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)

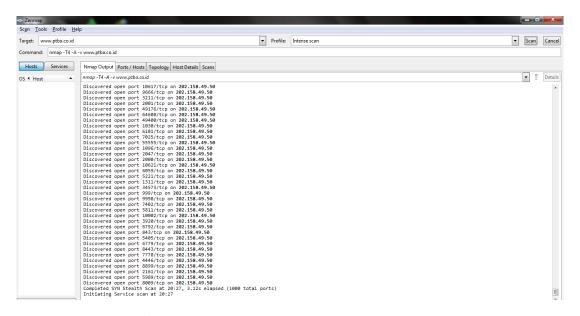
1. TARGET SITUS DAN TOOLS YANG DIGUNAKAN

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

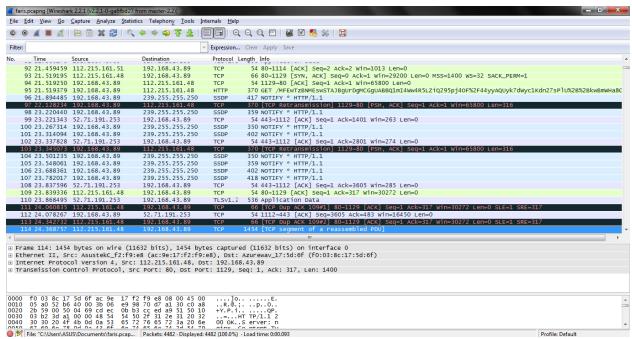
Langkah-langkah pada tugas ini adalah sebagai berikut:

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.

```
[**] [1:384:5] ICMP FING [**] [Classification: Misc activity] [Friority: 3] [ICMP] 192.168.43.89 -> 202.158.49.50

[**] [1:463:5] ICMF Timestamp Request [**] [Classification: Misc activity] [Friority: 3] [ICMP] 192.168.43.89 -> 202.158.49.50

[**] [1:403:5] ICMF DIAM STATE (Classification: Misc activity] [Friority: 3] [ICMP] 192.168.43.89 -> 202.158.49.50

[**] [1:334:8] MISC UPhP malformed advertisement [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:455:4] ICMF DIAM STATE (Communication Administratively Prohibited [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:485:4] ICMP Destination Unreachable Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3] (Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3] (Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3] (Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3] (Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3] (Communication Administratively Prohibited [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:1384:8] MISC UPhF malformed advertisement [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:1384:8] MISC UPhF malformed advertisement [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:1384:8] MISC UPhF malformed advertisement [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:1384:8] MISC UPhF malformed advertisement [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:1384:8] MISC UPhF malformed advertisement [**] [Classification: Misc Actack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255

[**] [1:1384:8] MISC UPhF malformed ad
 03/08-16:59:31.458859
03/08-16:59:31.480890
03/08-16:59:31.552459
03/08-16:59:31.596932
  03/08-16:59:31.630457
  03/08-16:59:31.690510
 03/08-16:59:38.110636
 03/08-16:59:38.688048
  03/08-16:59:39.771419
 03/08-16:59:41.22003

03/08-16:59:41.22003

03/08-16:59:41.268976

03/08-16:59:41.502938

03/08-16:59:41.502938

03/08-16:59:41.690403

03/08-16:59:41.784183
 03/08-16:59:48.415742
 03/08-16:59:49.833406
  03/08-16:59:49.864715
 03/08-16:59:51.330841
  03/08-16:59:51.377732
 03/08-16:59:51.424679
03/08-16:59:51.424679

03/08-16:59:51.611662

03/08-16:59:51.588689

03/08-16:59:51.798863

03/08-16:59:53.119938

03/08-16:59:55.119938

03/08-16:59:55.104336
 03/08-16:59:58.115839
 03/08-16:59:59.895177
 03/08-17:00:01.439690
    03/08-17:00:01.486577
03/08-17:00:01.533361
```

Gambar 2.3 Data Alert

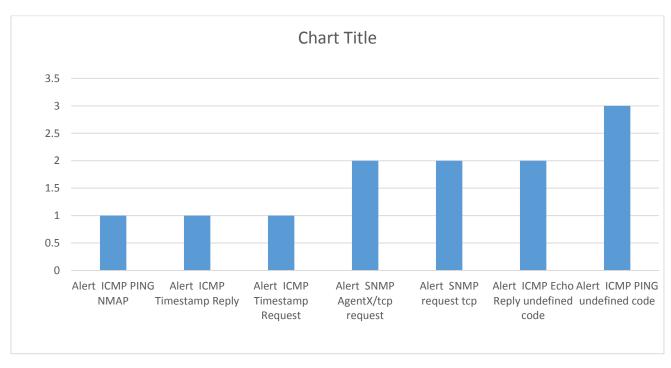
Pada gambar 2.3 terdapat data alert yang dimana pada Wireshark tidak didapatkan, atau lebih tepatnya diekstrak untuk mendapatkan hasil traffic yang tidak dapat dilihat secara rinci oleh wireshark. Dan untuk melakukan ini digunakan alat bantu yaitu countalert.py yang merupakan tools dengan bahasa pyton.

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