Pengertian Singkat Tentang Sniffing

Lutfi Nur Niswati

lutfinurniswati@gmail.com
http://luppippa.blogspot.com

Lisensi Dokumen:
Copyright © 2003-2007 IlmuKomputer.Com
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Sniffing adalah kegiatan penyadapan pada lalu lintas data di jaringan komputer. contohnya apabila anda pemakai komputer yang terhubung dengan suatu jaringan dikantor. saat anda melakukan pengiriman email ke teman anda atau rekan anda yang berada diluar kota maka email tersebut akan dikirimkan dari komputer anda trus melewati jaringan komputer kantor anda (mungkin server atau gateway internet), trus keluar dari kantor melalui jaringan internet, lalu akan sampai diinbox email teman anda. Pada saat email tersebut melalui jaringan komputer kantor anda itulah *sniffing* bisa dilakukan. sniffing bisa dilakukan oleh administrator jaringan yang mengendalikan server, atau oleh pemakai komputer lain yang terhubung pada jaringan komputer anda,bisa jadi malah teman sebelah anda yang melakukan sniffing tersebut. sangat berbahaya apabila isi email tersebut ternyata penting.
sniffing dibagi menjadi 2 bagian :

1. Passive sniffing adalah suatu kegiatan penyadapan tanpa merubah data atau paket apapun dijaringan. paket sniffing yang umunya dilakukan yaitu pada Hub, hal ini disebabkan karena prinsip kerja hub yang hanya bertugas meneruskan signal ke semua komputer

(broadcast). berbeda dengan switch yang mempunyai cara untuk menghindari collision atau bentrokan yang terjadi pada hub dengan mambaca MAC address komputer. Beberapa program yang umunya digunakan untuk melakukan aktifitas ini yaitu wireshark, cain-abel, dsb.

2. Active sniffing adalah kegiatan sniffing yang dapat melakukan perubahan paket data dalam jaringan agar bisa melakukan sniffing, active sniffing dengan kata lain merupakan kebalikan dari passive sniffing. Active sniffing umunya dilakukan pada Switch, hal ini di dasar karena perbedaan prinsip kerja antara Hub dan Switch, seperti yang dijelaskan di atas. Active sniffing yang paling umum dilakukan adalah ARP Poisioning, Man in the middle attack (MITM).

cara mencegah sniffing hampir tidak ada, karena sniffing terjadi pada saat data sudah keluar dari komputer korban yang berada dalam satu jaringan. sehingga sniffer tidak menyerang langsung pada komputer korban. Untuk mencegah terjadinya sniffing maka anda jangan melakukan aktifitas yang sifatnya rahasia seperti Email, M-Banking, chatting rahasia dan lain sebagainya pada jaringan yang belum anda kenal sebelumhya.

itulah pengenalan tentang sniffing.. teknik tentang penggunaan wireshark (salah satu aplikasi untuk sniffing) bisa dilihat post selanjutnya...

Referensi

http://rodcysky.wordpress.com

http://luppippa.blogspot.com/2012/10/taukah-anda-tentang-sniffing.html

Biografi Penulis

Lutfi Nur Niswati. Lahir di Semarang pada Tanggal 29 Agustus 1991, dan sekarang masih terdaftar sebagai Mahasiswi POLITEKNIK NEGERI SEMARANG. Jurusan Teknik Elektro Program Studi D4 Teknik Telekomunikasi.

FB : Lutfi Nur Niswati

Copyright © 2003-2007 IlmuKomputer.Com