Nama : Yayang Prayoga
NIM : 09011181320006

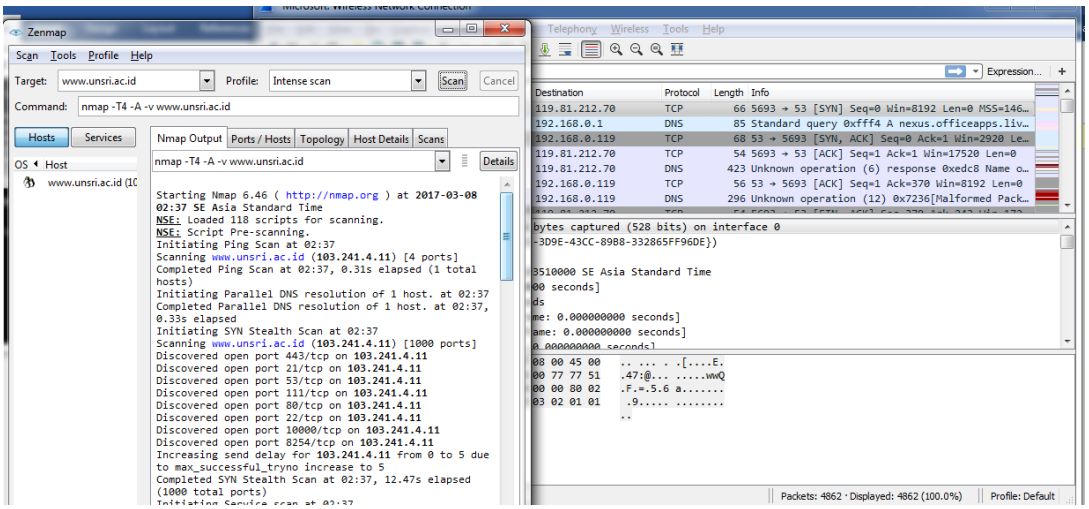
IDS Menggunakan Snort

IDS (*Intrusion Detection System*) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan yang berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan.

Dalam percobaan kali ini saya akan melakukan IDS dengan menggunakan aplikasi seperti *wireshark* dan *nmap* pada windows. Kemudian dilanjutkan dengan mengkompile data dengan menggunakan *Snort*

Langkah-langkahnya sebagai berikut :

1. Lakukan scanning menggunakan perintah "nmap -T4 -A -v www.unsri.ac.id" di nmap sambil menjalankan tool wireshark.

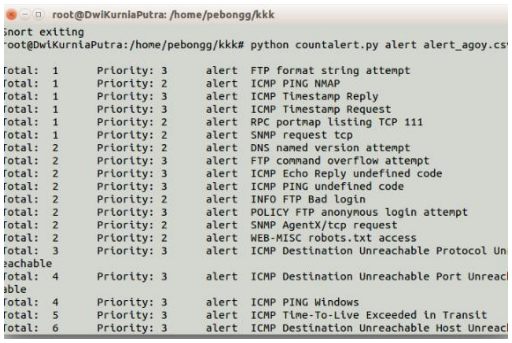


2. Setelah melakukan scanning input perintah ini pada linux "snort -A fast -c /etc/snort/snort.conf -r (dari direktori file pcap)", maka akan menampilkan sebuah table yang terorganisir seperti berikut

No	Alert	Priority	Total
1	FTP format string attempt	3	1
2	ICMP PING NMAP	2	1
3	ICMP Timestamp Reply	3	1
4	ICMP Timestamp Request	3	1
5	RPC portmap listing TCP 111	2	1
6	SNMP request tcp	2	1
7	DNS named version attempt	2	2
8	FTP command overflow attempt	3	2
9	ICMP Echo Reply undefined code	3	2
10	ICMP PING undefined code	3	2
11	INFO FTP Bad login	2	2
12	POLICY FTP anonymous login attempt	3	2

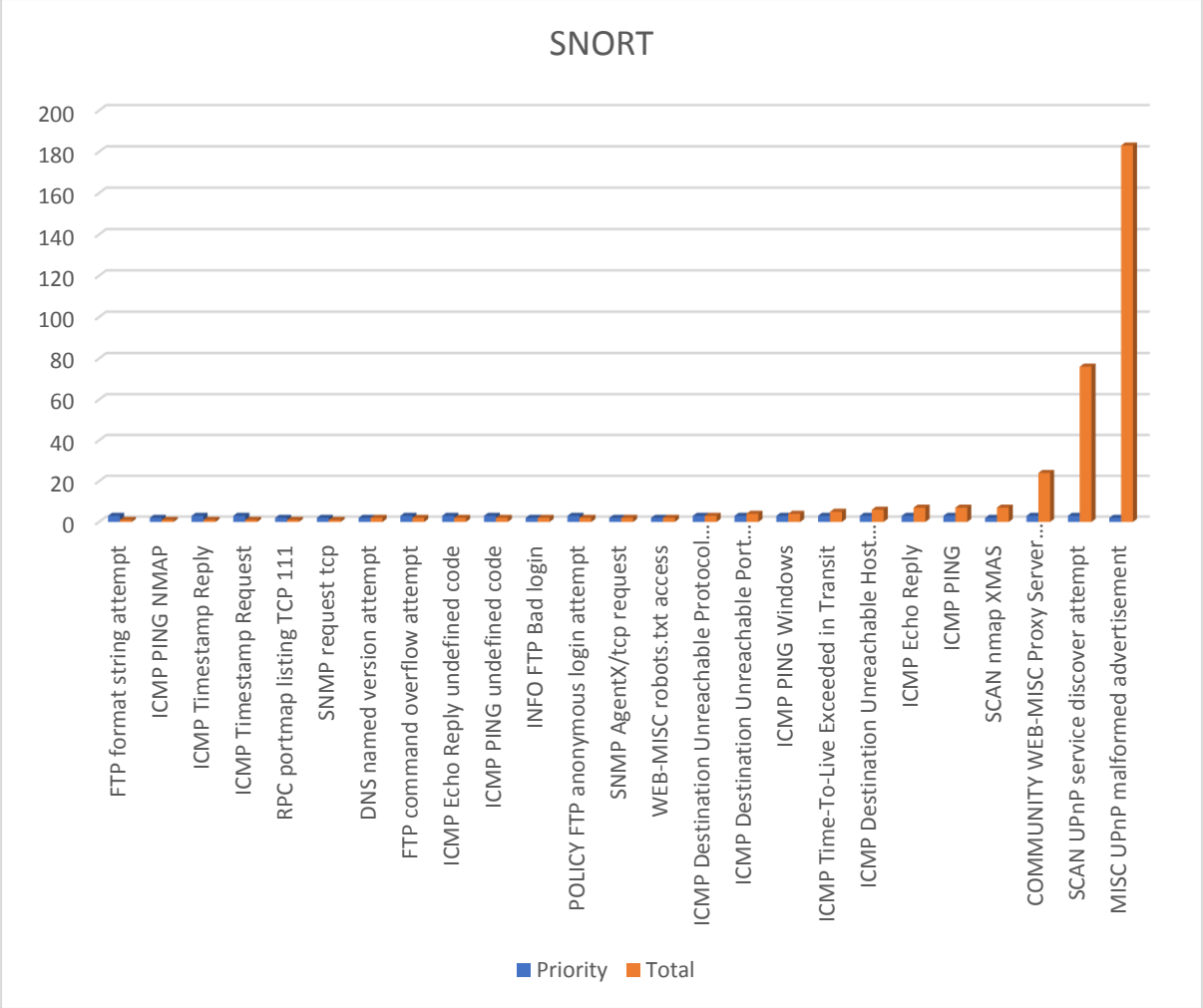
Nama : Yayang Prayoga
NIM : 09011181320006

13	SNMP AgentX/tcp request	2	2
14	WEB-MISC robots.txt access	2	2
15	ICMP Destination Unreachable Protocol Unreachable	3	3
16	ICMP Destination Unreachable Port Unreachable	3	4
17	ICMP PING Windows	3	4
18	ICMP Time-To-Live Exceeded in Transit	3	5
19	ICMP Destination Unreachable Host Unreachable	3	6
20	ICMP Echo Reply	3	7
21	ICMP PING	3	7
22	SCAN nmap XMAS	2	7
23	COMMUNITY WEB-MISC Proxy Server Access	3	24
24	SCAN UPnP service discover attempt	3	76
25	MISC UPnP malformed advertisement	2	183



3. Kemudian untuk mempermudah dalam pemetaan kita buat grafiknya.

Nama : Yayang Prayoga
NIM : 09011181320006



Dari data di atas kita mendapatkan informasi berapakali telah terjadi alert per kurun waktu.