TUGAS KEAMANAN JARINGAN KOMPUTER
ANALISA SNORT TREFIK SCANNING pada PT. Semen Batu Raja

NAMA: EDI SUKRISNO
NIM: 09011181320043

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

IDS

Deteksi penyusupan (Intrusion Detection) adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus. Program yang digunakan untuk pendeteksian disebut sebagai IDS (Intrusion Detection System (IDS).

Tipe Dasar IDS adalah

- Rule-based systems, berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mendeteksi Kemudian lintas sesuai dengan data dari database, maka pendeteksian tersebut langsung dikategorikan sebagai penyusupan.
- Adaptive systems, sama seperti Rule-based tetapi ditambah dengan teknik lain yaitu membuka kemungkinan untuk mendeteksi metode penyusupan yang baru.

Pendekatan yang digunakan dalam rule-based system ada dua, yaitu Preemptory (pencegahan) dan Reactionary (reaksi). Perbedaan dari kedua pendekatan tersebut adalah dalam waktu saja. Dalam Preemptory akan memperhatikan semua Kemudian-lintas jaringan. Apabila paket mencurigakan ditemukan maka program akan melakukan tindakan yang sesuai dengan paket mencurigakan tersebut. Reactionary, program hanya mengamati log. Jika ditemukan paket mencurigakan, program akan melakukan tindakan sesuai dengan paket tersebut.

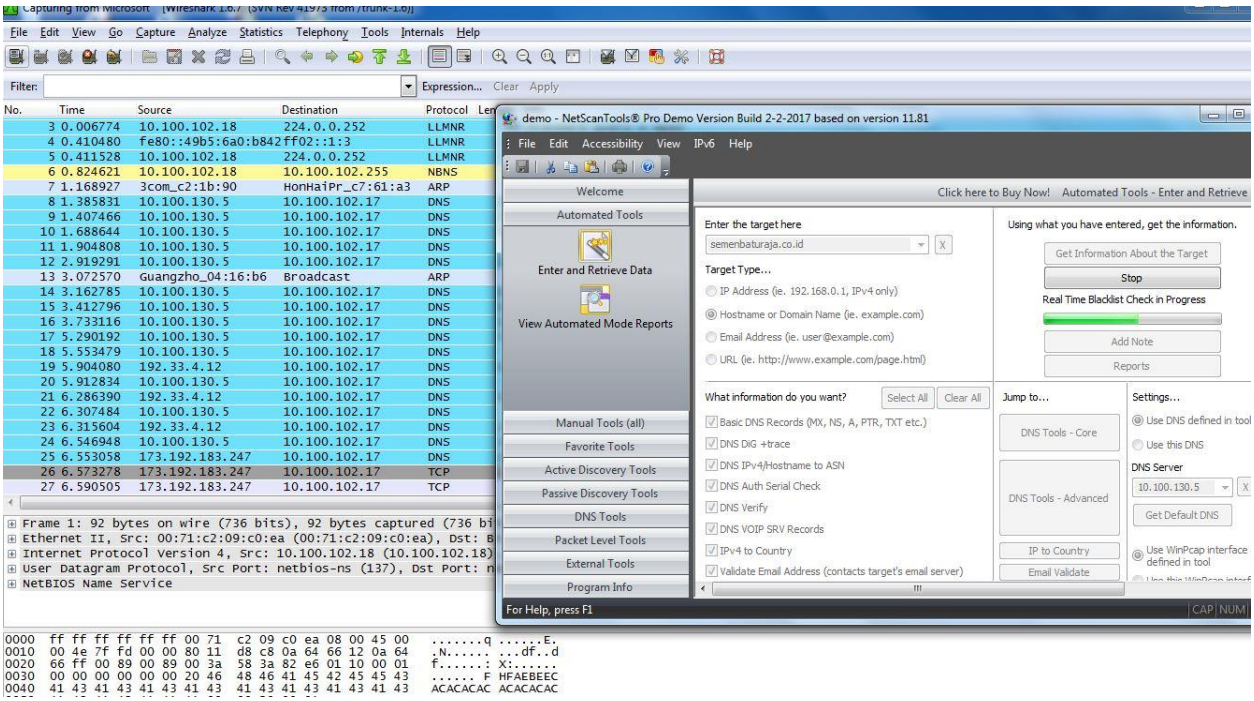
SNORT

Snort adalah deteksi intrusi jaringan dan sistem pencegahan. Ini adalah teknologi yang paling banyak digunakan dari jenisnya di dunia. Ia melakukan deteksi dengan menggunakan berbagai metode, termasuk aturan-berbasis deteksi, deteksi anomali, dan analisis heuristik Kemudian lintas jaringan.

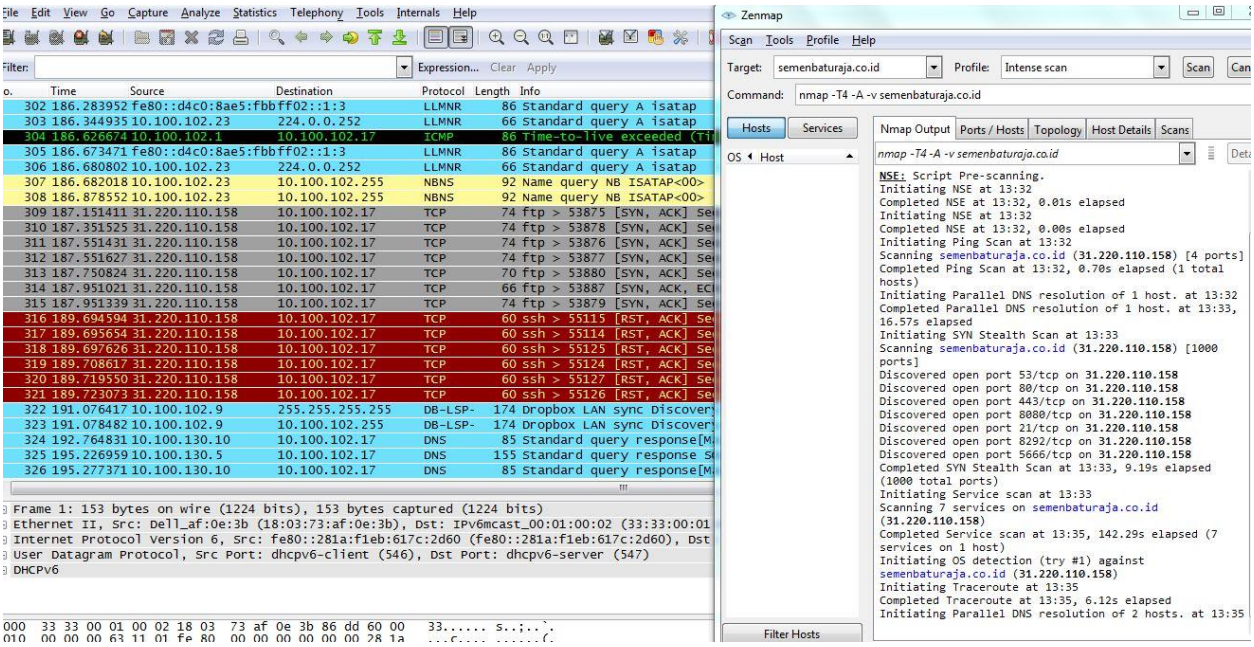
Aplikasi yang di gunakan dalam percobaan yaitu :

1. Nmap
2. Netscan
3. Super scan

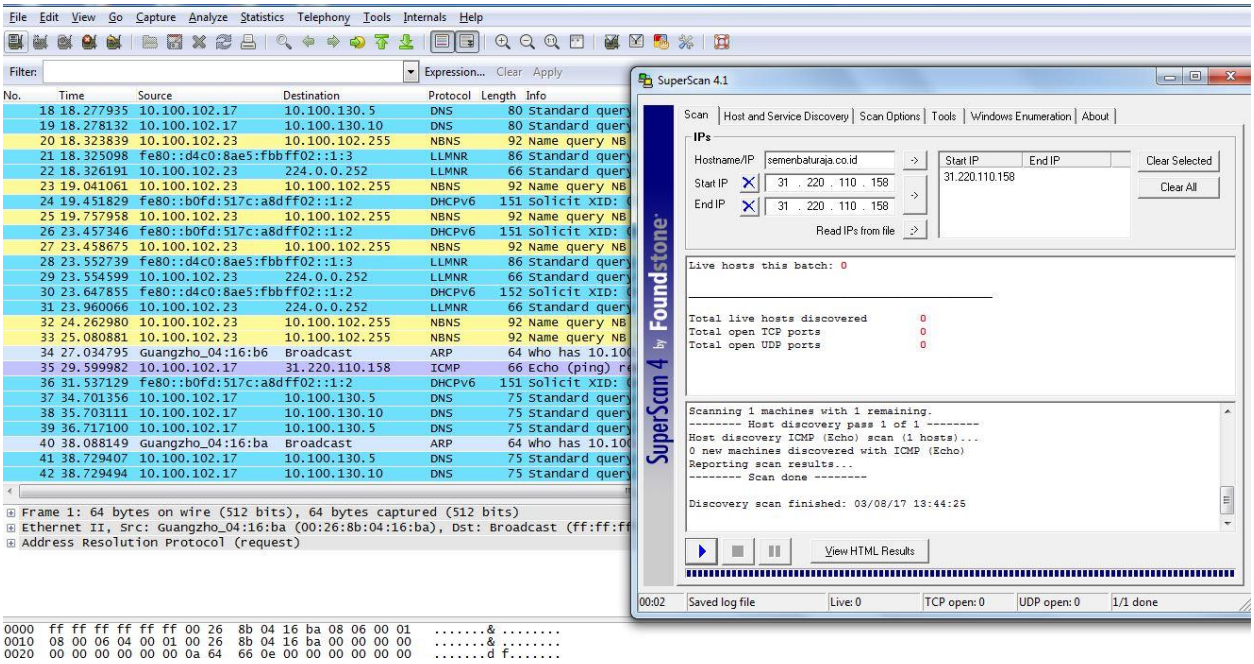
Berikut ini percobaan scanning dengan aplikasi diatas yaitu:



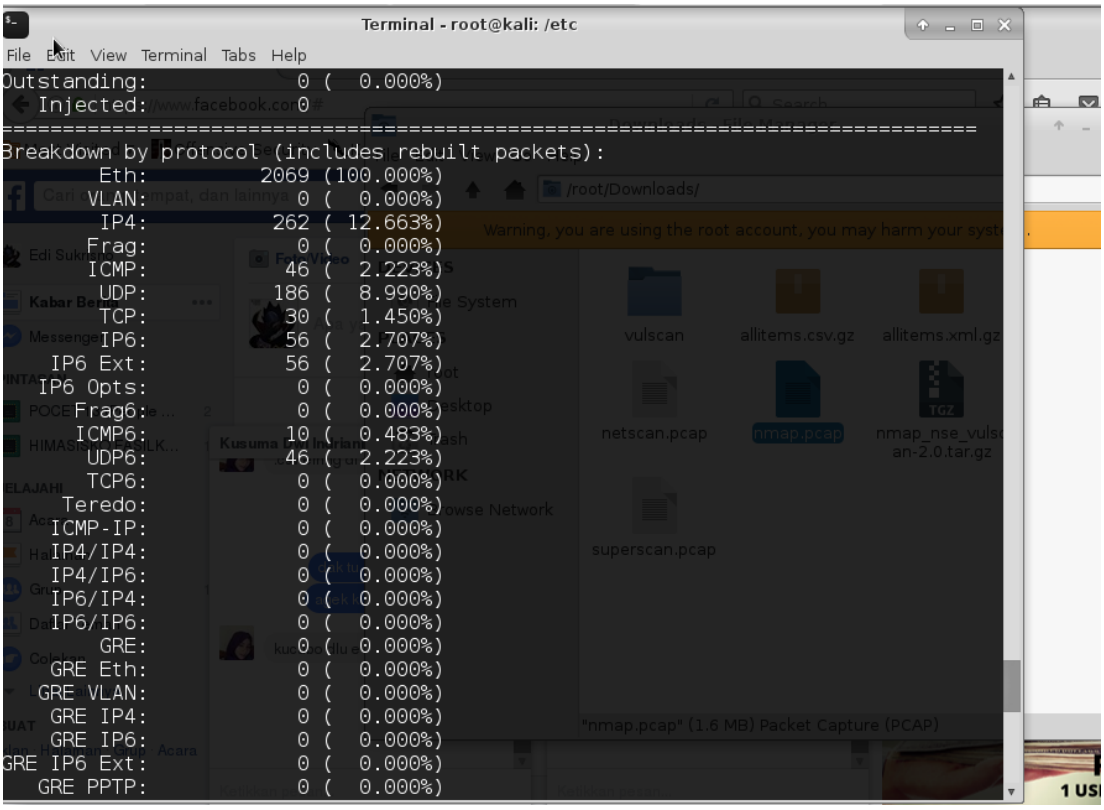
Gambar 1. Scanning dengan aplikasi netscan



Gambar 2. Scanning dengan aplikasi nmap



Gambar 3. Scanning dengan aplikasi superscan



Gambar 4. Hasil dengan menggunakan snort

Tabel Alert dari snort

No	Aleart	Jumlah
1	ICMP	46
2	TCP	30
3	UDP	186
4	ARP	40

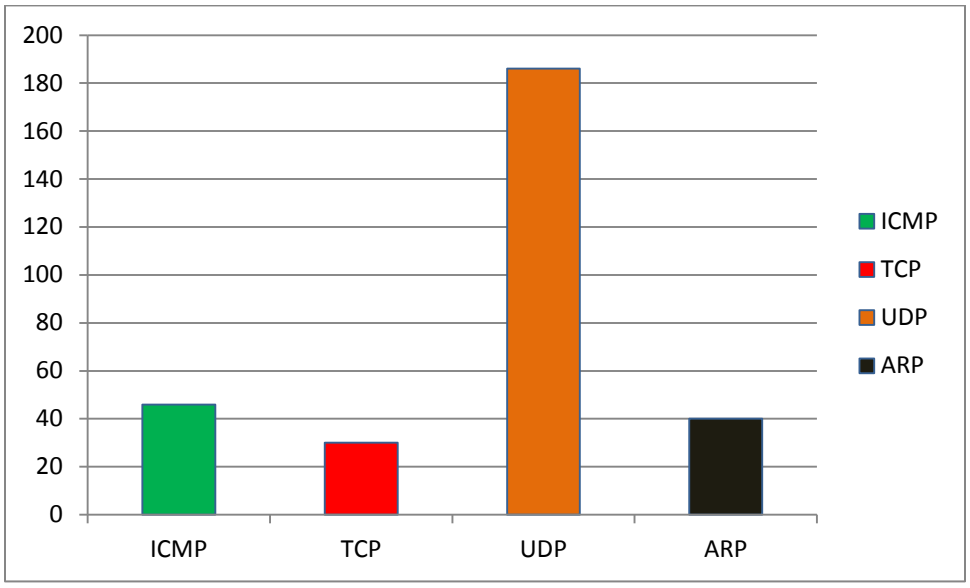


Diagram.1 Hasil diagram pada output snort