Tugas Mata Kuliah

KEAMANAN JARINGAN KOMPUTER

Nama : Faris Abdul Aziz

Nim : 09011181320020

Jurusan Sistem Komputer

Fakultas Ilmu Komputer Universitas Sriwijaya

2016

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 www.ptba.co.id 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)

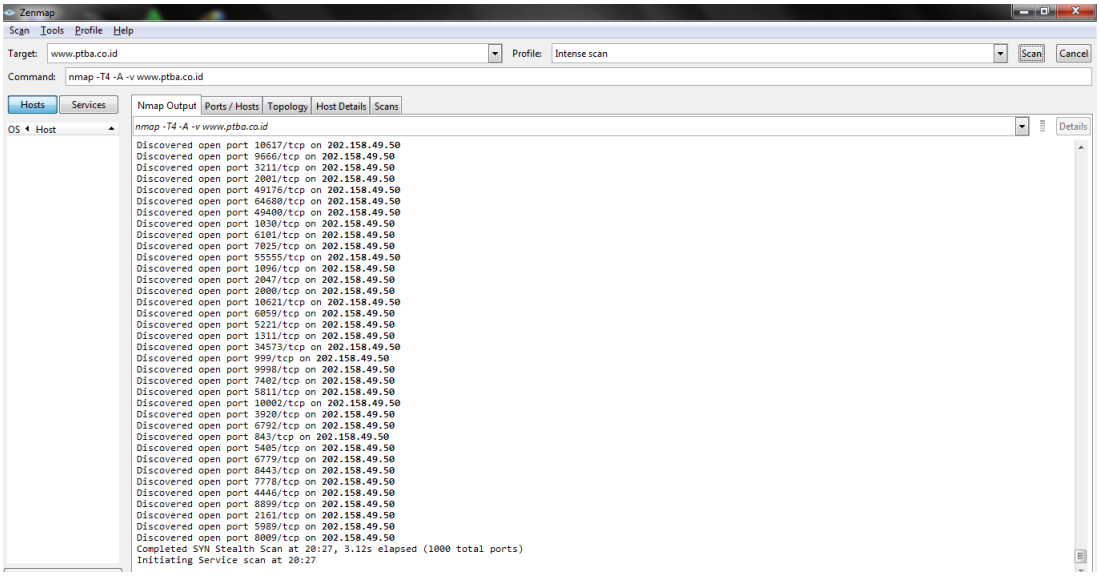
1. TARGET SITUS DAN TOOLS YANG DIGUNAKAN

Pada tugas ke-4 ini saya masih melakukan scanning terhadap perusahaan PT Bukit Asam yang memiliki IP , kemudian saya menggunakan beberapa tools untuk membantu melakukan tugas ini, berikut merupakan toolsnya adalah Wireshark dan Zenmap.

2. LANGKAH-LANGKAH YANG DILAKUKAN

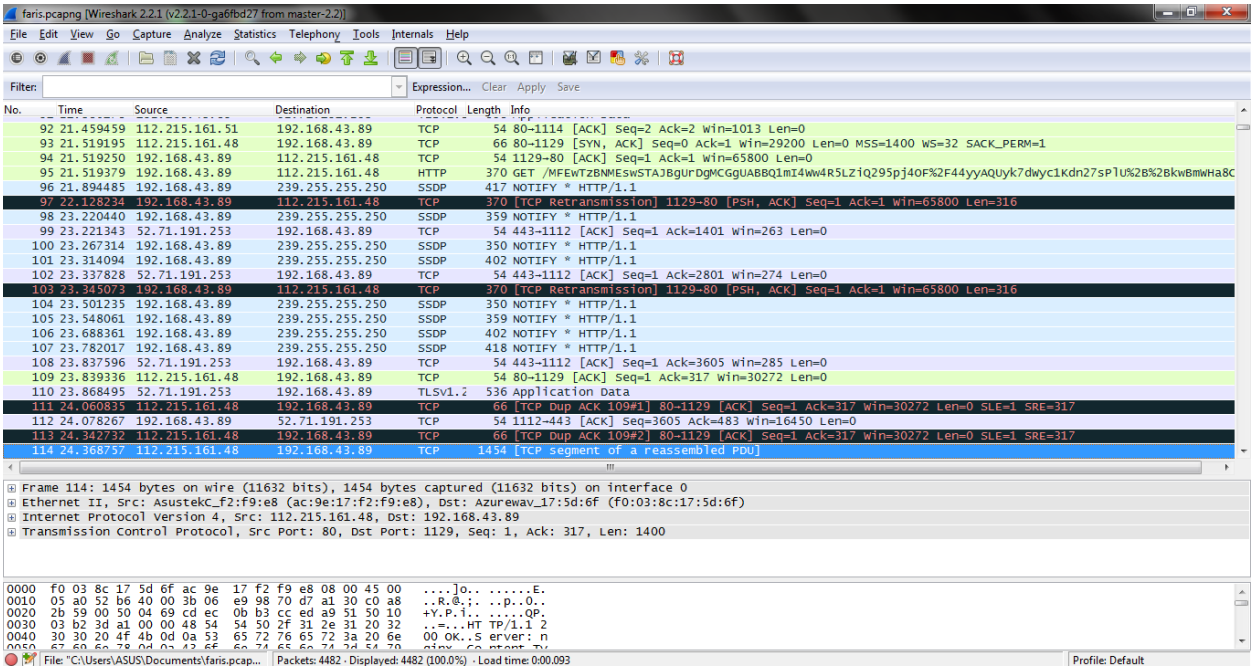
Langkah-langkah pada tugas ini adalah sebagai berikut:

1. Buka Wireshark dan lakukan scanning pada situs yang dituju



Gambar 2.1 Scanning menggunakan Zenmap

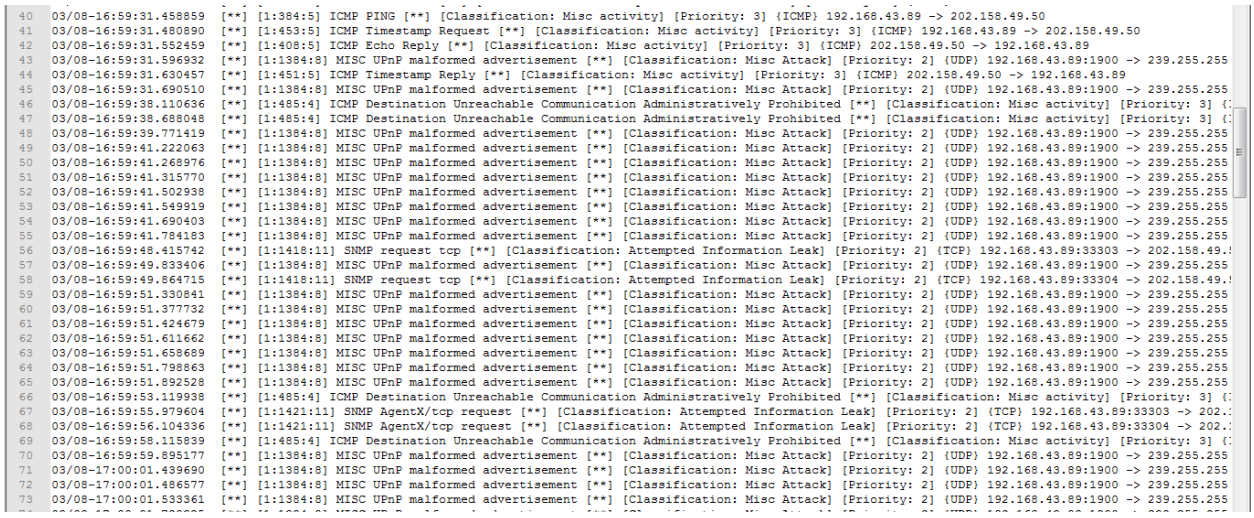
Pada gambar 2.1 melakukan scanning terhadap situs www.ptba.co.id dimana pada saat melakukan scanning pada situs tersebut, dilakukan juga scan wireshark untuk melihat traffic data pada saat scanning tersebut. Dan dapat dilihat pada gambar 2.2 untuk hasil scan wireshark



Gambar 2.2 Traffic Wireshark

2. 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

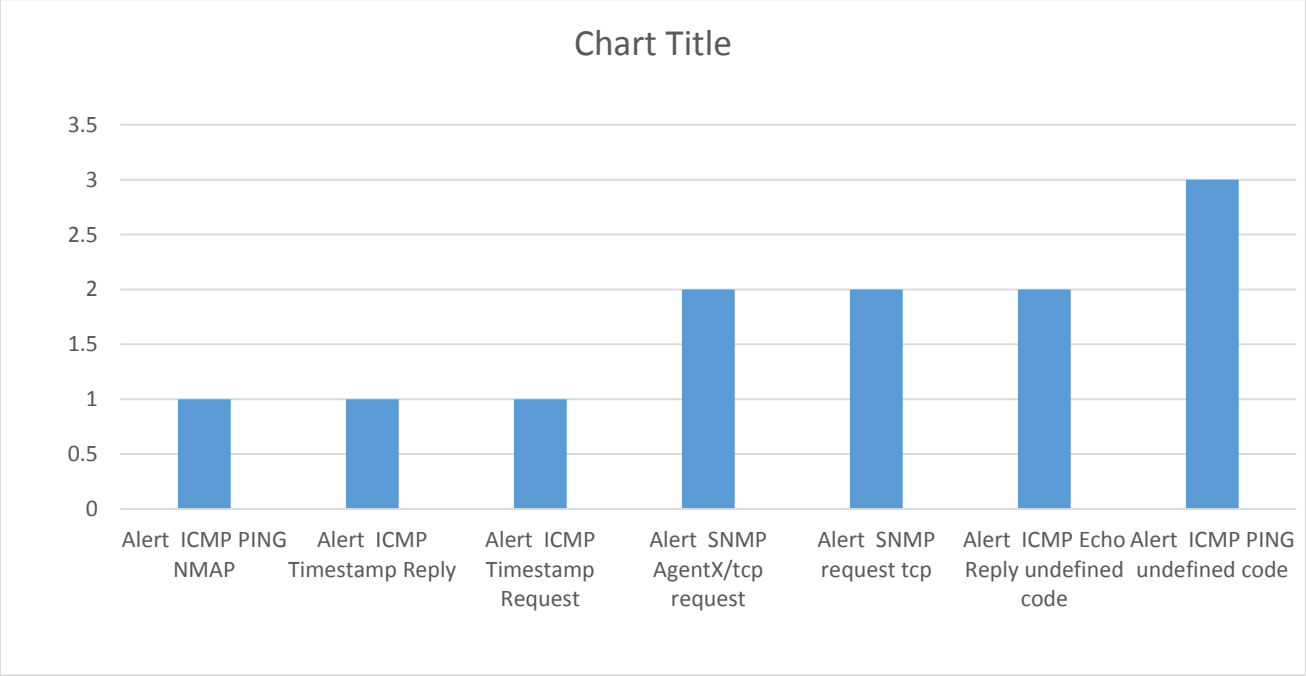
Pada gambar 2.3 terdapat data alert yang dimana pada Wireshark tidak didapatkan, atau lebih tepatnya diekstrak untuk mendapatkan hasil traffic yang tidak dapat dilihat secara rinci oleh wireshark. Dan untuk melakukan ini digunakan alat bantu yaitu countalert.py yang merupakan tools dengan bahasa pyton.

3. HASIL SAJIAN DATA

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

No	ALERT	JUMLAH
1	Alert ICMP PING NMAP	1
2	Alert ICMP Timestamp Reply	1
3	Alert ICMP Timestamp Request	1
4	Alert SNMP AgentX/tcp request	2
5	Alert SNMP request tcp	2
6	Alert ICMP Echo Reply undefined code	2
7	Alert ICMP PING undefined code	3

Table 3.1 Table Hasil Sajian Data



Gambar 3.2 Grafik Alert