UJIAN AHIR SEMESTER

KEAMANAN INFORMASI

Oleh

Nama **:NANANG SUGIYARTO**

Nim **:1310651087**

Kelas **:E**

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2014/2015

JAWABAN 1

Tujuan dari kontrol akses adalah untuk memungkinkan pengguna berwenang akses ke data yang tepat dan menolak akses ke pengguna yang tidak sah.Kontrol akses melindungi terhadap ancaman seperti akses yang tidak sah, modifikasi yang tidak pantas data, dan hilangnya kerahasiaan.

Untuk mencapai tiga tujuan utama: kerahasiaan, ketersediaaan, dan integrasi.
– Kerahasiaan: Untuk melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki hak akses. Sistem informasi eksekutif, sumber daya manusia, dan sistem pengolahan data transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi.
– Ketersediaan. Supaya data dan informasi yang tersedia bagi pihak-pihak yang memiliki hak akses untuk menggunakannya.
– Integritas. Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

Untuk mencapai tujuan keamanan informasi sebuah perusahaan yang mempunyai data yang di rahasiakan dan tidak ingin data tersebut di ketahui public, maka perusahaan tersebut harus menggunakan control akses untuk mencegah orang-orang yang tidak memiliki hak akses terhadap data tersebut tidak bisa mengakses sehingga data tetap aman dari orang-orang yang ingin mencuri atau merusak data perusahaan.

Digunakan sistem password untuk mencegah terjadinya pembobolan terhadap hak akses sehingga Cuma orang-orang tertentu atau orang yang memiliki password yang bisa mengakses data yang di rahasiakan. Ada dua macam password yang sering di gunakan dalam hak akses:

1. Password statis adalah password yang dapat digunakan kembali yang mungkin tidak berakhir.Mereka user-generated biasanya akan bekerja dengan baik ketika dikombinasikan dengan jenis otentikasi lain, seperti kartu pintar atau kontrol biometrik.Passphrase adalah password statis panjang, terdiri dari kata-kata dalam frase atau kalimat.Contoh passphrase adalah: "Aku akan lulus SEKOLAH dalam 6 bulan!" Passphrases dapat dibuat lebih kuat dengan menggunakan kata-kata omong kosong (menggantikan SEKOLAH dengan "xyzzy" di passphrase sebelumnya, misalnya), dengan mencampurkan kasus, dandengan menggunakan angka dan simbol tambahan.Satu kali password dapat digunakan untuk otentikasi tunggal.Mereka sangat aman tapi sulit untuk mengelola.Sebuah password satu kali tidak mungkin untuk menggunakan kembali dan berlaku hanya untuk satu kali penggunaan.
2. Password dinamis berubah secara berkala.RSA keamanan membuat perangkat tanda sinkron disebut SecurID yang menghasilkan kode token baru setiap 60 detik.Pengguna menggabungkan PIN statis mereka dengan RSA dinamis kode token untuk membuat satu password yang dinamis yang berubah setiap kali digunakan.Salah satu kelemahan bila menggunakan password yang dinamis adalah biaya token sendiri.

TEKNOLOGI AKSES KONTROL

Ada beberapa teknologi yang digunakan untuk pelaksanaan kontrol akses.Karena setiap teknologi disajikan, penting untuk mengidentifikasi apa yang unik tentang setiap solusi teknis.

Single sign-on

Sign-On tunggal (SSO) memungkinkan beberapa sistem untuk menggunakan server otentikasi pusat (AS).Hal ini memungkinkan pengguna untuk mengotentikasi sekali dan kemudian mengakses beberapa, sistem yang berbeda.Hal ini juga memungkinkan administrator keamanan untuk menambah, mengubah, atau mencabut hak pengguna pada satu sistem pusat.Kerugian utama untuk SSO itu memungkinkan penyerang untuk mendapatkan akses ke beberapa sumber setelah mengorbankan salah satu metode otentikasi, seperti password.SSO harus selalu digunakan dengan otentikasi multifaktor untuk alasan ini.

Menurut EDUCAUSE, "manajemen Identitas mengacu pada kebijakan, proses, dan teknologi yang membangun identitas pengguna dan menegakkan aturan tentang akses ke sumber daya digital.Dalam pengaturan kampus, banyak sistem-seperti informasi e-mail, sistem manajemen pembelajaran, database perpustakaan, dan komputasi grid-aplikasi mengharuskan pengguna untuk mengotentikasi diri (biasanya dengan username dan password).Sebuah proses otorisasi kemudian menentukan sistem yang pengguna dikonfirmasi diperbolehkan untuk mengakses.Dengan sistem manajemen identitas perusahaan, daripada memiliki kredensial yang terpisah untuk masing-masing sistem, pengguna dapat menggunakan identitas digital tunggal untuk mengakses semua sumber daya yang pengguna berhak.Manajemen identitas federasi izin-izin mendirikan memperluas pendekatan ini di atas tingkat perusahaan, menciptakan otoritas terpercaya untuk identitas digital di beberapa organisasi.Dalam sistem federasi, identitas pangsa lembaga yang berpartisipasi atribut berdasarkan disepakati standar, memfasilitasi otentikasi dari anggota lain dari federasi dan memberikan akses yang tepat untuk sumber daya online.Pendekatan ini arus akses ke aset digital sekaligus melindungi sumber daya terbatas.

Kerberos

Kerberos adalah layanan otentikasi pihak ketiga yang dapat digunakan untuk mendukung Single Sign-On. Kerberos menggunakan enkripsi simetris dan memberikan saling otentikasi kedua klien dan server.Ini melindungi terhadap jaringan mengendus dan ulangan serangan.

Dengan menggunakan sistem akses control maka data perusahaan tidak akan hilang atau di curi oleh orang yang tidak mempunyai hak akses data dengan menggunakan akses control single sigh on data akan aman dari orang-orang yang tidak memiliki hak akses yang ingin mengambil data perusahaan.

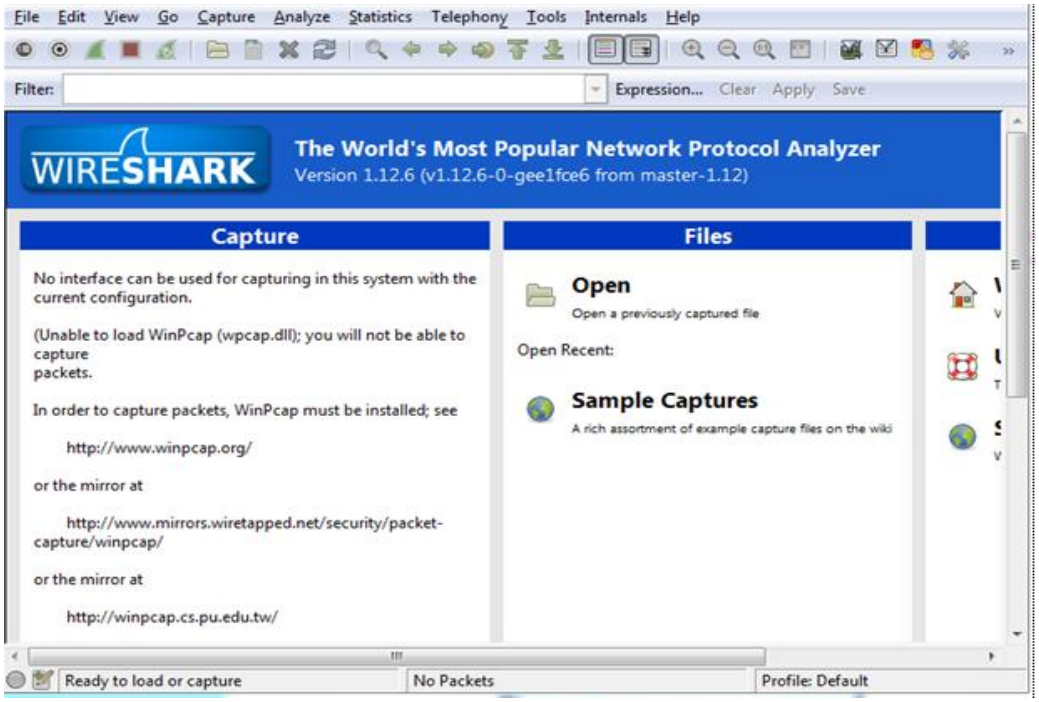
JWABAN 2

Tutorial penggunaan aplikasi wireshark

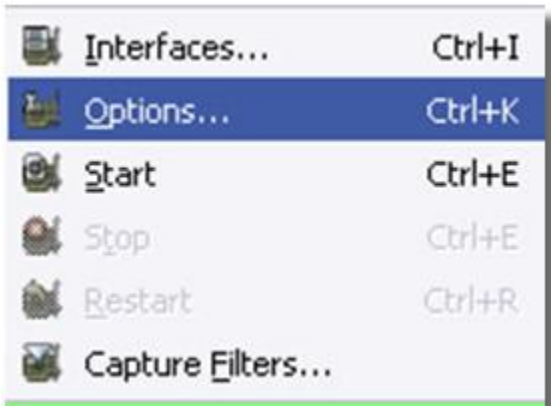
Pertama kita install aplikasi wireshark,

Setelah itu baru kita buka halaman web yang akan jadi target, yang akan menjadi target percobaan yaitu: http//blog.uad.ac.id/latif_ilkom/wp-admin. Sebelum melakukan login isikan dulu username dan password kita.

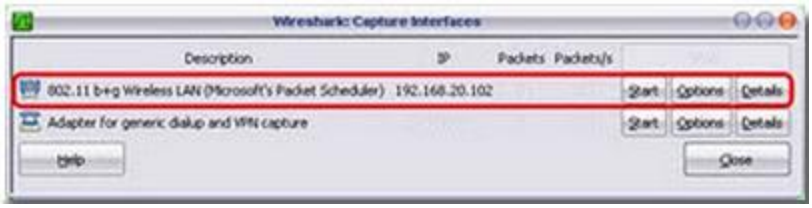
Pertama Bka program wireshark



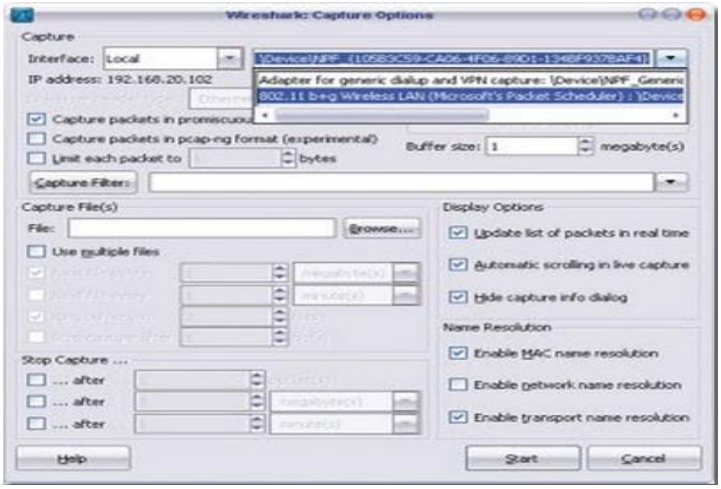
Setelah itu Masuk pada capture-option atau menekan tombol capture interface



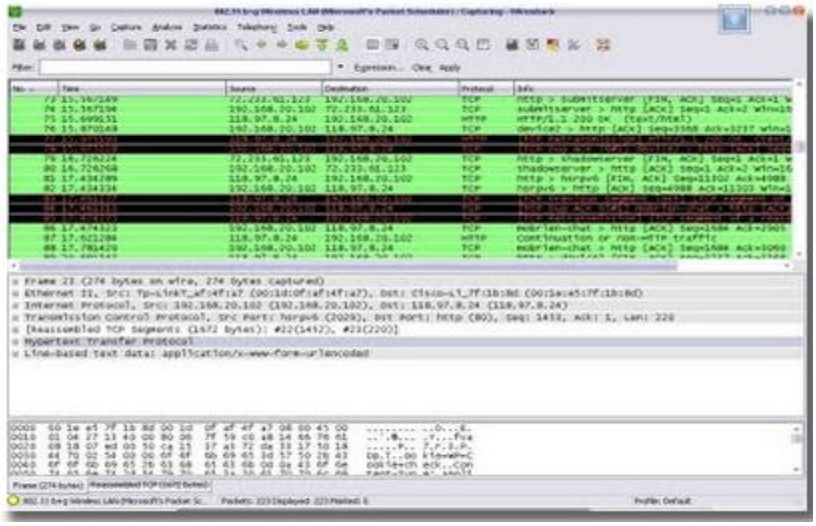
Akan muncul tampilan window capture interface seperti gambar di atas lalu tekan option pada Ethernet yang tersambung pada jaringan kita.



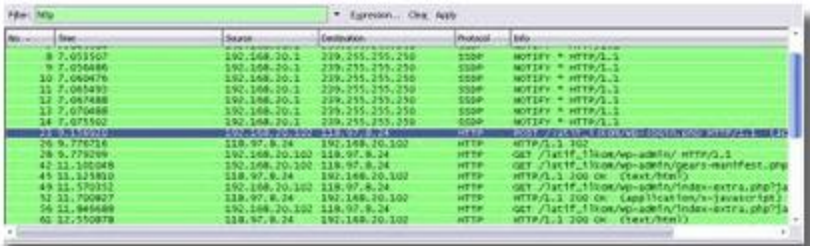
Pilih interface (network card) yang akan di gunakan untuk mengcapture packet, Dan pastikan capture paket dalam keadaan on



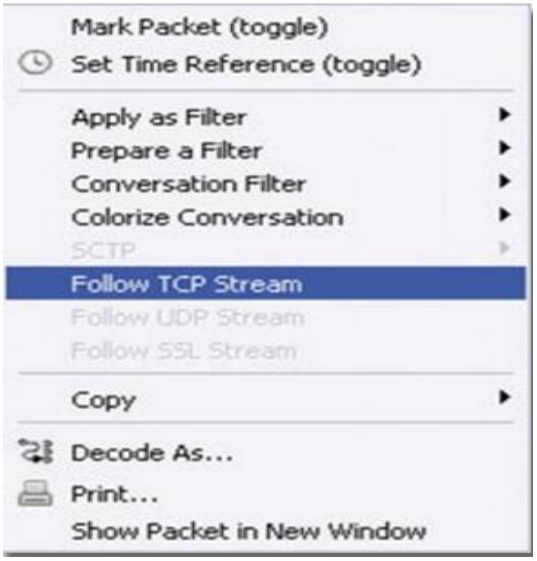
Untuk menyimpan record yang tercapture, bisa mengaktifkan kolom file seperti gambar di atas lalu pilih tombol start untuk memulai record.



Setelah muncul seperti gambar di atas clik tombol stop (Alt+E) setelah ada password yang masuk selama kita menekan tombol start.



Setelah itu carilah kata login, setelah menemukan kata login klik kanan pada paket tersebut, lalu pilih Follow TCP Stream seperti gambar di bawah.



Maka akan muncul informasi tentang paket yang kita pilih, di sini kita bisa melihat password dan username pada halaman blogspot tersebut