Network Sniffing

M Jafar Noor Yudianto
youdha_blink2@yahoo.co.id
http://jafaryudianto.blogspot.com/

Perkembangan jaringan komputer yang sangat pesat membuat keamanan jaringan sangatlah penting. Hal ini membuat keamanan jaringan sangatlah dibutuhkan. Maka dari itu saya akan mengulas salah satu teknik dalam keamanan jaringan yaitu *Network Sniffing*.

Network Sniffing adalah suatu aktifitas menyadap yang di lakukan dalam jaringan yang sangat sulit untuk di cegah, walaupun kita telah menginstall berbagai macam software untuk mencegah serangan dalam jaringan. ini adalah permasalahan dari komunikasi atau protokol jaringan dan tidak ada hubungannya dengan sistem operasi".

Aktifitas menyadap atau sniffing ini terbagi 2 jenis yaitu :

1. Passive Sniffing adalah suatu kegiatan penyadapan tanpa merubah data atau paket apapun di jaringan. Passive sniffing yang umum di lakukan yaitu pada Hub, hal ini di sebabkan 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 membaca MAC address komputer. Beberapa program yang umumnya di gunakan 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 umumnya di lakukan pada Switch, hal ini di dasar karena perbedaan prinsip kerja antara Hub

dan Switch, seperti yang di jelaskan di atas. Active sniffing yang paling umum di lakukan adalah ARP Poisoning, Man in the middle attack(MITM).

Sniffer paket dapat dimanfaatkan untuk hal-hal berikut:

- Mengatasi permasalahan pada jaringan komputer.
- Mendeteksi adanya penyelundup dalam jaringan (Network Intusion).
- Memonitor penggunaan jaringan dan menyaring isi isi tertentu.
- Memata-matai pengguna jaringan lain dan mengumpulkan informasi pribadi yang dimilikanya (misalkan password).
- Dapat digunakan untuk Reverse Engineer pada jaringan.

Beberapa sniffer yang terkenal adalah Wireshark (dulu namanya ethereal), Snort, TCPDump, Windump hingga sniffer yang lagi naik daun di kalangan Hacker yaitu Cain n Able yang saat posting artikel ini versi terakhirnya adalah 4.9.15 adalah produk dari Oxid.it.

Biografi Penulis

M Jafar Noor Yudianto. Saat menulis artikel ini sedang menjalani masa study D4 di Politeknik Negeri Semarang mengambil jurusan Elektro Program Studi D4 Telekomunikasi. Lahir pada 21 Juli 1991 di kota kudus.