Tugas UAS Keamanan Informasi

Telekomunikasi dan keamanan jaringan

Nama : Sugiono Heri Saputro

Nim : 1310651053

Kls: C

UNIVERSITAS MUHAMMADIYAH JEMBER
FAKULTAS TEKNIK INFOMATIKA

2014-2015

Perangkat telekomunikasi bertugas menghubungkan pemakainya dengan pemakai lain. Kedua pemakai ini bisa berdekatan tetapi bisa berjauhuan. Kalau memilik arti harfiah dari telekomunikasi (tele = jauh, komunikasi = hubungan dengan pertukaran informasi) memang teknik telekomunikasi dikembangkan manusia untuk menebus perbedaan jarak yang jauhnya bisa tak terbatas menjadi perbedaan waktu yang sekecil mungkin.

Telecommunications and Network Security atau telekomunikasi dan keamanan jaringan Model OSI, Dan Kemudian setelah Anda mendapatkan ke bawah dan Anda tahu perangkat jaringan yang beroperasi pada tingkat yang, Anda dapat beralih gigi dan pergi ke model TCP / IP. Model TCP / IP adalah NITA (Sekarang Ini Benar-benar hebat). Dalam itu bukan "butuh" (seperti dalam minuman) itu NITA atau Network, Internet, Transportasi dan Aplikasi. Jadi, inilah perbandingan:
Dan ingat, Anda perlu tahu mana perangkat jaringan beroperasi pada lapisan yang,

Untuk TCP / IP Anda perlu memahami IPv4. Tahu Alamat Swasta, sudah ada tiga dari Mereka. Dan Anda harus tahu keuntungan dari IPv6. Jadi pertanyaan trik, karena rentang alamat dari oktet Dalam IPv4 skema pengalamatan adalah 0-254; 10.10.10.255 adalah alamat IP yang valid dan jika Anda mengatakan ya, maka apa yang akan dipergunakan untuk? Dalam IPv6 apa "::" mewakili. Jawabannya = apa-apa. Sebenarnya itu nol. Tapi perbedaan yang sama.

Anda seharusnya memahami perbedaan antara Analog dan Digital komunikasi; Asynchronous dan Synchronous antara; dan antara broadband dan baseband. Berbicara tentang komunikasi analog, apa kelemahan utama menggunakan modem yaitu Mereka dapat digunakan untuk menghindari firewall dan perangkat IDS / IPS.

Untuk percakapan wilayah jaringan, Anda perlu mengetahui istilah tradisional LAN, WAN, MAN, PAN, WLAN, PWLAN, dll Anda juga harus mengetahui konfigurasi BUS, STAR, RING, dan MESH. Sebuah pertanyaan yang baik adalah dalam konfigurasi yang akan Anda menemukan Hub Paling Mungkin.

Dan berbicara tentang hub, mari kita bicara sedikit tentang perangkat yang berbeda Anda boleh berada di berbicara berdamai dengan. Yaitu Mereka hub, switch, repeater, jembatan, gateway, PBX, firewall dan honeypots hanya untuk beberapa nama. Anda harus mencari di bulan Oktober Mana yang hanya maju semua lalu lintas; Mana yang penyaring lalu lintas berdasarkan alamat MAC dan yang mana yang paling mudah untuk hack.

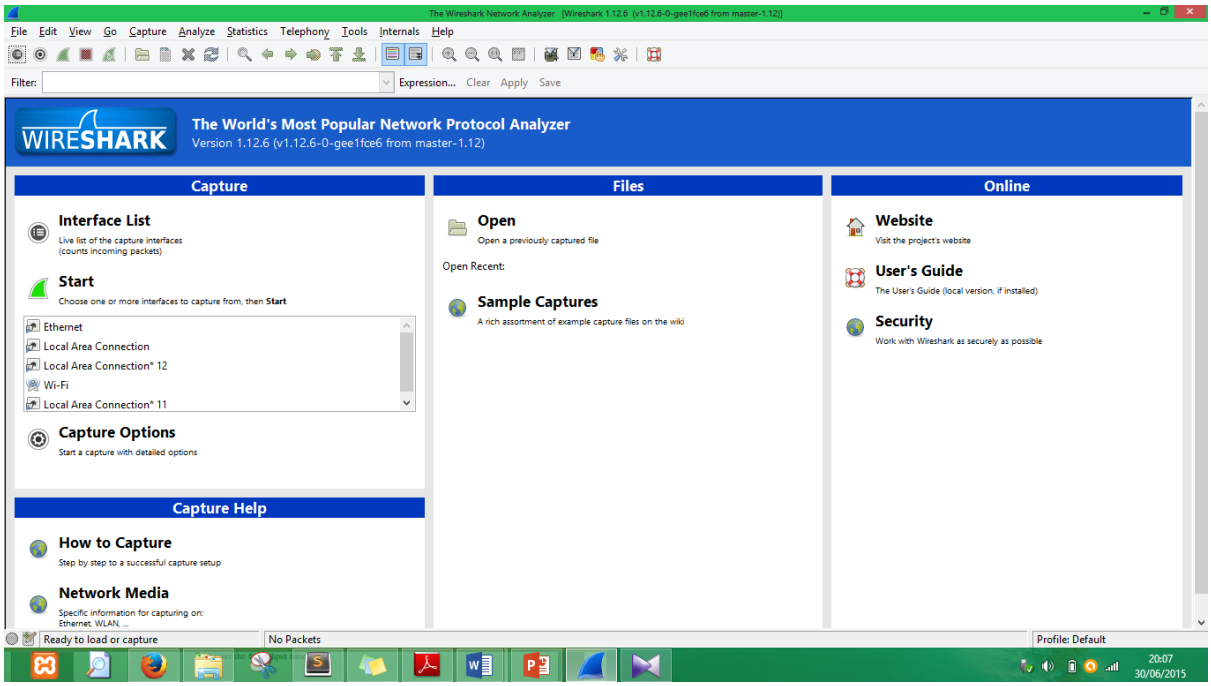
Dalam beberapa layanan dan protokol, memeriksa DNS, Terutama membaca rincian di belakang zona transfer dan Bagaimana Mereka bekerja. Kemudian melihat DHCP, layanan Active Directory, LDAP dan Kerberos. Bayar perhatian khusus untuk port yang dan menggunakan Kerberos Yang protokol yang digunakan untuk berkomunikasi antara klien dan Kerberos.

Remote akses semakin banyak perhatian dari (ISC) 2, sehingga membayar perhatian khusus pada bagaimana RADIUS mengotentikasi, mengapa ISDN (Ini masih tidak apa-apa) bukanlah pilihan yang baik, mengapa VPN dengan cepat Menjadi fakta bahwa standar untuk remote aman modem komunikasi dan mengapa tidak boleh pernah diizinkan di jaringan Anda.

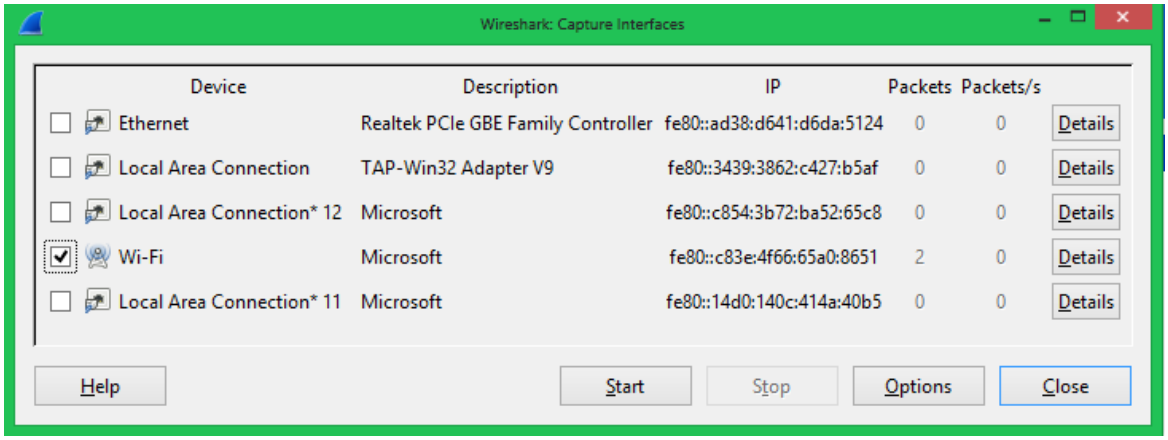
Wireless, ah nirkabel. Ini di mana-mana. Sebagian besar pendirian mengiklankan "GRATIS WIFI" Dan masing-masing tim profesional keamanan melihat que Mereka merasa ngeri, itu seperti menggantung tanda di leher Anda katakan di sini adalah userid dan password mandat. Tapi serius, mari kita lihat beberapa topik Anda harus Menjadi akrab dengan untuk ujian. Jadi untuk daftar cucian dari akronim, WEP, WPA, WPA2, 801.x (dan segala bentuk 801-802,11 termasuk A, B, G, N, I) dan jangan lupa SSID. Jangan SSID broadcast. Itu jawabannya, Anda hanya perlu ingat Ketika Anda sampai ke pertanyaan pada ujian. Anda juga harus memahami wardriving dan wardialing dan udara sniffing. Oh, dan sebelum aku lupa, biarkan aku menjawab dengan Blackberry dengan earphone remote menggunakan Bluetooth. Beberapa pertanyaan yang muncul di Bluetooth termasuk BlueScanner dan bluesniffer. Aku bahkan melihat beberapa pertanyaan pada versi terbaru yang lebih Yang menangani komunikasi nirkabel Apple untuk iPad dan lain lain.

No 2. Login ke elearning.unmuhjember.ac.id

Langkah pertama buka aplikasi wireshark seperti gambar di bawah ini



Pilih aplikasi wi-fi lalu pilih star seperti tampilan gambar di bawah ini



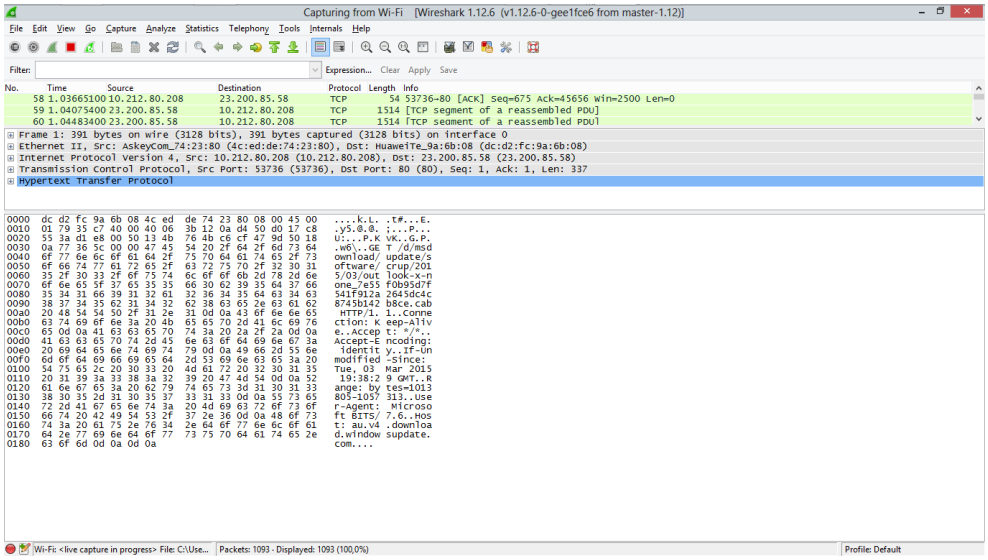
Buka web yang akan di coba seperti contoh : elearning.unmuhjember.ac.id

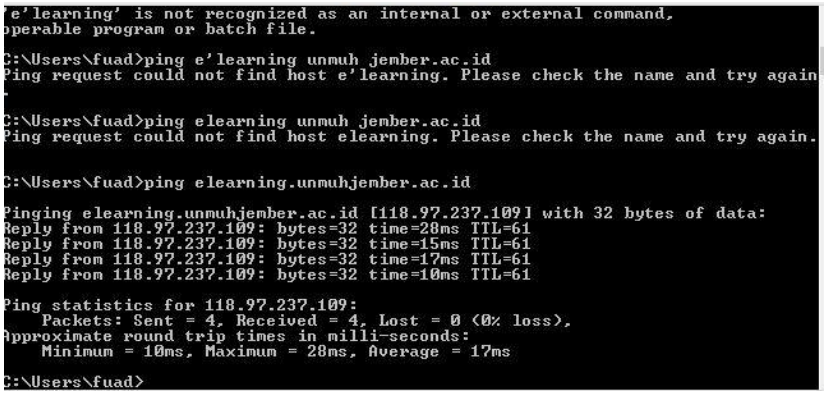
Tampilan seperti di bawah ini

Masukkan username dan kata sandi lalu login seperti biasa...

Ketika Selesai LOGIN, STOP Wreshark

Lihat Ipnya melalui cmd



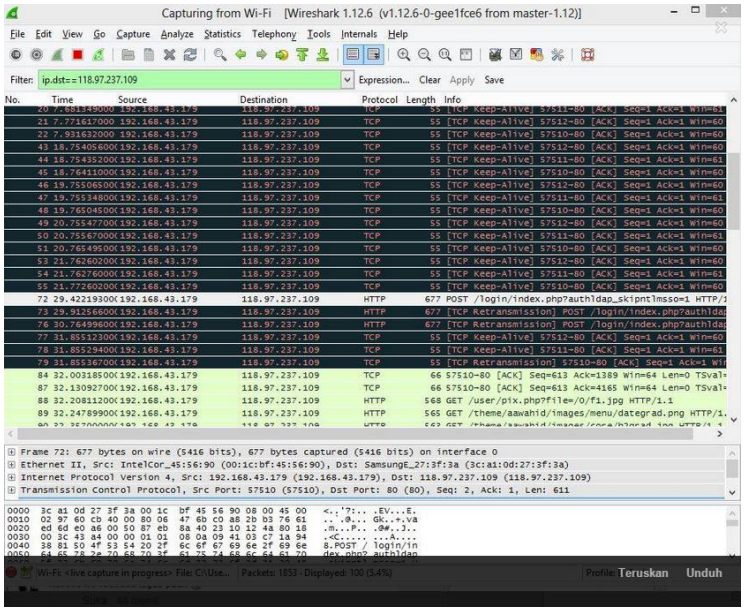


ip.dst==”118.97.237.109”

Filter ip nya dengan kode “ip.dst==”alamat IP”

Cari di info yg ada login.phpnya

Lihat di HTML Form URL Decoded



Maka akan terlihat passwordnya

Inilah yg dinamakan sniffing....

ALHAMDULILAH,,