketersediaan)* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan perangkat lunak.

Informasi perlu dilindungi keamanannya

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan, secara umum diartikan sebagai “*quality or state of being secure-to be free from danger*” [1]. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lainnya. Strategi keamanan informasi memiliki fokus dan dibangun pada masing-masing ke-khusus-annya. Contoh dari tinjauan keamanan informasi adalah:

- *Physical Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- *Personal Security* yang overlap dengan ‘*phisycal security’* dalam melindungi orang-orang dalam organisasi.
- *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
- *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.

- *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Masing-masing komponen di atas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan, menyimpan, dan mengirimkannya . Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha .

Information Security Management System

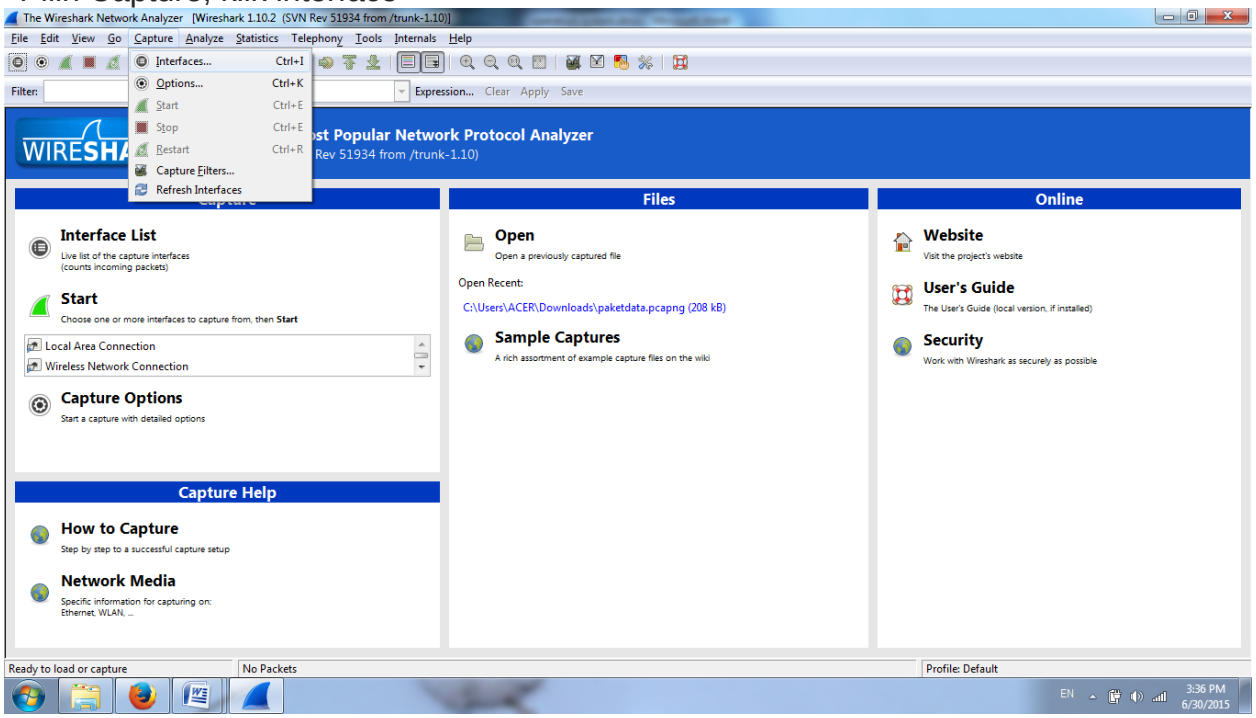
Information Security Management System (ISMS) merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan. Dan sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut:

- **Struktur organisasi**, biasarnya berupa keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi. Misalnya; Chief Security Offi cer dan beberapa lainnya.
- **Kebijakan keamanan,** atau dalam bahasa Inggris disebut sebagai *Security Policy*. Contoh kebijakan keamanan ini misalnya adalah sebagai berikut: Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk logon pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terkoneksi ke jaringan.
- **Prosedur dan proses,** yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur permohonan ijin akses aplikasi, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.
- **Tanggung jawab**, yang dimaksud dengan tanggung jawab atau responsibility di sini adalah tercerminnya konsep dan aspek-aspek keamanan informasi perusahaan di dalam job description setiap jabatan dalam perusahaan. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamaan informasi perusahaan untuk staf dan karyawannya.

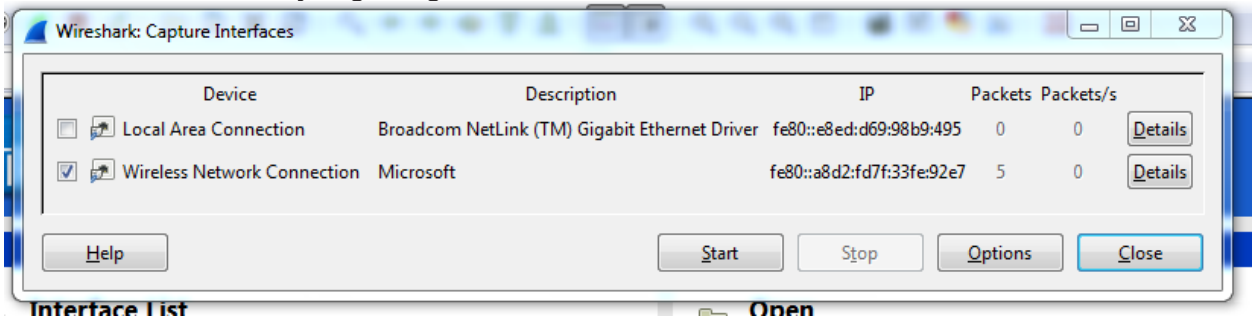
Sumber daya manusia, adalah pelaksana serta obyek pengembangan keamanan informasi di perusahaan. Manusia yang bisa memperbaiki serta merusak semua usaha-usaha tersebut.

2. Menganalisa paket yang keluar dan masuk dalam interface yang telah dipilih

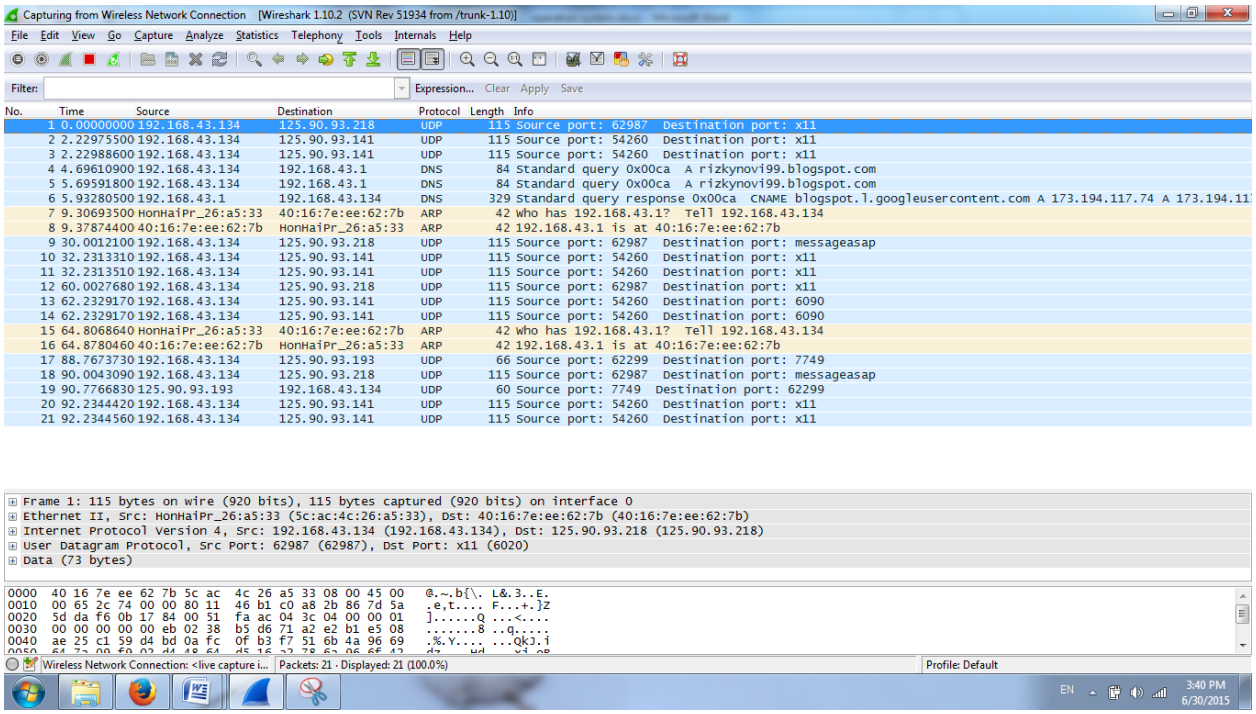
- Jalankan wireshark
- Pilih Capture, klik interface



- Pilih interface yang diinginkan, kemudian klik Start



- Hasil capture paket-paket yang lewat di jaringan. Tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp, dll.


Capturing from Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.00000000 192.168.43.134 125.90.93.218 UDP 115 Source port: 62987 Destination port: x11
2 2.22975500 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: x11
3 2.22988600 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: x11
4 4.69610900 192.168.43.134 192.168.43.1 DNS 84 Standard query 0x00ca A rizkynovi99.blogspot.com
5 5.69591800 192.168.43.134 192.168.43.1 DNS 84 Standard query 0x00ca A rizkynovi99.blogspot.com
6 5.93280500 192.168.43.1 192.168.43.134 DNS 329 Standard query response 0x00ca CNAME blogspot.l.googleusercontent.com A 173.194.117.74 A 173.194.11
7 9.30693500 HonHaiPr_26:a5:33 40:16:7e:ee:62:7b ARP 42 who has 192.168.43.1? Tell 192.168.43.134
8 9.37874400 40:16:7e:ee:62:7b HonHaiPr_26:a5:33 ARP 42 192.168.43.1 is at 40:16:7e:ee:62:7b
9 30.0012100 192.168.43.134 125.90.93.218 UDP 115 Source port: 62987 Destination port: messageasap
10 32.2313310 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: x11
11 32.2313510 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: x11
12 60.0027680 192.168.43.134 125.90.93.218 UDP 115 Source port: 62987 Destination port: x11
13 62.2329170 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: 6090
14 62.2329170 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: 6090
15 64.8068640 HonHaiPr_26:a5:33 40:16:7e:ee:62:7b ARP 42 who has 192.168.43.1? Tell 192.168.43.134
16 64.8780460 40:16:7e:ee:62:7b HonHaiPr_26:a5:33 ARP 42 192.168.43.1 is at 40:16:7e:ee:62:7b
17 88.7673730 192.168.43.134 125.90.93.193 UDP 66 Source port: 62299 Destination port: 7749
18 90.0043090 192.168.43.134 125.90.93.218 UDP 115 Source port: 62987 Destination port: messageasap
19 90.7766830 125.90.93.193 192.168.43.134 UDP 60 Source port: 7749 Destination port: 62299
20 92.2344420 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: x11
21 92.2344560 192.168.43.134 125.90.93.141 UDP 115 Source port: 54260 Destination port: x11
Frame 1: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface 0
Ethernet II, Src: HonHaiPr_26:a5:33 (5c:ac:4c:26:a5:33), Dst: 40:16:7e:ee:62:7b (40:16:7e:ee:62:7b)
Internet Protocol Version 4, Src: 192.168.43.134 (192.168.43.134), Dst: 125.90.93.218 (125.90.93.218)
User Datagram Protocol, Src Port: 62987 (62987), Dst Port: x11 (6020)
Data (73 bytes)
0000 40 16 7e ee 62 7b 5c ac 4c 26 a5 33 08 00 45 00 @.~.b{\. L&.3..E.
0010 00 65 2c 74 00 00 80 11 46 b1 c0 a8 2b 86 7d 5a .e,t.... F...+.}Z
0020 5d da f6 0b 17 84 00 51 fa ac 04 3c 04 00 00 01].....Q ...<....
0030 00 00 00 00 00 eb 02 38 b5 d6 71 a2 e2 b1 e5 08 ....8 ..q.....
0040 ae 25 c1 59 d4 bd 0a fc 0f b3 f7 51 6b 4a 96 69 .%.Y.... ...QkJ.i
Wireless Network Connection: <live capture i... Packets: 21 · Displayed: 21 (100.0%) Profile: Default
EN 3:40 PM 6/30/2015