KEAMANAN JARINGAN KOMPUTER

Eko Pratama

09011181320004

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

TUGAS 4

INSTRUCTION DETECTION SYSTEM MENGGUNAKAN SNORT

Instruction Detection System (IDS) adalah sebuah system yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan kegiatan yang mencurigakan didalam sebuah system jaringan. Dimana pada Tugas kali ini saya akan melihat traffic yang ada pada situs Krakatausteel.com dengan menggunakan aplikasi snort. Aplikasi snort sendiri berfungsi sebagai sniffer dan packet logger pada sebuah jaringan selain itu snort dapat digunakan untuk mendeteksi sebuah serangan.

TUGAS : scanning situs target sambil menjalankan wireshark, kemudian compile menggunakan snort, lihat apa yang terjadi? (ketika telah mendapatkan data alert buat table dan grafiknya)

1. TARGET SITUS DAN TOOLS YANG DIGUNAKAN

Pada tugas ke-4 ini saya masih melakukan scanning terhadap perusahaan PT. krakatau steel yang memiliki IP 118.97.204.70, kemudian saya menggunakan beberapa tools untuk membantu melakukan tugas ini, berikut merupakan toolsnya:

- **Wireshark :** merupakan sebuah tools yang digunakan untuk menganalisa traffic dari sebuah jaringan
- **Nmap :** merupakan sebuah alat bantu untuk melakukan scanning pada target yang dituju

2. LANGKAH-LANGKAH YANG DILAKUKAN

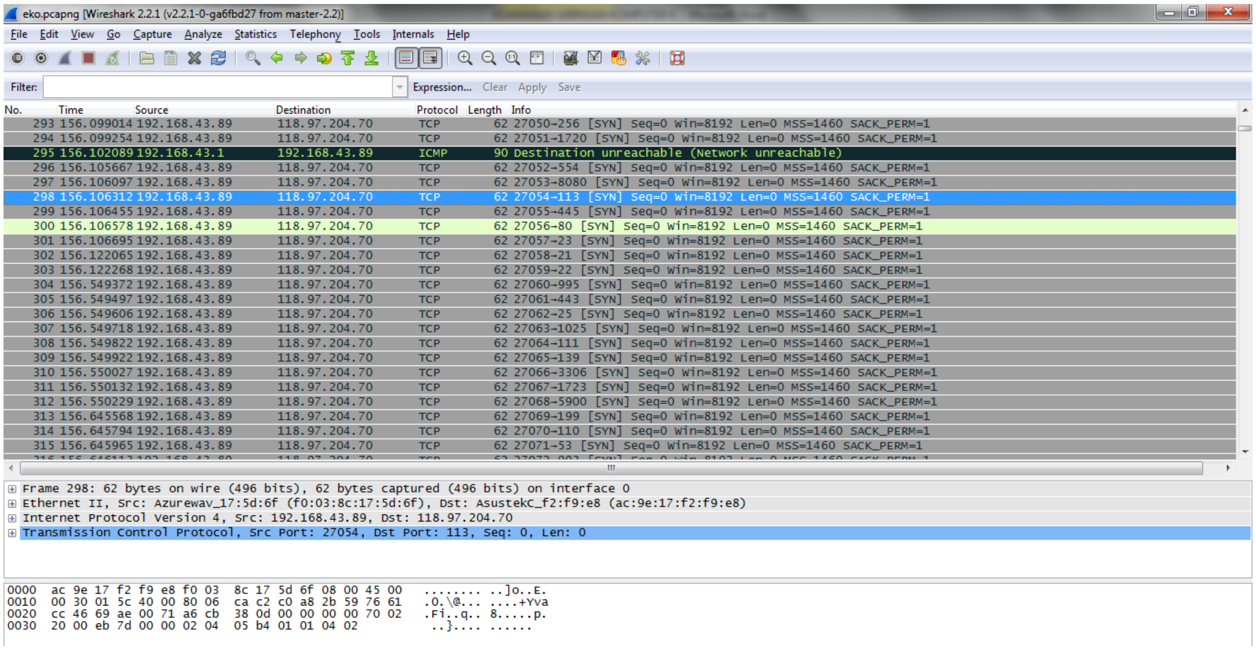
Langkah yang dilakukan untuk tugas kali ini dapat dilihat seperti beberapa gambar dibawah ini:

- **Buka wireshark sambil melakukan scanning**

```
root@Server:/home/server# nmap -O 118.97.204.70

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-07 01:19 EST
Nmap scan report for 118.97.204.70
Host is up (0.00079s latency).
All 1000 scanned ports on 118.97.204.70 are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.17 seconds
root@Server:/home/server# nmap -v -sX 118.97.204.70

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-07 01:22 EST
Initiating Ping Scan at 01:22
Scanning 118.97.204.70 [4 ports]
Completed Ping Scan at 01:22, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:22
Completed Parallel DNS resolution of 1 host. at 01:22, 13.00s elapsed
Initiating XMAS Scan at 01:22
Scanning 118.97.204.70 [1000 ports]
Completed XMAS Scan at 01:22, 1.40s elapsed (1000 total ports)
Nmap scan report for 118.97.204.70
Host is up (0.000073s latency).
All 1000 scanned ports on 118.97.204.70 are closed
```

Gambar 2.1 Scanning

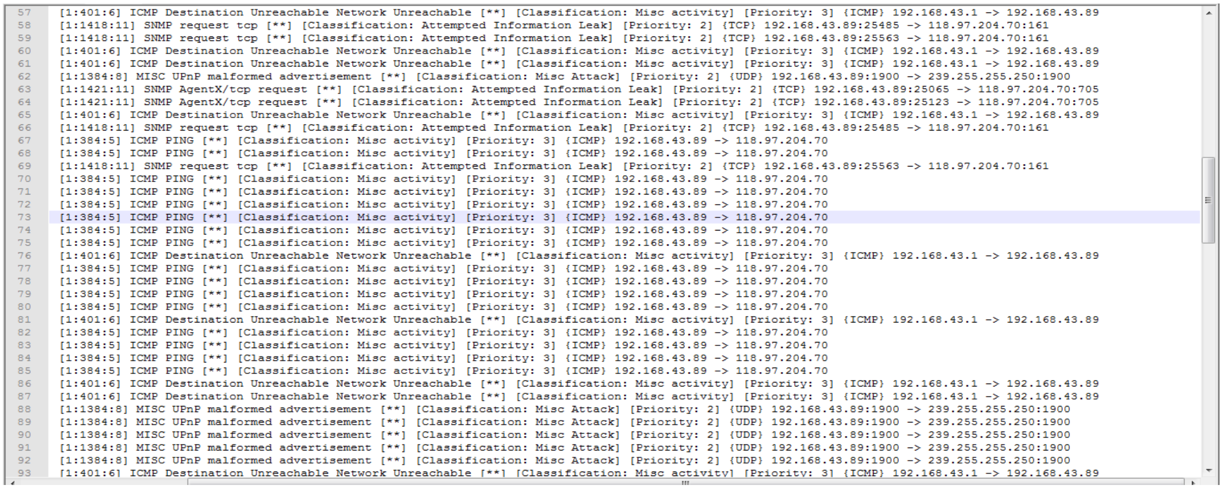
Pada gambar 2.1 saya melakukan scanning terhadap situs target www.krakatausteel.com dimana saat melakukan scanning saya menjalankan aplikasi wireshark untuk melihat traffic data yang terjadi saat melakukan scanning. Pada gambar 2.2 dibawah merupakan hasil dari traffic di aplikasi wireshark saat melakukan scanning.



Gambar 2.2 Traffic data pada Wireshark

- **Compile data menggunakan Snort**

Setelah mendapatkan hasil pcap dari wireshark lakukan compile file pcap dengan perintah snort –A fast –c /etc/snort/snort.conf –r (tempat direktori file pcap tersimpan) lalu jika tidak terdapat error lihat apakah data alert berhasil didapatkan. Berikut screenshoot hasil alert yang didapatkan



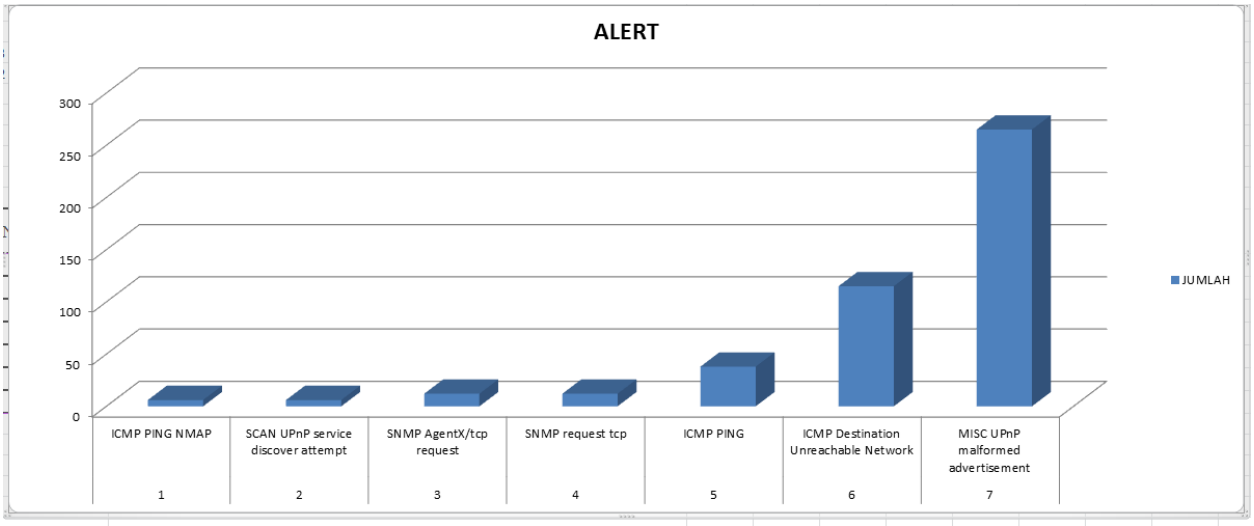
Gambar 2.3 Data Alert

Setelah berhasil mendapatkan alert kita melakukan compile terhadap data alert dengan alat bantu countalert.py yang dimana alat bantu tersebut merupakan tools dengan bahasa python yang berfungsi untuk mengekstrak data alert yang telah didapatkan. Setelah melakukan ekstrak didapatlah hasil dari traffic yang telah kita lakukan dengan wireshark.

3. HASIL SAJIAN DATA

Setelah mendapatkan data berikut merupakan tampilan dari hasil sajian data alert berupa table dan grafik

NO	ALERT	JUMLAH
1	ICMP PING NMAP	6
2	SCAN UPnP service discover attempt	6
3	SNMP AgentX/tcp request	12
4	SNMP request tcp	12
5	ICMP PING	38
6	ICMP Destination Unreachable Network	115
7	MISC UPnP malformed advertisement	265



Gambar 3.1 Grafik alert