IlmuKomputer.Com
Ikatlah ilmu dengan menuliskannya

Penyadapan Menggunakan Wireshark

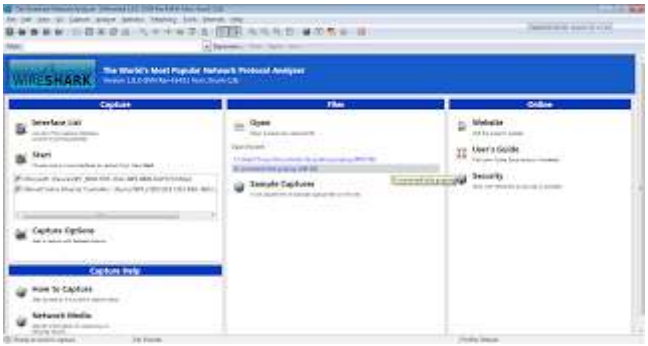
Firman Setya Nugraha

Someexperience.blogspot.com

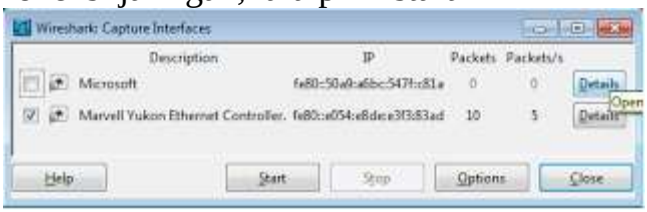
Firmansetyan@gmail.com

Kali ini saya akan mencoba cara sniffing jaringan menggunakan wireshark. Tapi, apakah sniffing itu??
Saya ambil dari wikipedia Indonesia, : “Sniffer Paket (arti tekstual: pengendus paket — dapat pula diartikan ‘penyadap paket’) yang juga dikenal sebagai Network Analyzers atau Ethernet Sniffer ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap-tiap paket dan terkadang menguraikan isi dari RFC (Request for Comments) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti hub atau switch), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk (promiscuous mode) untuk "mendengarkan" semuanya (umumnya pada jaringan kabel).”

Secara singkat, sniffing, adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer. Contohnya, anda adalah pemakai komputer yang terhubung dengan suatu jaringan. Dengan aktifitas sniffing ini user dan password anda bisa di tangkap / dicapture sehingga isinya bisa dibaca oleh orang yang melakukan SNIFFING tadi.
Langsung prakter....
Pertama, yang saya lakukan adalah mempersiapkan software wireshark dan browser (saya menggunakan GC), buka wireshark

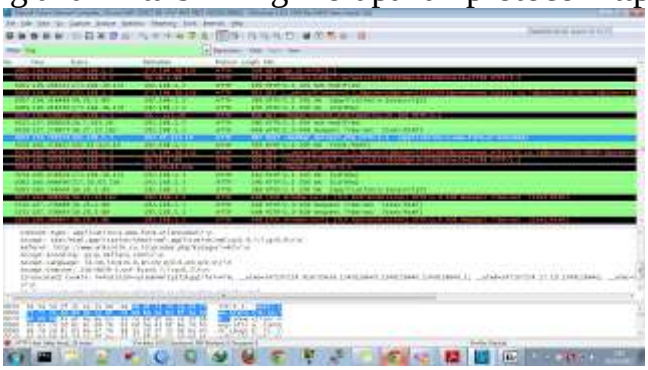


Lalu untuk memulai chapture paket, tekan Ctrl+I pilih hardware yang akan digunakan sebagai koneksi jaringan, lalu pilih start

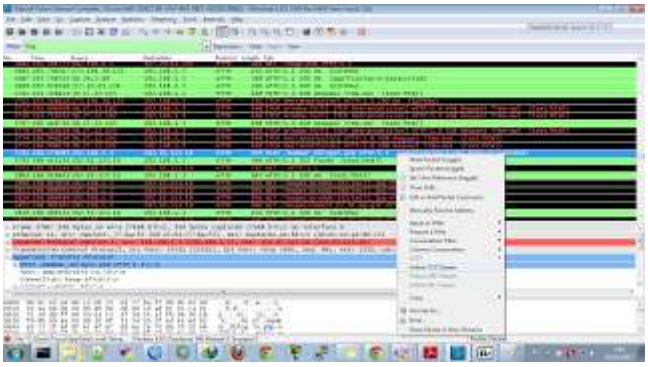


Kemudian, untuk simulasi (sebagai client yang akan memasukkan akun dan password) buka browser lalu masuk pada mikrotik.co.id. Lalu masukkan username dan password

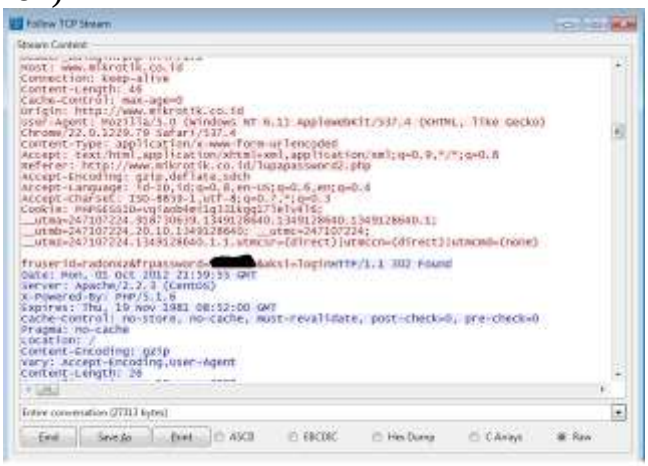
Sebagai sniffer, lihat hasil paket yang telah di sniffing, pada filter ketik "http" karena protokol yang akan kita sniffing merupakan protocol http.



Disana terlihat pada info ada keterangan "POST /member_dologin.php" kita klick kanan lalu pilih "follow tcp steam". Kegunaan follow tcp steam sendiri, untuk melihat data dari aliran TCP dengan cara melihatnya pada lapisan aplikasi (layer 7). Dapat digunakan untuk mencari password dalam aliran Telnet, atau untuk memahami aliran data.



Akan telihat tampilan sebagai berikut: disana tertera fruser id=radonxz & frpassword=(saya blok)



Jadi apabila kita menggunakan jaringan internet berhati-hatilah, karena mungkin saat kita memasukkan user dan password ada orang yang melakukan sniffing, pastikan jaringan yang anda gunakan memang aman.
Semoga bermanfaat....